# EXHIBIT 21A

# Table of Contents


Executive Summary ..... 4

Introduction ..... 5

The digital economy is critical to the U.S. economy ..... 6
- Domestic value added by sector and by type ..... 6

Digital economy jobs are proliferating in the United States ..... 6
- Domestic jobs by sector ..... 7

Trade is key to the U.S. digital economy's growth ..... 7
- U.S. exports of ICT services are significant ..... 8
- U.S. exports of potentially ICT-enabled services are even greater ..... 8
- U.S. exports of digitally tradeable services are a consistent "bright spot" for American services providers .. 8
- The make up of ICT exports has been shifting over the decade ..... 9
- The export of many potentially ICT-enabled services is increasingly digital ..... 9
- U.S. exports are concentrated in 10 markets ..... 10
- Digitally tradeable services exports support millions of jobs ..... 10
- Digital trade matters to American small businesses ..... 11
- Every U.S. state exports digitally tradeable services ..... 13

Foreign competitors are also keen to increase exports of digitally tradeable services ..... 13
- Global barriers to U.S. digital exports are on the rise ..... 14
- The case for strong U.S. leadership on digital trade rules . 15

Appendix I: Global Digital Policy Declaration

Appendix II: State Digital Trade One-Pagers

# Executive Summary

The digital economy has become critical to the U.S. economy, driving growth, prosperity, and dynamism across every state. A diverse range of firms not traditionally seen as actors in the digital economy are producing and benefiting from digital goods and services, including businesses in transportation and warehousing, arts and entertainment, and even agriculture and mining. Nearly two-thirds of the digital economy consists of digital services, not digital goods. The digital economy is expanding nearly three times as rapidly as the economy writ large. In short, digitally enabled products and services are not confined to a handful of "big" companies, let alone the "tech" sector.

Digital economy jobs are proliferating in the United States. Jobs tied to the digital economy can be found in nearly every sector, and their number has grown at a faster rate than that of overall job growth over the last decade. These jobs pay well, and compensation growth for digital jobs exceeds that for all jobs generally.

Trade is key to the U.S. digital economy's growth. The bulk of U.S. services exports are digitally tradeable, but the potential for expansion of the digital delivery of services exports remains largely untapped.[1] Developed economies—and particularly Europe—are the top markets for U.S. exports of digitally tradeable services. These exports, coming from every U.S. state, supported more than 3 million direct and indirect U.S. jobs in 2022. America's small business exporters are among those with the most to gain from digital technologies that have the potential to overcome the longstanding hurdles to exporting they face.

Global competition is real. Foreign competitors also see opportunities to increase exports of digitally tradeable services. Leading competitors in international markets include companies based in the European Union, India, and China.

Our competitiveness is being undermined. Unfortunately, global barriers to U.S. digitally tradeable services exports are on the rise. The proliferation of these trade barriers threatens to deprive American workers and companies of the potential benefits of exporting digitally tradeable services.

Equally, if not even more concerning, is the hesitation–or outright failure–of the United States to tackle these trade barriers head-on. The administration needs to work with like-minded partners to secure policies that guarantee the ability to move data across international borders, prohibit forced localization of data or restrictions based on nationality of ownership, and protect source codes, among other objectives. However, U.S. leadership on digital trade is being undermined as the administration increasingly kowtows to radical, fringe views.

The United States finds itself at a moment of promise and peril on digital trade. Export opportunities for digitally tradeable services are expanding rapidly, and the United States is well positioned to build on its formidable advantages in these areas. However, these opportunities are endangered by the spread of digital protectionism and the accumulation of discriminatory digital rules that often target American firms. Here at home, the U.S. failure to address these challenges or recognize the consequences to U.S. companies and workers is compounding the problem.

It is not too late to change course and restore U.S. leadership on digital trade policy. The case for American leadership on digital trade is strong: The administration must recognize these benefits and push forward a vision for digital trade that secures these opportunities for American workers, consumers—and U.S. companies of all sectors and sizes.

1 "Digitally tradeable services" includes exports tied directly to information technologies and the movement of data (e.g., telecommunications services, computer software services, cloud computing and data storage, and other computer services) as well as services that have the potential to be traded digitally: architectural, engineering, project management, and specialized design services; accounting, bookkeeping, auditing, and payroll services; legal services; consulting; research services; advertising; audiovisual and photographic services; banking, insurance, and other financial services; travel arrangement and reservation services; and waste management. The United States is home to world-beating firms in all of these growing industries.

# Introduction

The digital economy is critical to the U.S. economy, driving growth, prosperity, and dynamism across every state. The digital economy is generating good jobs for a growing number of American workers in nearly every sector of the U.S. economy. International trade is playing a central role in the U.S. digital economy's growth: Export opportunities for digitally tradeable services are expanding rapidly, particularly for small businesses and in services sectors that employ millions of Americans.

However, foreign competitors see the same opportunities to increase exports of digitally tradeable services and are moving ahead rapidly. At the same time, global barriers to U.S. digitally tradeable services exports are on the rise. Left unchecked, the proliferation of these trade barriers threatens to deprive American workers and companies of the potential benefits of exporting digitally tradeable services. Advancing digital trade rules would enable the United States to take the lead in fostering digital commerce and push back against the trade barriers that threaten to deprive American workers and companies of the benefits and dynamism of the digital trade era.

Unfortunately, current U.S. policy risks abandoning America's leadership in developing and defending the strong digital trade rules needed to spur growth and innovation at home and around the world. Instead, the Office of the U.S. Trade Representative (USTR) is allowing a faction of fringe interests that have long opposed trade and pro-growth policies to define the U.S. approach to digital trade, undermining the future success of businesses of all sizes and across sectors, from autos, agriculture, pharmaceuticals, medical devices, and aerospace to services like energy, finance, IT, and telecommunications. Now more than ever, the U.S. government needs to advance policies that support the digital trade revolution.

**Value Added by the Digital Economy, 2022 (Billions of Dollars, and Percent)**

| | Value Added | Share of Total Sector Value Added |
|---|---|---|
| All Industries | $2,569.5 | 10.0% |
| Private non-agricultural industries | 2,559.1 | 11.4% |
| Information | 1,024.2 | 73.5% |
| Professional and business services | 575.9 | 17.4% |
| Wholesale trade | 502.2 | 32.5% |
| Manufacturing | 219.3 | 8.3% |
| Retail trade | 193.3 | 11.9% |
| Educational services, health care, and social assistance | 16.1 | 0.8% |
| Transportation and warehousing | 11.5 | 1.2% |
| Finance, insurance, real estate, rental, and leasing | 7.0 | 0.1% |
| Other services, except government | 7.0 | 1.3% |
| Arts, entertainment, rec., accommodation, & food services | 0.8 | 0.1% |
| Utilities | 0.7 | 0.2% |
| Mining | 0.5 | 0.1% |
| Construction | 0.4 | nil |
| Government | 10.4 | 0.4% |

Source: Bureau of Economic Analysis. Data are not available for the agriculture sector.

2 2022 American Community Survey, U.S. Census Bureau, https://data.census.gov/table/ACSDT1Y2022.B28011?q=with%20internet%20subscription and https://data.census.gov/table/ACSDT1Y2022.B28004?q=with%20internet%20subscription.

**U.S. Value Added in the Digital Economy by Type of Good or Service, 2022 (Billions of dollars and Percent)**

| | Value Added | Share of Total, Subtotal |
|---|---|---|
| Total digital economy | $2,569.5 | 100.0% |
| Digital goods (hardware and software) | 901.1 | 35.1 |
| Digital services | 1,668.2 | 64.9 |
| E-commerce | 599.7 | 35.9 |
| Cloud services | 191.9 | 11.5 |
| Telecommunications services | 464.8 | 27.9 |
| Internet and data services | 154.3 | 9.3 |
| All other priced digital services | 257.5 | 15.4 |
| Federal nondefense digital services | 0.3 | nil |

Source: Bureau of Economic Analysis. Data are not available for the agriculture sector.

## The digital economy is critical to the U.S. economy

The digital economy has emerged as a critical driver of growth, prosperity, and dynamism for every state and sector across the United States. According to the U.S. Census Bureau, in 2022 91% of American households had internet subscriptions, including 79% of households earning under $35,000 annually.[2] In 2019, according to the Commerce Department's Bureau of Economic Analysis (BEA), the U.S. digital economy's output surpassed $2 trillion or 10% of total U.S. economic output.[3] It is not surprising that sectors that produce semiconductors, computers and software, or provide internet services and e-commerce sales have a large stake in the digital economy. However, the production of digital goods and services also takes place among a host of firms not traditionally seen as actors in the digital economy, including businesses in transportation and warehousing, arts and entertainment, and even mining. New digital technologies enable firms, workers, and consumers across the economic spectrum to offer new services (e.g., telemedicine in health care) and make ever more sophisticated goods (e.g., GPS-enabled cars).

The importance of the digital economy has also been growing. Digital value-added output increased from $1.8 trillion in 2017 to $2.6 trillion in 2022. The digital economy's share of the total economy expanded from 9.4% to 10.0% in that same period. The value of the digital economy, adjusted for inflation, has grown at an average annual rate of 7.1%, compared to just 2.2% for the economy generally. In other words, the digital economy is expanding more than three times as rapidly as the economy writ large. Even as overall economic output declined in 2020 as a result of pandemic disruptions, output in the digital economy grew.

Nearly two-thirds of the digital economy is digital services as opposed to digital goods (such as hardware and software sold on physical media). Digital services include e-commerce, cloud services, telecommunications services, internet and data services, and other digital services. E-commerce and telecommunications services account for most of these digital services. Cloud services have been a particular benefit to small and medium-sized businesses, enabling them to access the same information and computing power as large firms.[4]

## Digital economy jobs are proliferating in the United States

Millions of people work in the digital economy. As expected, a large number of these jobs are related to computer systems design and related to services, e-commerce, software and data processing. However, many digital economy jobs are in sectors such as the manufacturing of machinery and parts and

3 BEA includes in its definition of the digital economy four major types of goods and services: Infrastructure, or the basic physical materials and organizational arrangements that support the existence and use of computer networks and the digital economy, primarily information and communications technology (ICT) goods and services; e-commerce, or the remote sale of goods and services over computer networks; priced digital services, or services related to computing and communication that are performed for a fee charged to the consumer, and federal nondefense digital services, which is the annual budget for federal nondefense government agencies whose services are directly related to supporting the digital economy. See: Bureau of Economic Analysis, U.S.. Department of Commerce, "Digital Economy," https://www.bea.gov/data/special-topics/digital-economy.

4 Congressional Research Service, "Digital Trade and U.S. Trade Policy," December 9, 2021, p. 8, https://sgp.fas.org/crs/misc/R44565.pdf.

**Full-and Part-time Employment in the Digital Economy, 2022 (Thousands, and Percent)**

| | Jobs | Share of total Industry |
|---|---|---|
| All Industries | 8,857 | 5.7% |
| Private non-agricultural industries | 8,808 | 6.6% |
| Professional and business services | 3,044 | 13.4% |
| Wholesale trade | 1,981 | 33.0% |
| Information | 1,977 | 64.8% |
| Manufacturing | 798 | 6.2% |
| Retail trade | 675 | 4.3% |
| Educational services, health care, and social assistance | 156 | 0.6% |
| Other services, except government | 91 | 1.3% |
| Transportation and warehousing | 61 | 0.9% |
| Finance, insurance, real estate, rental, and leasing | 15 | 0.2% |
| Arts, entertainment, rec., accommodation, & food services | 7 | nil |
| Mining | 1 | 0.2% |
| Construction | 1 | nil |
| Utilities | 1 | 0.2% |
| Government | 48 | 0.2% |

Source: Bureau of Economic Analysis. Data are not available for the agriculture sector.

(truck) transportation and warehousing. One study estimates that the "tech-ecommerce ecosystem" (which includes some tech manufacturing as well as some services tech-related sectors) was the "main job producer" in 40 states from 2017-2021.[5]

The digital economy is a growing source of employment in the United States. The number of jobs tied to the digital economy has increased from 7.6 million in 2017 to 8.9 million in 2022, or at an annual average rate of 3.2% over the decade. This compares to comparable overall job growth of 1.1% per year over this period.

Jobs supporting the digital economy generally pay well. According to BEA data, total compensation paid to workers in the digital economy reached $1.3 trillion in 2022, up from $875 billion in 2017. Compensation has been growing at an average annual rate of 7.7% since 2017, compared to a 5.2% growth rate for all jobs generally.

Because digital services play such a vital role in the U.S. digital economy and are the source of much of its growth, the balance of this report focuses on global markets for U.S. digital services output and employment and the role U.S. exporters play in those markets.

## Trade is key to the U.S. digital economy's growth

Currently, digital exports play a smaller role in U.S. services output than exports of goods do for manufacturing. But because the digital economy has become such an important generator of both economic and job growth, pursuing an expansion of digital trade opportunities in global markets presents an opportunity to support that growth with feedback effects that are no less important than those sought from goods exports.

The United States exported nearly $1 trillion in non-government services in 2022. Most of these exports were delivered digitally: 10% were information and communications technology (ICT) services, 61% were potentially ICT-enabled services, and the balance were non-digitally delivered services. All of these exports contribute to the health of the digital economy and the jobs tied to it.

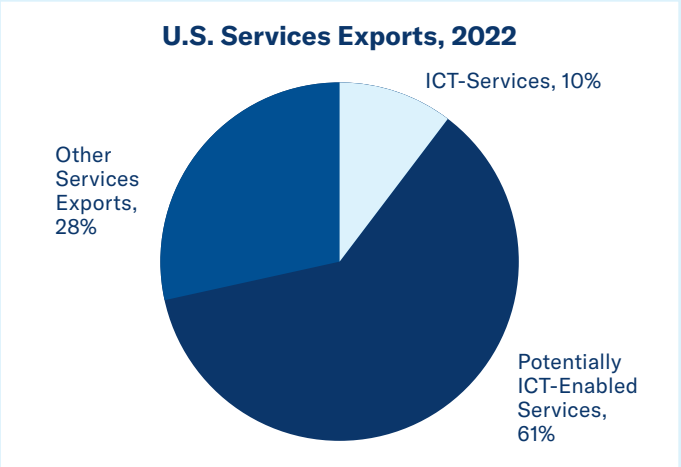
5 Michael Mandel, "Tech-Ecommerce Drives Job Growth in Most States," Progressive Policy Institute, October 18, 2021, https://www.progressivepolicy.org/blogs/tech-ecommerce-drives-job-growth-in-most-states/.

## U.S. exports of ICT services are significant

ICT services are those tied directly to information technologies and the movement of data, such as telecommunications services, computer software services, cloud computing and data storage, and other computer services. The United States exported $93 billion in ICT services to the world in 2022. U.S. exports of ICT services are significant—more than U.S. exports of key manufactured goods including basic chemicals ($86 billion), semiconductors ($75 billion), motor vehicles ($68 billion), or agricultural crops($66 billion).

## U.S. exports of potentially ICT-enabled services are even greater

The total value of exports of ICT services pales in comparison to the total value of services exports that could be traded digitally. U.S. government agencies refer to these as "potentially ICT-enabled services," and they include architectural, engineering, project management, and specialized design services; accounting, bookkeeping, auditing, and payroll services; legal services; consulting services; research services; advertising; audiovisual and photographic services; banking, insurance, and other financial services; travel arrangement and reservation services; and certain waste treatment and de-pollution services. The United States is home to world-beating firms in all of these growing industries. In 2022, exports of potentially-ICT enabled services totaled $553 billion. Some of the value of these services were delivered in person in foreign markets; others were delivered digitally, via the internet.

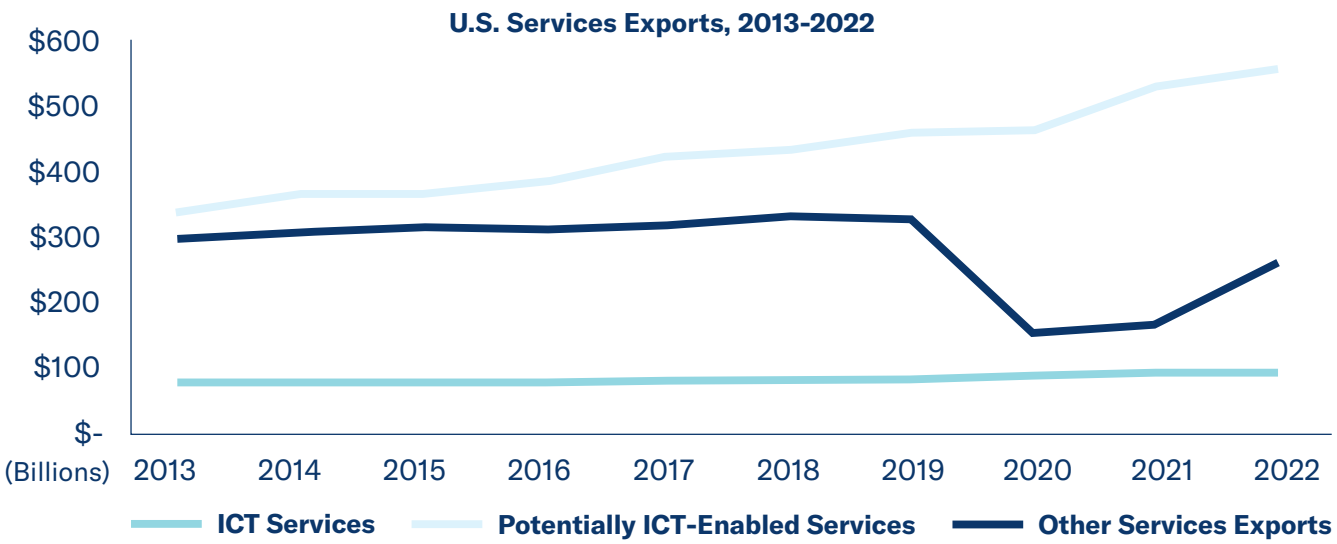



Source: Estimated by Trade Partnership Worldwide

This paper will refer to the full array of these ICT services and potentially ICT-enabled services together as digitally tradeable services.

## U.S. exports of digitally tradeable services are a consistent "bright spot" for American services providers

U.S. exports of digitally tradeable services have been steadily growing over the last decade–even when the pandemic reduced U.S. exports of non-digital services exports by half. Overall, U.S. services exports increased by 29% over the past decade, primarily due to the strength in growth in digital trade exports. Since 2013, U.S. ICT exports have grown by 29%. Potentially ICT-enabled exports increased by 66%. Over the decade, exports of other services declined by 13%.




Source: Estimated by Trade Partnership Worldwide

## The make up of ICT exports has been shifting over the decade

The steady increase in overall export growth of ICT services masks some important shifts in the services that make up this group. While still the largest component, the value of royalties from computer software paid by foreign customers has dropped 12% over the decade. Similarly, exports of telecommunications services have declined, by 46%. But these declines have been more than offset by strong increases in exports of cloud computing and data storage services (up 794% from 2013-2022), and computer software services (up 240% over the period).

## The export of many potentially ICT-enabled services is increasingly digital

The pandemic had an important impact on the delivery of potentially ICT-enabled services. When in-person delivery of these services was not universally possible with the global Covid-19 reductions in travel, many providers figured out how to deliver their services digitally. This transition happened both domestically and internationally, and the delivery of services to foreign customers became increasingly digital.

The ability to deliver these services digitally likely contributed to the increase in export growth experienced by several potentially ICT-enabled services. For example, from 2013-2019, business management and consulting services exports grew at an average annual rate of 10%; from 2020 to 2022, that annual rate of growth increased to 17%. Similarly, exports of insurance services grew at an average annual rate of 8% pre-pandemic and 33% post-pandemic; legal services were up 6% per year pre-pandemic and 10% post-pandemic, and architectural, engineering and miscellaneous technical services exports fell at an average annual rate of 4% pre-pandemic, then grew 10% per year beginning in 2020.

The diversity of sectors within the potentially ICT-enabled services category shows why digital trade matters so much for industries that are

**U.S. Exports of Potentially ICT-Enabled Services, by Type (Millions, and Percent)**

| Sector | 2013 | 2022 | Change ($) | Change (%) |
|---|---|---|---|---|
| Business Management and Consulting Services | $36,346 | $101,594 | $65,248 | 180% |
| Financial Management and Advisory Services | 51,798 | 71,066 | 19,268 | 37% |
| Royalties from Industrial Processes | 45,969 | 59,631 | 13,662 | 30% |
| Research and Development and Testing Services | 30,113 | 57,754 | 27,641 | 92% |
| Credit-Related Services | 18,142 | 32,850 | 14,708 | 81% |
| Misc. Financial Services | 18,213 | 30,348 | 12,135 | 67% |
| Insurance Services | 15,651 | 22,668 | 7,017 | 45% |
| Implicit Financial Services | 10,427 | 22,594 | 12,167 | 117% |
| Advertising | 10,043 | 22,237 | 12,194 | 121% |
| Misc. Business, Professional, and Technical Services | 4,956 | 20,670 | 15,714 | 317% |
| Payments for Trademarks | 16,268 | 19,834 | 3,566 | 22% |
| A/V Services (Personal) | 17,150 | 19,751 | 2,601 | 15% |
| Legal Services | 9,251 | 16,426 | 7,175 | 78% |
| Architectural, Engineering, and Misc. Tech. Services | 16,453 | 12,233 | (4,220) | -26% |
| Securities Transactions | 11,218 | 10,865 | (353) | -3% |
| Database and Other Information Services | 6,563 | 10,485 | 3,922 | 60% |
| Misc. Personal, Cultural, and Recreational Services | 3,029 | 6,544 | 3,515 | 116% |
| Franchise Fees | 6,132 | 6,117 | (15) | 0% |
| Accounting, Auditing, and Bookkeeping | 1,399 | 3,308 | 1,909 | 136% |
| Trade-Related Services | 1,129 | 2,135 | 1,006 | 89% |
| A/V Services (Books and Tapes) | 623 | 1,869 | 1,246 | 200% |
| A/V Services (Live Events) | 934 | 1,827 | 893 | 96% |
| News Agency Services | 331 | 273 | (58) | -18% |
| A/V Services (Movies and TV) | 1,077 | 236 | (841) | -78% |

Source: Estimated by Trade Partnership Worldwide

not generally associated with "information technology." For example, business, management and consulting services have overtaken financial management and advisory services as the leading potentially ICT-enabled services export sector.

## U.S. exports are concentrated in 10 markets

Ten countries accounted for 70% of total U.S. digitally tradeable exports in 2022. Developed economies are the top markets for U.S. exports of digitally tradeable services. In 2022, Ireland was the top export market for both ICT services ($13 billion) and potentially ICT-enabled services ($70 billion). Canada, China, Germany, Japan, Switzerland, and the UK were among the top 10 individual markets for digitally tradeable services. Hong Kong, Brazil, and Australia were among the top 10 markets for ICT services, while the UK's Caribbean Islands (largely financial services), Singapore, and the Netherlands were among the top 10 markets for potentially ICT-enabled services. Collectively, EU countries accounted for $29 billion (31%) of U.S. exports of ICT services exports and $163 billion (29%) of potentially ICT-enabled services exports in 2022.

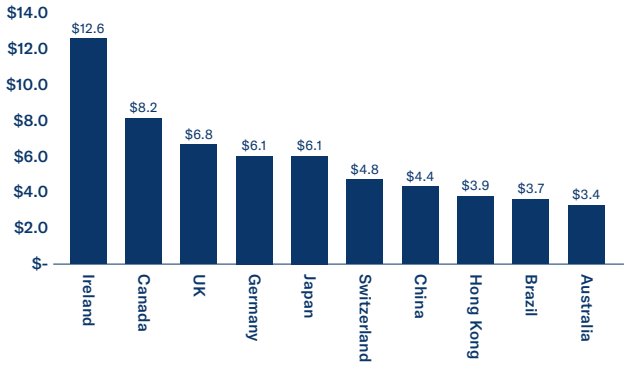
As a region, Europe is the top destination for U.S. exports of digitally tradeable services, particularly potentially ICT-enabled services exports. For this reason, the U.S. business community has urged the administration to prioritize implementation of the EU-U.S. Data Privacy Framework (the successor agreement to Privacy Shield) and to ensure that EU initiatives such as the Digital Markets Act and the Digital Services Act do not discriminate against U.S. firms.

Asia and the Pacific are the second largest regional market for U.S. digital trade. Exports of ICT services are currently strong, but potentially ICT-enabled services remains a much larger category, suggesting untapped potential that could be unlocked through the implementation of strong digital trade rules.

## Digitally tradeable services exports support millions of jobs

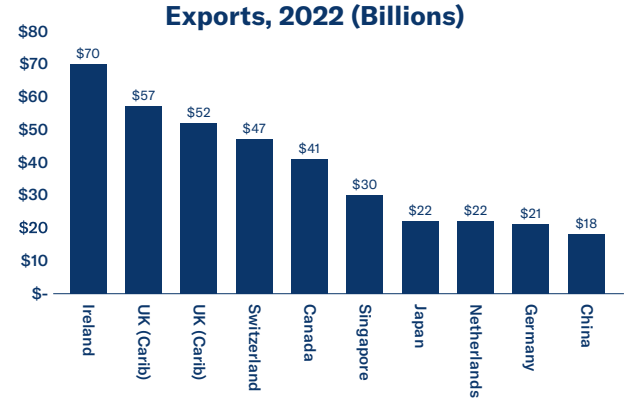
Exports of digitally tradeable services support millions of American jobs. In 2022, just over 3 million U.S. jobs were supported by digital trade. U.S. exports of ICT services supported an estimated 358,000 U.S. jobs,

**Top Markets for U.S. ICT Services Exports, 2022 (Billions)**




Source: Estimated by Trade Partnership Worldwide

**Top Markets for U.S. Potentially ICT-Enabled Exports, 2022 (Billions)**




Source: Estimated by Trade Partnership Worldwide

**U.S. Digitally Tradeable Services Exports, by Region and Type, 2022 (Millions, and Percent)**

| | ICT Services | | Potentially ICT-Enabled Services | |
|---|---|---|---|---|
| **Region** | **Exports** | **Export Share** | **Exports** | **Export Share** |
| Europe | $41,483 | 44% | $316,215 | 50% |
| Asia & Pacific | $29,105 | 31% | $147,498 | 21% |
| Central & South America | $9,807 | 11% | $95,392 | 16% |
| North America | $11,039 | 12% | $65,751 | 10% |
| Middle East & Africa | $1,904 | 2% | $21,527 | 4% |

Source: Estimated by Trade Partnership Worldwide

more than the number of jobs supported by U.S. petroleum product exports (340,000). Exports of potentially ICT-enabled services supported nearly 2.7 million U.S. jobs, more than the combined number of U.S. jobs supported by exports of primary metals, fabricated metal products, machinery, and computers and electronics.

Jobs supported by exports of digitally tradeable services grew over the last decade. More than 955,000 U.S. jobs were added as a result of the increase in U.S. digital trade from 2013-2022. These jobs are found in every sector of the economy, not just those directly related to exporting. As the companies exporting digital services grow, the ripple effects of that growth are felt throughout the economy, supporting still more jobs in still more sectors (e.g., restaurants, schools, entertainment venues).

## Digital trade matters to American small businesses

America's small business exporters are among those with the most to gain from digital trade. While U.S. small and medium-sized businesses generate about two-thirds of all new U.S. jobs, it is often overlooked that 97% of the nearly 300,000 American companies that export are small and medium-sized businesses. These firms account for about one-third of U.S. merchandise exports, according to data from the U.S. Department of Commerce. However, only about one in every 100 of America's 30 million small businesses export. In countries such as Germany and Switzerland, the share of small or medium-sized firms that sell their products abroad is approximately five to ten times larger on a per capita or per firm basis.

In this context, the digital trade revolution offers impressive new opportunities for America's small businesses. New digital technologies have the potential to overcome longstanding hurdles facing small exporters.

A U.S. Chamber report entitled *Growing Small Business Exports: How Technology Strengthens American Trade* uncovered some surprising findings. Based on a national survey of more than 3,800 small businesses and a related economic analysis, the report produced a new estimate that 9% of U.S. small businesses currently export goods or services, a figure considerably higher than indicated by official statistics. The report estimated that small business exports generated $541 billion in output in 2017 and supported more than 6 million U.S. jobs. Small businesses that export have been expanding the overseas markets they serve, the report found, from an average of seven countries in 2016 to 10 countries in 2018.

These larger-than-the-official-statistics results indicate that digital trade is already contributing to the expansion of U.S. small business exports and job creation. The Chamber's study found digital trade's boost to small business exporters is especially pronounced in the following three areas:

1. Digital advertising plays an overlooked but critical role in allowing U.S. small businesses to economically reach potential foreign customers in a targeted fashion. Small businesses simply had no such tools in the pre-internet era: print advertising in newspapers or direct mail were never feasible options for U.S. small businesses trying to tap even nearby and familiar markets such as Canada or Europe.

2. Modern digital tools are revolutionizing payment collection, cited by small business exporters as a top challenge. Uncertainty around international payment collection was a principal brake on small business exports even a few years ago, but such risks and foreign exchange complexities can now be managed in a cost-effective manner by digital payment services.

3. International shipment firms, including express delivery companies, today provide comprehensive services that handle customs clearance procedures and costs for small business owners who lack the expertise and time to tackle the minutiae of such matters. The evidence supports the view that online channels reduce transaction costs associated with international trade significantly.

One takeaway is that digital trade allows small business exporters and larger firms to prosper together. Some of the services mentioned above in areas such as digital advertising (e.g., Google's Market Finder) are fostering new trade ecosystems of mutual benefit.

The cumulative effect of these digital technologies is that more small business exporters are able to reach more international markets. The Chamber's findings are supported by an earlier study which found that 94% of the smallest 10% of commercial sellers on eBay engage in exporting, not far behind the largest 10% (99%). Only 5% of commercial sellers in that study were single country exporters, with a remarkable 81% selling to five or more foreign countries.

The Chamber report found that the digital trade revolution nonetheless remains a work in progress for U.S. small business exporters. While 92% of small businesses that export use digital tools, a large majority flagged ongoing concerns. Small

## State Services Exports, by Type, 2022 (Millions, and Percent)

| State | Value | | | | Share | | |
|---|---|---|---|---|---|---|---|
| | ICT | Potentially ICT-Enabled | Not ICT-Enabled | Total | ICT | Potentially ICT-Enabled | Not ICT-Enabled |
| AK | $0.5 | $185.9 | $1,821.0 | $2,007.4 | 0% | 9% | 91% |
| AL | 179.7 | 2,936.7 | 1,778.0 | 4,894.3 | 4% | 60% | 36% |
| AR | 146.5 | 1,169.1 | 946.9 | 2,262.5 | 6% | 52% | 42% |
| AZ | 1,175.1 | 8,403.1 | 4,678.4 | 14,256.6 | 8% | 59% | 33% |
| CA | 27,927.3 | 114,748.6 | 35,959.2 | 178,635.1 | 16% | 64% | 20% |
| CO | 3,467.4 | 8,472.6 | 4,533.8 | 16,473.9 | 21% | 51% | 28% |
| CT | 637.7 | 11,230.7 | 1,718.9 | 13,587.2 | 5% | 83% | 13% |
| DC | 802.7 | 5,684.7 | 1,178.4 | 7,665.9 | 10% | 74% | 15% |
| DE | 14.0 | 3,542.2 | 537.7 | 4,093.8 | 0% | 87% | 13% |
| FL | 2,450.7 | 22,240.7 | 22,258.9 | 46,950.4 | 5% | 47% | 47% |
| GA | 3,607.1 | 14,335.5 | 8,753.1 | 26,695.8 | 14% | 54% | 33% |
| HI | 21.4 | 573.7 | 2,242.7 | 2,837.8 | 1% | 20% | 79% |
| IA | 74.7 | 3,429.7 | 865.0 | 4,369.4 | 2% | 78% | 20% |
| ID | 55.6 | 1,262.9 | 752.9 | 2,071.3 | 3% | 61% | 36% |
| IL | 1,536.8 | 26,716.5 | 14,513.1 | 42,766.4 | 4% | 62% | 34% |
| IN | 132.9 | 6,174.7 | 2,790.6 | 9,098.2 | 1% | 68% | 31% |
| KS | 162.1 | 2,692.2 | 1,043.0 | 3,897.4 | 4% | 69% | 27% |
| KY | 60.1 | 1,929.8 | 1,989.1 | 3,978.9 | 2% | 48% | 50% |
| LA | 26.5 | 2,647.7 | 6,246.7 | 8,920.9 | 0% | 30% | 70% |
| MA | 5,121.0 | 26,991.5 | 7,177.2 | 39,289.7 | 13% | 69% | 18% |
| MD | 1,900.0 | 10,234.8 | 4,106.7 | 16,241.5 | 12% | 63% | 25% |
| ME | 45.8 | 977.3 | 1,008.6 | 2,031.7 | 2% | 48% | 50% |
| MI | 520.9 | 7,233.3 | 5,920.3 | 13,674.4 | 4% | 53% | 43% |
| MN | 853.9 | 8,465.3 | 2,666.9 | 11,986.1 | 7% | 71% | 22% |
| MO | 1,114.8 | 6,419.9 | 3,071.5 | 10,606.2 | 11% | 61% | 29% |
| MS | 7.6 | 775.4 | 1,045.4 | 1,828.4 | 0% | 42% | 57% |
| MT | 33.3 | 562.0 | 653.9 | 1,249.2 | 3% | 45% | 52% |
| NC | 2,579.5 | 18,119.5 | 5,790.9 | 26,489.9 | 10% | 68% | 22% |
| ND | 30.8 | 347.8 | 593.1 | 971.7 | 3% | 36% | 61% |
| NE | 272.2 | 1,541.8 | 512.8 | 2,326.8 | 12% | 66% | 22% |
| NH | 515.9 | 2,203.6 | 894.4 | 3,613.9 | 14% | 61% | 25% |
| NJ | 2,155.6 | 16,813.5 | 7,918.5 | 26,887.6 | 8% | 63% | 29% |
| NM | 14.0 | 1,364.5 | 1,004.0 | 2,382.5 | 1% | 57% | 42% |
| NV | 117.1 | 1,936.9 | 4,341.1 | 6,395.1 | 2% | 30% | 68% |
| NY | 6,822.3 | 88,205.3 | 24,472.2 | 119,499.7 | 6% | 74% | 20% |
| OH | 513.2 | 14,942.0 | 7,770.4 | 23,225.6 | 2% | 513.2 | 33% |
| OK | 36.8 | 1,218.9 | 2,009.4 | 3,265.1 | 1% | 36.8 | 62% |
| OR | 1,350.8 | 4,198.0 | 2,717.1 | 8,265.9 | 16% | 1,350.8 | 33% |
| PA | 1,383.0 | 16,199.0 | 6,884.5 | 24,466.5 | 6% | 1,383.0 | 28% |
| RI | 112.8 | 961.7 | 806.4 | 1,880.9 | 6% | 112.8 | 43% |
| SC | 167.7 | 2,957.8 | 3,553.1 | 6,678.6 | 3% | 167.7 | 53% |
| SD | 8.0 | 1,310.7 | 301.7 | 1,620.3 | 0% | 8.0 | 19% |
| TN | 417.1 | 7,459.2 | 4,340.6 | 12,217.0 | 3% | 417.1 | 36% |
| TX | 5,485.3 | 37,836.4 | 22,201.2 | 65,522.9 | 8% | 5,485.3 | 34% |
| UT | 1,626.2 | 4,931.4 | 2,192.9 | 8,750.5 | 19% | 1,626.2 | 25% |
| VA | 3,544.3 | 12,948.5 | 6,929.0 | 23,421.8 | 15% | 3,544.3 | 30% |
| VT | 86.0 | 582.5 | 512.7 | 1,181.2 | 7% | 86.0 | 43% |
| WA | 12,758.5 | 12,626.9 | 6,387.6 | 31,773.1 | 40% | 12,758.5 | 20% |
| WI | 1,255.3 | 3,947.3 | 2,140.9 | 7,343.4 | 17% | 1,255.3 | 29% |
| WV | 8.9 | 450.2 | 567.1 | 1,026.3 | 1% | 8.9 | 55% |
| WY | 0.5 | 175.0 | 325.5 | 501.0 | 0% | 0.5 | 65% |
| **US** | **$93,338.0** | **$553,315.0** | **$255,424.6** | **$902,077.6** | **10%** | **$93,338.0** | **28%** |

Source: Estimated by Trade Partnership Worldwide

businesses surveyed noted the challenge posed by foreign regulations such as data localization requirements, privacy rules, and liability risks, as well as taxes. However, with further progress on these fronts and further steps to take advantage of digital trade, the small businesses surveyed projected a 14% increase in sales, which would increase U.S. economic output by $81 billion and add 900,000 jobs.

## Every U.S. state exports digitally tradeable services

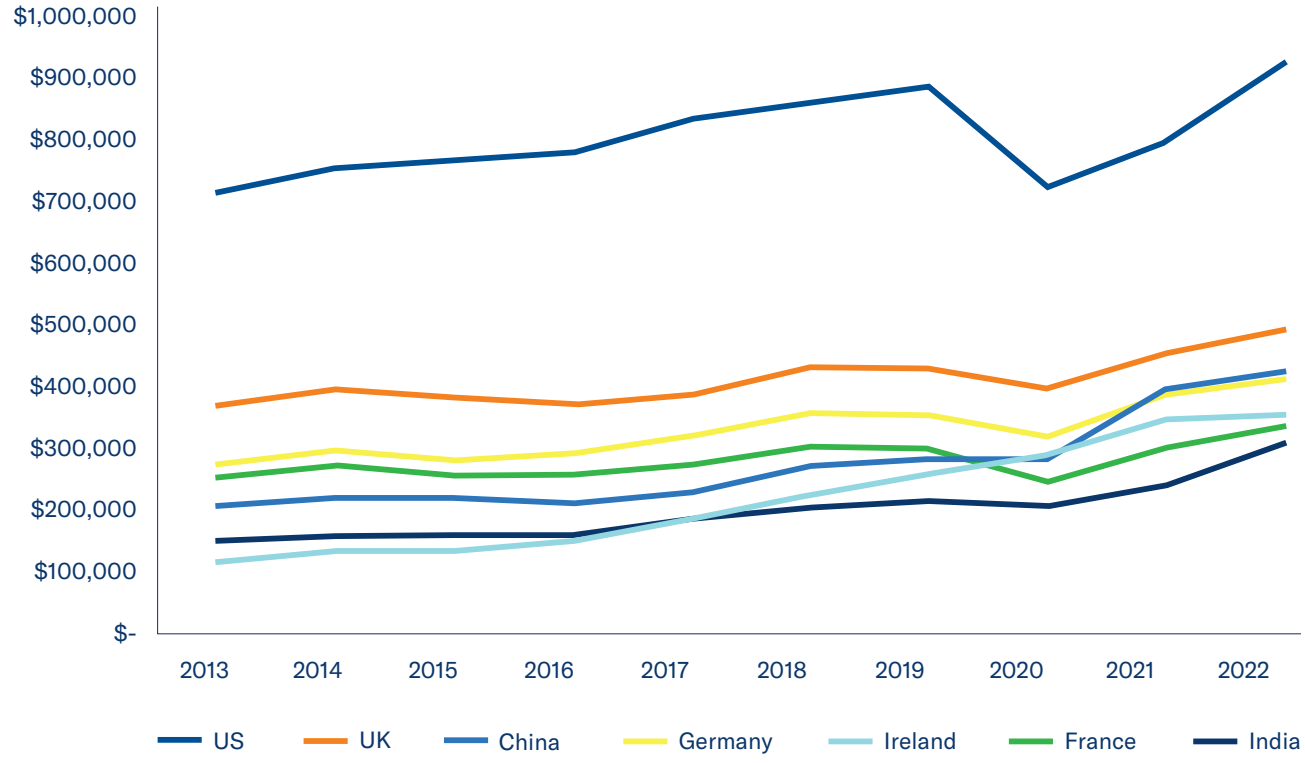
Every U.S. state exports digitally tradeable services. Digital services trade accounts for most of the services exports of 40 states plus the District of Columbia. ICT services accounted for 40% of Washington's total services exports in 2022, the highest share of any state. Potentially ICT-enabled services exports accounted for 80% or more of the total services exports of Delaware (87%), Connecticut (83%) and South Dakota (81%).

In all, potentially ICT-enabled services accounted for greater shares of total exports than the national average (61%) for 18 states plus the District. These states have particularly large stakes in securing strong digital trade rules that opens new markets for these services.

## Foreign competitors are also keen to increase exports of digitally tradeable services

U.S. services exporters do not operate in a vacuum, and they face growing competition from foreign competitors similarly trying to increase exports of digitally tradeable services. While not quite apples-to-apples,[6] data from the World Trade Organization (WTO) allows comparisons between export trends for the United States and other top exporters.

**7 Largest World Exporters of Digitally Tradeable Services, 2013-2022**




Source: WTO Data

6 The World Trade Organization (WTO) data for ICT services differs slightly from the classification used by the U.S. Bureau of Economic Analysis. The WTO data includes the entire "Telecommunications, computer, and information services" (BOP6–SI), while the United States classifies some of the information services subsectors as potentially ICT-enabled. Additionally, the United States includes "Royalties from Computer Software" among its ICT services sectors, which falls under "Licenses to reproduce and/or distribute computer software" (BOP6–SH3) in the WTO data. Unfortunately, only a limited number of countries report data in BOP6–SH3, so it is not possible to aggregate the various WTO data and better approximate the U.S. definition.

Global exports of digitally tradeable services have been growing. In 2022, the value of these exports exceeded $7 trillion, nearly double the $4.9 trillion exported in 2013. Seven countries accounted for nearly half world exports of digitally tradeable services in 2022. The United States strongly leads, followed by the United Kingdom, China, Germany, Ireland, France and India.

While the United States has a strong lead, other countries are growing their digitally tradeable services exports by nearly the same value. Between 2013 and 2022, WTO data show the total value of U.S. digitally tradeable services exports increased by $209 billion. However, Ireland increased its digitally tradeable services exports by $239 billion over the same period, and China by $217 billion. India's exports increased by $160 billion.

As other countries have competed for and won sales of these important services in international markets, the U.S. share of world digitally tradeable services exports has fallen over the last decade, from 15% in 2013 to 13% in 2022, as these other growing suppliers make inroads into new markets.

## Global barriers to U.S. digital exports are on the rise

Even though there are significant opportunities for American workers and companies to increase digital trade, the outlook for their ability to increase sales to foreign markets is uncertain. Barriers to digital trade exist and in many cases have been proliferating.[7] While tariffs on digital goods exports largely have been tamed by plurilateral and bilateral trade agreements, this is not the case for digital services trade. Barriers affecting digitally tradeable services include data localization requirements, cross-border data flow limitations, infringement of intellectual property rights, forced technology transfer, measures that violate the WTO's national treatment obligations by discriminating against partially foreign-owned firms, strictures on government procurement that violate the WTO Government Procurement Agreement, and a host of regulatory barriers. In some cases, these measures are crafted to target American firms exclusively.

Multilateral and many bilateral and regional trade agreements address some—but not all—of these barriers, and often in different ways. Additionally, a policy tool that is not updated to reflect new technologies can very quickly become a barrier to digital exports. Left unchecked, the proliferation of these trade barriers threatens to deprive American workers and companies of the potential benefits of exporting digitally tradeable services.

To illustrate the extent of digital trade barriers, the European Centre for International Political Economy published several years ago its Digital Trade Restrictiveness Index (DTRI), which "measures how 64 countries in the world restrict digital trade." The index "reveals that many leading economies put significant restrictions on digital trade. These restrictions drive up costs for businesses as well as for consumers."

This index indicates that China maintains the most restrictive digital trade policies, followed by Russia, India, Indonesia, Vietnam, Brazil, and Turkey. The appearance on this list of large emerging markets of significant commercial interest to American business underscores the significant scope of the harm digital protectionism can inflict. But ECIPE also makes a point of noting that France and Germany are of concern as well (and noteworthy given their place as top global exporters of digitally tradeable services: "It is worth repeating that the DTRI shows that two European countries–France and Germany–are among the 15 most restrictive countries in digital trade policy. Their restrictive culture is very different from the digital openness of a country like Ireland. Their restrictive stand has often prevented the EU from making fast progress to create a Digital Single Market (DSM)."

The ongoing proliferation of these barriers to digitally tradeable services trade has been further documented in a recent study by the Information Technology & Innovation Foundation, entitled *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. It found that "the number of data-localization measures in force around the world has more than doubled in four years. In 2017, 35 countries had implemented 67 such barriers. Now, 62 countries have imposed 144 restrictions—and dozens more are under consideration." The experience of Chamber member companies affirms this trend and its widespread nature.

Not only does the spread of barriers to digital services trade threaten to block the opportunities described above, it threatens to consign economies to a low-productivity path of slower growth. The ITIF study found that "a 1point increase in a nation's

7 An excellent overview of these barriers can be found in Congressional Research Service, op. cit., pp. 14-23.

data restrictiveness cuts its gross trade output 7 percent, slows its productivity 2.9 percent, and hikes downstream prices 1.5 percent over five years." The result is that the economic prospects of major emerging markets will be dampened even in areas not directly touched by digital trade.

## The case for strong U.S. leadership on digital trade rules

For decades, through Democratic and Republican administrations, the United States has been the leader in developing and defending digital trade rules that have spurred growth and innovation in the United States and around the world. These rules secure the ability to move data across international borders, prohibit forced localization of data or restrictions based on nationality of ownership, and protect source codes, among other objectives. Now more than ever, the U.S. government needs to work with like-minded partners to secure policies that achieve these goals.

However, current U.S. policy seems poised to snatch defeat from the jaws of victory for American workers and companies engaged in digital trade. USTR decided in October 2023 to withdraw its support for strong digital trade rules—proposed earlier by the United States—in the context of negotiations at the World Trade Organization (WTO) for an agreement on e-commerce (known as the Joint Statement Initiative on e-commerce). USTR took a similar, fumbling approach to digital trade in negotiations for the Indo-Pacific Economic Framework's trade pillar, which was aimed at offering the region an alternative to China's growing economic influence. Rather than secure strong digital provisions that aligned with many framework partners' aspirations, the U.S. paused discussions in this space, abandoning policies that large, bipartisan majorities in Congress had enshrined in U.S. law. This is an unforced error that will have enormous consequences.

These haphazard decisions are being driven by a faction of fringe interests that have long opposed trade and pro-growth policies. They are attempting to hijack sound trade policy by arguing that Congress is tying its hands to regulate in the future, ignoring the fact that Congress has long ensured trade agreements leave appropriate breathing room for future policy considerations. Yet, these fringe groups argue that it's in the U.S. national interest to cut off data flows and allow countries around the world to discriminate against and force leading American companies to turn over intellectual property.

The United States has long opposed such an agenda. Instead, policymakers have supported digital trade because they understood that data flows are critical to businesses of all sizes and across sectors, from autos, agriculture, pharmaceuticals, medical devices, and aerospace to services like energy, finance, IT, and telecommunications. USTR has defended American companies against discrimination and has pushed back on tech transfer. It is not too late to change course. The annexed "Global Digital Policy Declaration" offers widely supported principles to guide this process.

Congress has made clear its understanding that the "U.S. can regulate companies within our borders without giving foreign countries, including our adversaries, the impression that the United States will no longer protect our industries and workers against discrimination."[8] A broad range of stakeholders across the business community and civil society have demonstrated that the current U.S. approach is ill-devised and short-sighted. U.S. allies are looking to the U.S. to return to a position of leadership on digital trade because they know that abandoning such an approach will leave their economies vulnerable to reduced investment and their companies exposed to the same harmful practices that are increasingly targeting American companies.

It is incumbent upon the administration to urgently heed these calls for a return to U.S. leadership.

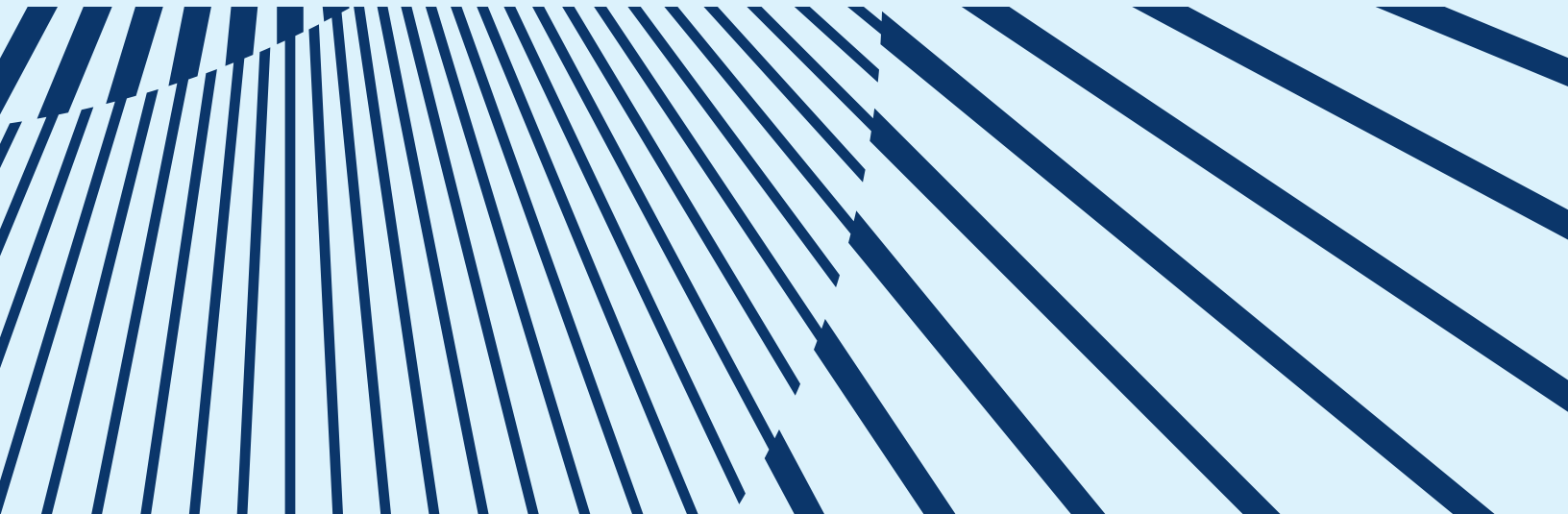
In sum, the United States finds itself at a moment of promise and peril on digital trade. Export opportunities for digitally tradeable services are expanding rapidly, and the United States is well-positioned to build on its formidable advantages in these areas. However, these opportunities are endangered by the spread of digital protectionism and the accumulation of discriminatory digital rules that often target American firms. Failure to address these challenges or recognize the consequences to U.S. companies and workers has compounded the problem.

The United States must change course and resume its position of leadership on digital trade. The case for American leadership on digital trade is strong: It is imperative that the United States push forward a vision for digital trade that secures these opportunities for American workers and consumers—and U.S. companies of all sectors and sizes.

8 Digital Trade Caucus letter to Ambassador Tai, November 16, 2023

Appendix I

# Global Digital Policy Declaration



U.S. Chamber of Commerce

# Global Digital Policy Declaration

**1. Cross-Border Data Flows**

The ability to move data across borders—and access information across borders—is essential to the 21st century economy. No company, regardless of sector, can do business, let alone engage in international trade, without the ability to transfer data. The free flow of data is essential to the creation of global value chains that increase efficiency and permit companies of all sizes to access the global market. The worrisome proliferation of data localization measures around the globe is counterproductive to data protection and poses a threat to economic growth and new market opportunities. To counter the spread of digital trade barriers, policymakers need to commit to support the free flow of data internationally.

**2. Data Protection**

The need to protect data and respect privacy is not in dispute. Privacy protection means different things to different people in different contexts. Prioritizing protection of personal data at the expense of legitimate uses of those data only serves to harm consumers and limit innovation. An optimal regulatory model avoids a one-size-fits-all approach to data protection in favor of a more nuanced approach that recognizes differences among industries in their use of data, enables legitimate business uses of personal data, empowers consumers to make informed choices, and enables cross-border data flows.

**3. Data Governance & Innovation**

Data is central to the digital economy—and so are the laws, regulations, and standards that govern how data is collected and used. Data drives innovation, which in turn promotes economic growth and rising incomes. It is imperative that governments recognize that data is a resource companies create through substantial investments—it is made, not found—and it enhances competition in the marketplace. Governments should refrain from imposing onerous data sharing, access, ownership, and other policies to regulate non-personal data.

**4. Promote Trust and Innovation in Artificial Intelligence**

Artificial intelligence is an important contributor to the global digital economy, and fostering public trust and trustworthiness in AI technologies is necessary to advance its responsible development, deployment, and use. Governments should work together in this rapidly evolving sector and commit to flexible, risk-based frameworks that encourage AI innovation and collaborate across borders to advance sound and interoperable practices. When appropriately regulated, AI has the potential to act as a force for good, tackling challenges and spurring economic growth for the benefit of consumers, businesses, and society.

**5. Foster Sound Regulatory Environments**

Regulation in response to the digital transformation of the economy is a given—industriesrecognize this, and society demands it. However, careful deliberation is essential to well-informed regulatory decisions. New regulations, designed with flexibility to account for new opportunities and challenges, might be necessary as the digital economy develops. However, it is equally possible that existing regulatory frameworks will remain effective in mitigating potential risks or, conversely, hinder

incumbent economic actors, spurring the need for less regulation due to increased competition. In all cases, rulemaking can only be adopted after a deliberative and consultative process governed by good regulatory practices that allow businesses and workers to trade, invest, and innovate with confidence.

**6. Non-Discrimination**

The principle of non-discrimination is foundational to any trade agreement—digital or otherwise Companies from countries with a demonstrated commitment to open markets and nondiscriminatory rules have made greater strides in the creation and development of new digital products than other countries. Companies that have succeeded in bringing outstanding products to market should not be unfairly placed at a competitive disadvantage as punishment for their success; nor should countries whose policy environment fosters such success be subject to discriminatory treatment.

**7. Ban Forced Technology Transfers and Ensure Technology Choice**

Forced localization, local content requirements, and compelling technology transfer as conditions of market access are discriminatory in nature and violate the standards of the global rules-based trading system. These policies deter investment, stifle innovation, and deprive an economy of the transformative benefits of digital products and services. Further, companies should not be forced to transfer their technology—including source code and proprietary algorithms—to competitors or governments. Companies should be able to rely upon technologies they deem optimal for their business operations and not be limited to local and at times less competitive technologies.

**8. Advance Risk-Based Industry Solutions to Cybersecurity**

Cyberattacks undermine trust in an economy that is increasingly reliant on technology. Governments and business agree that international law applies to cyberspace, and applying that law is essential to an open, interoperable, secure, and reliable information and communications infrastructure that supports international commerce, strengthens international security, and fosters free expression and innovation. Governments that view the private sector as a valued partner and engage in deep collaboration across borders are best positioned to safeguard their citizens and their economies. To respond to the fast-changing threat landscape, policies need to focus on flexible, risk-based approaches to cybersecurity that leverage international standards and frameworks, enabling the private sector to develop solutions that address specific cyber needs and scale them across national borders. Encryption is increasingly seen as a valuable tool to enhance privacy and security in the digital ecosystem, and policies need to support it. Encryption policies and procedures should be technology neutral, reasonable, and fully capture views across multiple sectors of the business community.

**9. Abide by Market-Driven International Standards**

Standards are at the heart of digital products and play a growing role in digital services. Far too often, government policies fail to recognize the trade facilitating, self-regulatory attributes of a private-sector market approach to standards development in recognized international standards bodies and consortia. Governments should advance standards policies that support open and competitive markets where companies can compete on the merits. Standards development led by the private sector is the best way to promote common, technically sound approaches that deliver technology solutions and achieve policy objectives. Such standards should be voluntary, open, transparent, globally recognized, consensus-based, and technology-neutral.

# Global Digital Policy Declaration

**10. Prioritize Internet Access, Consumer Choice, and Good Governance**

Governments around the world are making increased investments in digital infrastructure. While more investment is needed, unencumbered access to the Internet and a competitive, interoperable, and inclusive online environment is critical to economic and social development. The Internet is the modern marketplace, and an open Internet allows companies and customers to reach one another on a global scale. Government limitations that restrict barriers to legitimate commerce only serve to constrain the power of the Internet to support sustainable and inclusive economic growth. At the same time, safeguards need to be in place to ensure that online platforms and marketplaces can operate at scale to host a wide range of lawful speech and commerce.

**11. Protect Intellectual Property**

The digital economy is home to creative minds that bring forth amazing products and services. Innovation and creativity drive growth, investment, and competition. In our rapidly evolving digital age, protection for cutting-edge digital products and services is critical. Patents, copyrights, trademarks, and trade secrets (including proprietary algorithms) all play central roles in technological competitiveness, protecting jobs and encouraging growth as businesses of all sizes can engage in trade in digital goods and services. This enables private sector investment in long-term, high-risk, resource intensive projects that advance the state of the art.

**12. Modernize Customs for the Digital Era**

Small business and e-commerce are huge drivers of economic growth and job creation for every economy. Antiquated, burdensome, complex, and costly customs procedures make it difficult for businesses to compete by slowing delivery times and raising transaction costs. Modern approaches to customs that address this problem by raising de minimis thresholds, providing more efficient clearance for low value shipments, and streamlining customs procedures will support supply chains that increase economic competitiveness. Trade agreements should continue to prohibit customs duties on digital products, which is especially useful to small and mid-sized businesses that would not be able to compete on a global scale if they were required to pay those duties.

**13. Improve Trade Facilitation with Digital Technology**

Digital trade is only possible with the advent of paperless trade, interoperable payment systems, and secure authentication methods. Digital trade agreements should embrace paperless trade since it reduces administrative barriers across borders, which maximizes the benefits of trade and foreign investment for all parties. Similarly, countries should work to improve e-invoicing and e-payment systems to ensure that they are interoperable so that the processing of payments remains efficient and reliable. Lastly, parties must agree on standards for electronic signature and authentication methods to protect consumers as well as transactions in the e-marketplace.

**14. Seek Intergovernmental Cooperation and Accountability**

Connectivity is at the heart of the digital economic revolution. This connectivity is a key ingredient in the rising tide of international trade and investment that is boosting incomes and the creation of good jobs. In this context, policy leadership within governments and among governments is essential to securing our shared prosperity. From international forums to bilateral dialogues and trade agreements, governments must make high-standard commitments and agree to be held accountable to them.

# EXHIBIT 21B

# Trade and American Jobs

## The Impact of Trade on U.S. and State-Level Employment:

## 2020 Update

**Prepared by Trade Partnership Worldwide LLC**

**for**

**Business Roundtable**

**October 2020**

# Executive Summary

As the global pandemic took hold around the world at the beginning of 2020, economic growth, global trade, and national employment collapsed. Declines in demand and economic growth are triggering a stall in trade; the stall in trade is boomeranging back to further slow economic growth. This cycle results in lost American jobs that depend on trade. Restoring trade, for example with policies that support the free and fair exchange of goods and services, can help more Americans get back to work and accelerate a U.S. economic recovery.

To spur hiring dependent on trade, it is important to understand first how important trade is to economies and jobs under "normal" circumstances. This report reviews the data of these benefits for U.S. workers *before* the global pandemic took hold. By looking at this relationship prior to the pandemic, one can better appreciate what has been lost and see the importance of adopting trade-enhancing policies that will help American workers, farmers, and families get back on their feet through the pandemic and beyond.

Based on the latest available data for this assessment (2018) and taking into account both the gains and the losses (i.e., a net estimate), trade supported over 40 million U.S. jobs in 2018. One in every five U.S. jobs was linked to exports and imports of goods and services. Two times as many jobs were supported by trade in 2018 as in 1992 – before the accelerated wave of trade liberalization that began with the implementation of the North American Free Trade Agreement (NAFTA) in 1994 – when our earlier research found that trade supported 14.5 million net jobs, or one in every ten U.S. jobs.

- U.S. trade – both exports and imports – has grown over the past two decades, caused in part by trade liberalizing international agreements as well as increasing demand, purchasing power, and growth outside the U.S. This led to the growth of the number of U.S. jobs tied to trade. Indeed, trade-dependent U.S. jobs grew four times as fast as U.S. jobs generally.

- Every U.S. state realized net employment gains directly attributable to trade in 2018.

- Trade had a positive net impact on U.S. jobs in both the services and manufacturing sectors.

- U.S. trade with our North American partners, as well as with Europe, Japan, Korea, China, and India, among others, accounted for important shares of this trade related employment. In 2018, trade with Canada supported, on net, 7.8 million jobs; Mexico, 5.0 million jobs; European Union (27), 6.2 million jobs;

China, 7.7 million jobs; Japan, 2.0 million jobs; and Korea, the UK and India, each over 1 million jobs.

In 2018, tens of millions of American jobs and U.S. economic growth depended on trade. Today, as the United States faces dual public health and economic crises, trade can be a critical driver of job restoration and economic recovery.

# Trade and American Jobs
## The Impact of Trade on U.S. and State-Level Employment: 2020 Update

Laura M. Baughman and Joseph F. Francois*

## I. Introduction

The 2020 Trade and American Jobs report updates a series of path-breaking studies, first issued by Business Roundtable in 2007, that offer a thorough examination of the impacts of trade on U.S. jobs.[1] The report examines the impacts, positive and negative, of both exports *and* imports of goods and services on U.S. employment based on the latest available data (2018). It confirms that trade has a net positive impact on American jobs. Importantly, the positive impact of trade on U.S. employment has grown significantly during the past two decades, coinciding with the liberalization of U.S. trade both multilaterally through the World Trade Organization and bilaterally and regionally through trade agreements.

* Laura M. Baughman is President of Trade Partnership Worldwide, LLC (TPW, www.tradepartnership.com). She holds degrees in economics from Columbia and Georgetown Universities. Dr. Joseph Francois is Managing Director of Trade Partnership Worldwide, LLC, and Professor of Economics, University of Bern, Department of Economics and Managing Director, World Trade Institute. He also holds numerous research fellowships and professorships at think tanks and universities around the world. Dr. Francois formerly was the head of the Office of Economics at the U.S. International Trade Commission, and a research economist at the World Trade Organization. Dr. Francois holds a PhD in economics from the University of Maryland, and economics degrees from the University of Virginia.

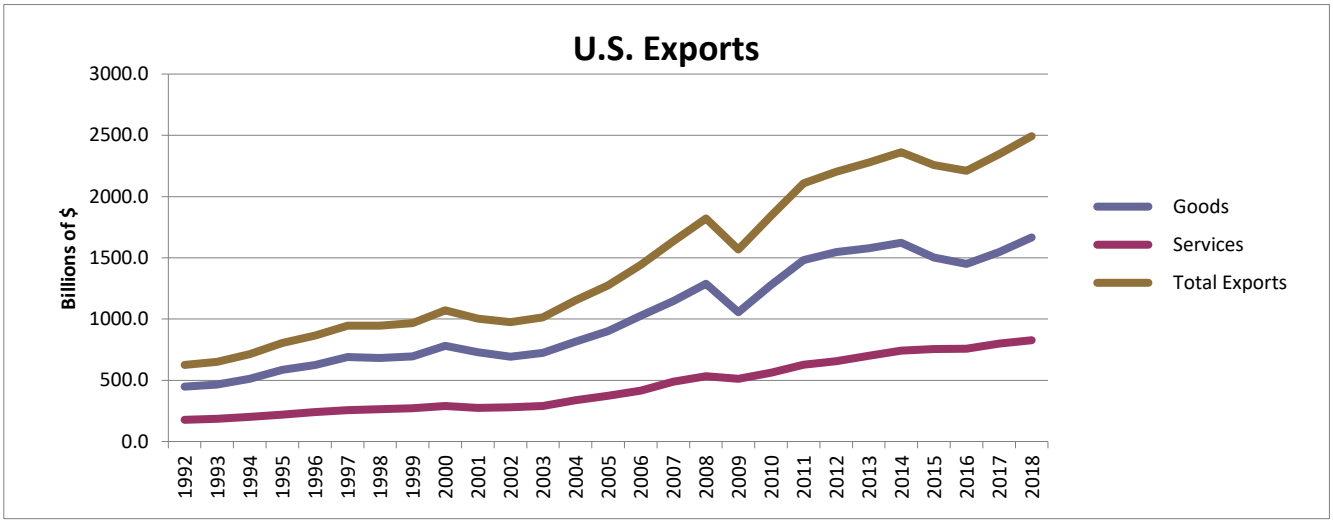
[1] Laura M. Baughman and Joseph Francois, *Trade and American Jobs: The Impact of Trade on U.S. and State-Level Employment*, prepared for the Business Roundtable, February 2007; *Trade and American Jobs: The Impact of Trade on U.S. and State-Level Employment, An Update*, prepared for the Business Roundtable, July, 2010; *How the U.S. Economy Benefits from International Trade and Investment* (2013), prepared for the Business Roundtable; *Trade and American Jobs: The Impact of Trade on U.S. and State-Level Employment, 2014 Update*, prepared for the Business Roundtable, October 2014, *Trade and American Jobs: The Impact of Trade on U.S. and State-Level Employment, 2016 Update*, prepared for the Business Roundtable, January 2016; *Trade and American Jobs: The Impact of Trade on U.S. and State-Level Employment, 2018 Update*, prepared for the Business Roundtable, March 2018, and *Trade and American Jobs: The Impact of Trade on U.S. and State-Level Employment, 2019 Update*, prepared for the Business Roundtable, February 2019.

# II. The Importance of Trade to the United States

Trade remains a vital part of the U.S. economy through the COVID-19 pandemic and will continue to support millions of jobs and economic growth on the other side of the outbreak. Because we are seeking to understand the impacts of trade under "normal" circumstances (i.e., absent the pandemic), we focus on data through 2018 in this report. Since the middle of the 20th century through 2018, U.S. exports and imports grew strongly and by 2018 trade reflected a large share of the nation's economic activity. From 2011-2018, total trade (exports plus imports) represented nearly 30 percent of gross domestic product (GDP), up from 10.6 percent when the General Agreement on Tariffs and Trade — the precursor to the World Trade Organization (WTO) — was launched in 1947.

***Export Trends***

U.S. exports have been generally increasing over the last 25 years. For more than two decades, total U.S. exports have increased at an average *annual* rate of 5.7 percent, notwithstanding the declines experienced during the 2001-2002 and 2008-2009 recessions. Since our last report, services exports have continued to increase and by 2018 accounted for one-third of total U.S. exports. Goods exports (e.g., industrial, agricultural) still dominate total U.S. exports, accounting for just under 70 percent of the total, so their declines in 2015 and 2016 drove the overall decline in U.S. exports in those years. Growth in both goods and services exports rebounded in 2017 and 2018. (Detailed data are provided in Appendix A, Table A1.)




Source: Bureau of Economic Analysis, U.S. Department of Commerce, as detailed in Appendix Table A1.

Leading U.S. goods exports[2] in 2018 included aerospace products and parts; petroleum and coal products; oil and gas; motor vehicles and parts; basic chemicals; pharmaceuticals and medicines; measuring, electro-medical and control instruments; resins, rubber and artificial

[2] Based on four-digit North American Industrial Classification System codes.

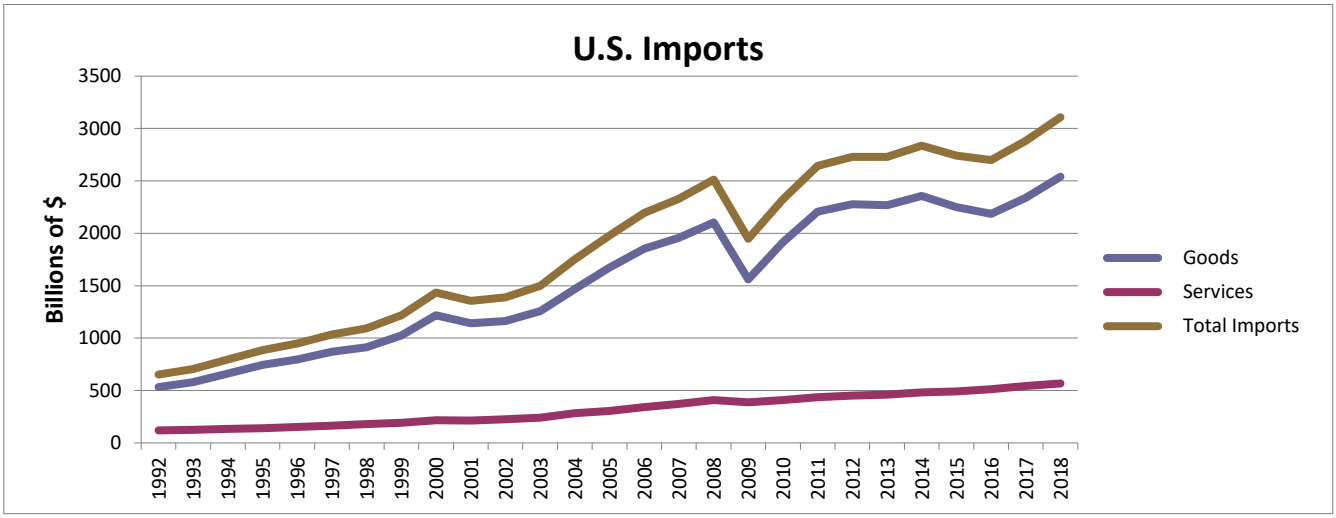
fibers; oilseeds and grains; and semiconductors. These sectors accounted for half of 2018 goods exports.

Contributing to the return to growth in the total value of goods exports from 2016-2018 (up at an average annual rate of 3.4 percent) were surges in exports of oil and gas (up 60.5 percent *per year* over that period), and petroleum and coal (up 11.6 percent per year).

Leading services exports include business; professional and technical services; royalties and license fees; and financial services.

***Import Trends***

U.S. imports also generally increased over the past two decades, spurred by periods of strong economic growth and curtailed by the 2001-2002 and 2008-09 recessions. (Detailed aggregate data are provided in Appendix A, Table A2.) In general, there is a positive correlation between changes in imports and changes in U.S. economic growth. This correlation makes sense given that nearly 60 percent of U.S. merchandise imports are raw materials, capital goods and industrial products used by U.S. manufacturers and farmers to produce goods in the United States. When U.S. manufacturing or agricultural output slows or contracts, producers' and farmers' need for imported raw materials and other inputs declines. Likewise, when household income drops as it does during a recession, families put off buying expensive consumer goods, including consumer goods imports which constitute about 40 percent of total goods imports. The 2016-2018 uptick in the total value of imports was thus owed in part to strong economic growth of the U.S. economy in 2017 and 2018. Increases in 2018 were likely due in part to importers seeking to get goods into the United States before they would be subject to higher tariffs imposed on imports from most foreign steel and aluminum suppliers, as well as products generally from China.




Source: Bureau of Economic Analysis, U.S. Department of Commerce, as detailed in Appendix A, Table A2.

In terms of services, key imports include business, professional, and technical services; travel; and insurance services. These are services purchased by U.S. entities, such as U.S.

companies using foreign legal services, or U.S. tourists traveling abroad.

***"Openness" of the U.S. Economy to Trade***

Trade agreements have been an important contributor to the growth in trade, particularly during the past two decades. They have increasingly reduced foreign barriers to trade, opening new markets for U.S. exports, while also opening the U.S. market to increased imports from other countries reducing costs of inputs for manufacturers and reducing prices for consumers and families.

- Significant global liberalization began between the United States and members of the WTO as the Uruguay Round was implemented in 1995.

- China joined the WTO in December 2001, starting the process of opening its market to U.S. exports of goods and services. A recent assessment of trade with China by the Federal Reserve Bank of St. Louis depicts the growing importance of U.S. exports of key products to China since 2001.[3] Further removing barriers to trade and investment in China would open additional opportunities for U.S. exporters and businesses.

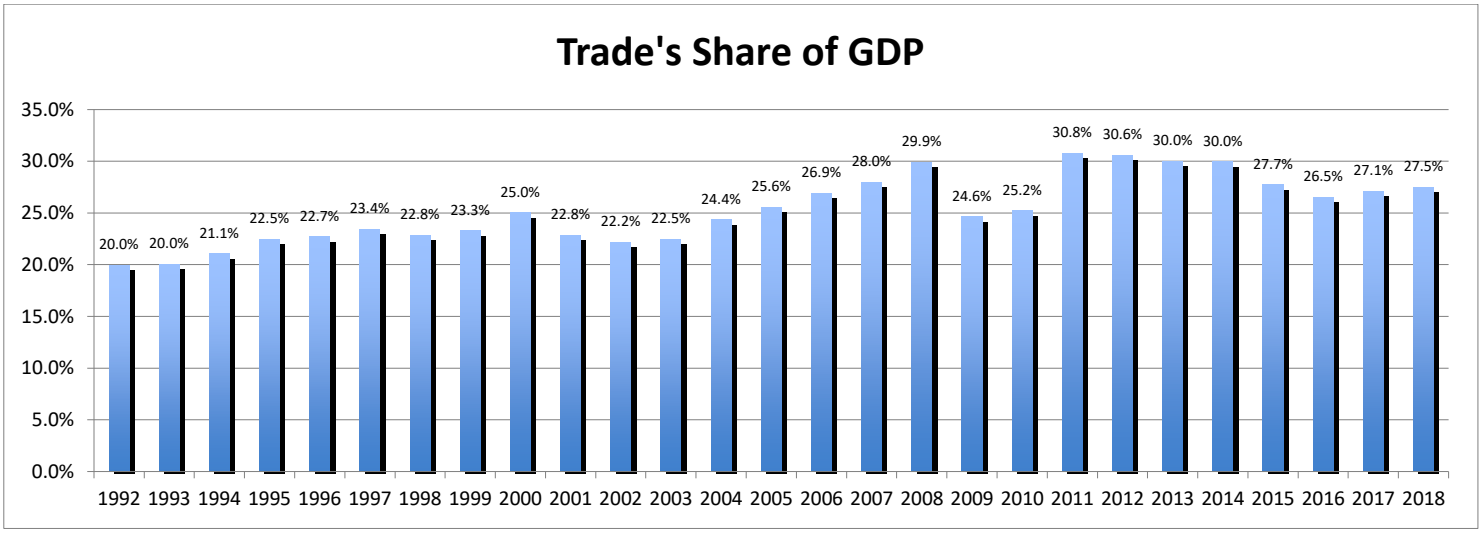

- FTAs were implemented with Mexico and Canada (NAFTA 1993), Jordan (2001), Chile and Singapore (2004), Australia (2005), Morocco (2006), Central America (2006- 2009), Bahrain (2006), Oman (2009), Peru (2009), and South Korea, Colombia and Panama (2012). Each of these agreements helped to increase total

[3] Subhayu Bandyopadhyay, Asha Bharadwaj and Suryadipta Roy, "Taking a Closer Look at U.S. Exports to China," *Regional Economist*, Federal Reserve Bank of St. Louis, September 12, 2018, https://www.stlouisfed.org/publications/regional-economist/third-quarter-2018/closer-look-exports-china.

U.S. trade, including both exports and imports. The share of total U.S. goods and services exports with bilateral or regional trade agreement partners has increased from less than 1 percent in 1992 (when the United States had just two FTA partners, Israel and Canada), to 39 percent in 2018 (when the United States had 20 FTA partners).

As U.S. manufacturers, farmers and services providers have taken advantage of the tariff and other benefits of trade agreements, the importance of global value chains to U.S. companies, farmers and their workers has increased. Companies have lowered costs through these value chains, becoming more competitive in U.S. and foreign markets and relying more than ever on suppliers in other countries for inputs to U.S. production to improve U.S. competitiveness selling goods and services at home and around the world.

Consequently, the importance of trade – both exports *and* imports – to the U.S. economy has increased significantly during the last two decades. During this period of accelerating trade liberalization, total trade (exports plus imports) rose from 20 percent of GDP in 1992 to 28 percent in 2018 (see Appendix A, Table A3 for detailed data).




Source: Derived from Bureau of Economic Analysis, U.S. Department of Commerce.

Studies have also demonstrated the correlation between growth in trade and growth of economies. They find that trade is a factor in driving economic growth.[4] Countries with higher rates of GDP growth also have higher rates of growth in trade as a share of output (e.g., the Chart above). Economic growth is supported by trade when competition with foreign firms spurs domestic firms to innovate and become more productive; when firms seek to operate on a large scale (to supply not only domestic customers but foreign as well) so they are able to lower their costs per unit produced, for example.

[4] For a summary see Esteban Ortiz-Ospina, "Does Trade Cause Growth?," October 22, 2018, https://ourworldindata.org/trade-and-econ-growth.

# III. Trade and American Jobs

Concerns about the impact of trade on U.S. jobs remain widespread in America. Some policymakers are convinced that U.S. goods trade deficits equate to lost U.S. jobs. It is generally accepted that exports have a positive impact on U.S. jobs. However, many worry that imports have a negative impact on U.S. jobs.

A proper assessment of the impacts of trade on U.S. jobs should use an approach that captures the full range of the many ways in which those impacts are experienced by farmers, manufacturers, services providers, workers and consumers. This study uses such an approach, which is detailed in Appendix B. Briefly stated, it explores the direct and indirect effects of exports, the direct and indirect effects of imports, and the effects of additional trade-induced spending on U.S. output and consumption and, consequently, jobs. It reflects the differences in price, quantity and quality between imported goods and U.S.-produced goods. It also captures the jobs directly and indirectly related to the process of importing goods and services into the United States (e.g., jobs associated with transporting imports from the ports to warehouses, jobs at the warehouses, or retail jobs that sell the imported goods if they are finished consumer products). Finally, our methodology also considers the positive and negative effects of trade on jobs, and results reported are therefore "net" job impacts.

Briefly, the findings of this analysis are as follows:

- In 2018, an estimated 40.6 million net jobs were tied to trade.
- These jobs represented 20.2 percent of total employment, or one in five jobs.
- Employment related to trade has increased at four times the rate of employment overall. Between 1992 and 2018, trade-dependent jobs increased by 180 percent (from a net of 14.5 million[5] to 40.6 million), compared to 45 percent for employment generally.[6]
- Nearly two times as many jobs were supported by trade in 2018 (20.2 percent) as in 1992 (10.4 percent) – before the accelerated wave of trade liberalization that began with the implementation of NAFTA in 1994.[7]
- Trade has a net positive impact on U.S. jobs in both the services and manufacturing sectors.

---

[5] Baughman and Francois (2007), *op cit*.

[6] Derived from U.S. Bureau of Economic Analysis, "Total full-time and part-time employment by industry," (accessed September 14, 2020).

[7] Baughman and Francois (2007), *op cit*., Table 6, p. 12.

**Table 1**
**Net Number of U.S. Jobs Related to Trade,* 2018**
**(Thousands)**

| | |
|---|---|
| **Total** | **+40,620.1** |
| | |
| **Good-producing sectors** | **+3,402.4** |
| Agriculture, forestry, fishing | +647.4 |
| Mining and energy | +260.3 |
| Construction | +1,865.0 |
| Manufacturing | +629.7 |
| | |
| **Services-producing sectors** | **+37,217.7** |
| Utilities | +151.9 |
| Wholesale and retail trade | +9,339.4 |
| Finance | +1,242.2 |
| Insurance | +610.9 |
| Transportation | +1,414.2 |
| Communications | +690.1 |
| Business and professional services | +6,786.4 |
| Personal and recreational services | +2,707.2 |
| Other services (e.g. educ., health, gov't, etc.) | +14,276.3 |
| | |
| **Share of Total U.S. Employment** | **20.2%** |

* "Trade" = exports plus imports of goods and services.
See Appendix Table B.1 for sector descriptions
Source: Authors' estimates.

As noted above, the biggest impacts of trade are the ways in which it increases spending across the U.S. economy. But most analysts seeking to assess the impacts of trade on U.S. jobs stop with the direct and indirect impacts of exports and imports. In doing so, they miss the largest source of job-creating activity that comes from trade: the extra spending power companies, workers and consumers have in their bank accounts, spending power that generates still more job-supporting economic activity. Additional spending power comes from, for example, wages of direct and indirect workers in export-related jobs, from wages of direct and indirect workers in import-related jobs, and from consumers who take advantage of lower prices for goods and services resulting from imports, which in turn supports still more economic activity that supports even more jobs. The extra income is spent on other goods and services that are not traded internationally – like dinners out, pre-school or day care for one's child, or a home renovation project. Thus, Table 1 reports large trade-related jobs in sectors like "Construction" and "Personal and recreation services." The estimates in Table 1 reflect the increased spending that goes on throughout the economy as a result of higher incomes and lower costs due to trade. The methodology

in the report captures all these effects.[8]

It is worth noting that the bulk of the jobs associated with U.S. trade are in these other sectors not commonly thought to benefit from trade. And it is these sectors that have been hardest hit from the pandemic-triggered shut down in the U.S. economy that began in earnest in March 2019. Thus, as the economy recovers, trade begins to rebound, and employers in these sectors restart their operations, trade-induced consumer spending will be more important than ever to supporting their operations and their ability to keep workers employed.

***U.S. Jobs Related to Trade with Selected Trading Partners***

Table 2 and the chart detail jobs supported by trade with selected leading U.S. trading partners. Trade with Canada and Mexico together supported nearly 13 million jobs in 2018, 31 percent of all trade-related jobs. Trade with China supports a *net positive* number of U.S. jobs, over 7 million, accounting for an additional 19 percent of total U.S. trade-related jobs and 3.8 percent of all U.S. jobs. Trade with Japan, Korea, the EU (27), UK and India also add importantly to net U.S. employment rolls. Together, trade with these partners accounted for half of all U.S. trade-related jobs in 2018.

**Table 2**
**Net Number of U.S. Jobs Related to Trade with Leading U.S. Trading Partners,* 2018**
**(Thousands)**

| | Canada | Mexico | China | Japan |
|---|---|---|---|---|
| Total | +7,848.0 | +4,961.1 | +7,698.6 | +1,978.8 |
| Good-producing | +545.7 | +447.0 | +621.4 | +140.1 |
| Of which, Manufacturing | +376.1 | +147.4 | -318.6 | -124.3 |
| Services- | +7,302.3 | +4,514.1 | +7,077.2 | +1,838.6 |
| Share of Total U.S. Jobs | 3.9% | 2.5% | 3.8% | 1.0% |
| Share of Trade-Related Jobs | 19.3% | 12.2% | 19.0% | 4.9% |

| | Korea | EU (27) | UK | India |
|---|---|---|---|---|
| Total | +1,094.1 | +6,217.8 | +1,148.6 | +1,612.4 |
| Good-producing | +77.8 | +572.3 | +165.3 | +119.9 |
| Of which, Manufacturing | -27.7 | +45.1 | +14.6 | +70.2 |
| Services | +1,016.3 | +5,645.5 | +983.4 | +1,492.5 |
| Share of Total U.S. Jobs | 0.5% | 3.1% | 0.6% | 0.8% |
| Share of Trade-Related Jobs | 2.7% | 15.3% | 2.8% | 4.0% |

* "Trade"= exports plus imports of goods and services.
Source: Authors' estimates.

[8] Our methodology does not capture the number of jobs supported by foreign investments in the United States, and therefore our results **likely understate** the number of U.S. jobs tied to the international economy. We do capture the jobs at U.S. subsidiaries of foreign firms that are linked to trade (exports and/or imports). We do not capture jobs at foreign companies not engaged directly or indirectly in foreign trade.

Source: Author's estimates.

***State-Level Trade-Related Employment***

As demonstrated by a breakdown of the national employment estimates by state (see Table 3), every U.S. state realizes a net positive impact from trade. Not surprisingly, the largest states benefit the most.

See Appendix B for an explanation of our methodology for breaking down trade-related employment by state. As noted there, these estimates report the state-level jobs linked to *national* exports and imports.

Appendix C presents our employment results by state for each of the leading U.S. trading partners detailed in Table 2.

**Table 3**
**Net Number of U.S. Jobs Related to Total Trade, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +534.6 | Montana | +143.4 |
| Alaska | +101.9 | Nebraska | +270.7 |
| Arizona | +783.5 | Nevada | +376.7 |
| Arkansas | +335.2 | New Hampshire | +175.3 |
| California | +4,874.3 | New Jersey | +1,135.9 |
| Colorado | +788.9 | New Mexico | +237.0 |
| Connecticut | +473.1 | New York | +2,649.5 |
| Delaware | +123.4 | North Carolina | +1,216.6 |
| District of Columbia | +205.2 | North Dakota | +120.3 |
| Florida | +2,563.4 | Ohio | +1,396.9 |
| Georgia | +1,269.0 | Oklahoma | +475.3 |
| Hawaii | +200.9 | Oregon | +513.4 |
| Idaho | +208.9 | Pennsylvania | +1,577.9 |
| Illinois | +1,591.2 | Rhode Island | +133.3 |
| Indiana | +746.7 | South Carolina | +568.9 |
| Iowa | +412.8 | South Dakota | +124.5 |
| Kansas | +395.5 | Tennessee | +816.2 |
| Kentucky | +504.2 | Texas | +3,539.6 |
| Louisiana | +570.5 | Utah | +410.9 |
| Maine | +176.1 | Vermont | +91.0 |
| Maryland | +788.5 | Virginia | +1,107.9 |
| Massachusetts | +994.4 | Washington | +940.8 |
| Michigan | +1,105.4 | West Virginia | +190.0 |
| Minnesota | +755.9 | Wisconsin | +726.5 |
| Mississippi | +326.2 | Wyoming | +84.6 |
| Missouri | +767.2 | TOTAL | +40,620.1 |

Source: Authors' estimates.

# IV Conclusion

Our analysis demonstrates that trade supports American jobs and the U.S. economy. As the U.S. economy has become more open and both exports and imports have grown, so too have U.S. jobs dependent on trade. To meet the public health and economic challenges from COVID-19, trade and effective trade policy can restore many trade-related American jobs and accelerate economic recovery.

Thus, policymakers and others seeking to create new jobs for unemployed Americans should focus on harnessing the opportunities afforded by trade policies, negotiations and programs that increase America's participation in the international marketplace. Trade in 2018 supported over 40 million American jobs and strengthened U.S. economic competitiveness and purchasing power for American families. In 2020 and beyond, trade can support millions more American jobs and position the U.S. economic for a strong recovery and enhance U.S. competitiveness.

# Appendix A

***Trade Data***

**Table A1**
**U.S. Exports to the World, 1992-2018**
**(Billions)**

| | Goods Exports | Services Exports | Total Exports |
|---|---|---|---|
| 1992 | $448.2 | $177.3 | $625.5 |
| 1993 | 465.1 | 185.9 | 651.0 |
| 1994 | 512.6 | 200.4 | 713.0 |
| 1995 | 584.7 | 219.2 | 803.9 |
| 1996 | 625.1 | 239.5 | 864.6 |
| 1997 | 689.2 | 256.1 | 945.3 |
| 1998 | 682.1 | 262.8 | 944.9 |
| 1999 | 695.8 | 271.3 | 967.1 |
| 2000 | 781.9 | 290.4 | 1,072.3 |
| 2001 | 729.1 | 274.3 | 1,003.4 |
| 2002 | 693.1 | 280.7 | 973.8 |
| 2003 | 724.8 | 290.0 | 1,014.7 |
| 2004 | 814.9 | 338.0 | 1,152.8 |
| 2005 | 901.1 | 373.0 | 1,274.1 |
| 2006 | 1,026.0 | 416.7 | 1,442.7 |
| 2007 | 1,148.2 | 488.4 | 1,636.6 |
| 2008 | 1,287.4 | 532.8 | 1,820.2 |
| 2009 | 1,056.0 | 512.7 | 1,568.7 |
| 2010 | 1,278.5 | 562.8 | 1,841.3 |
| 2011 | 1,482.5 | 627.0 | 2,109.5 |
| 2012 | 1,545.7 | 655.7 | 2,201.4 |
| 2013 | 1,578.4 | 700.5 | 2,278.9 |
| 2014 | 1,621.9 | 741.1 | 2,363.0 |
| 2015 | 1,503.1 | 755.3 | 2,258.4 |
| 2016 | 1,451.0 | 758.4 | 2,209.9 |
| 2017 | 1,546.5 | 799.0 | 2,345.5 |
| 2018 | 1,666.0 | 827.0 | 2,538.0 |

Source: U.S. Department of Commerce, Bureau of Economic Analysis, using "Census basis" trade data for goods.

**Table A2**
**U.S. Imports from the World, 1992-2018**
**(Billions)**

| | Goods Imports | Services Imports | Total Imports |
|---|---|---|---|
| 1992 | $532.7 | $119.6 | $652.3 |
| 1993 | 580.7 | 123.8 | 704.4 |
| 1994 | 663.3 | 133.1 | 796.3 |
| 1995 | 743.5 | 141.4 | 884.9 |
| 1996 | 795.3 | 152.6 | 947.8 |
| 1997 | 869.7 | 165.9 | 1,035.6 |
| 1998 | 911.9 | 180.7 | 1,092.6 |
| 1999 | 1,024.6 | 192.9 | 1,217.5 |
| 2000 | 1,218.0 | 216.1 | 1,434.1 |
| 2001 | 1,141.0 | 213.5 | 1,354.5 |
| 2002 | 1,161.4 | 224.4 | 1,385.7 |
| 2003 | 1,257.1 | 242.2 | 1,499.3 |
| 2004 | 1,469.7 | 283.1 | 1,752.8 |
| 2005 | 1,673.5 | 304.4 | 1,977.9 |
| 2006 | 1,853.9 | 341.2 | 2,195.1 |
| 2007 | 1,957.0 | 372.6 | 2,329.5 |
| 2008 | 2,103.6 | 409.1 | 2,512.7 |
| 2009 | 1,559.6 | 386.8 | 1,946.4 |
| 2010 | 1,913.9 | 409.3 | 2,323.2 |
| 2011 | 2,208.0 | 435.8 | 2,643.7 |
| 2012 | 2,276.3 | 452.0 | 2,728.3 |
| 2013 | 2,268.0 | 461.1 | 2,729.1 |
| 2014 | 2,356.4 | 480.8 | 2,837.2 |
| 2015 | 2,248.8 | 492.0 | 2,740.8 |
| 2016 | 2,186.8 | 511.6 | 2,698.4 |
| 2017 | 2,339.9 | 543.9 | 2,883.7 |
| 2018 | 2,540.8 | 567.3 | 3,108.1 |

Source: U.S. Department of Commerce, Bureau of Economic Analysis, using “Census basis” data for goods.

**Table A3**
**"Openness" of U.S. Economy, 1992-2018**
**(Billions and Percent)**

| | Total U.S. Trade* | Total Trade's Share of U.S.GDP |
|---|---|---|
| 1992 | $1,300.9 | 20.0% |
| 1993 | 1,374.8 | 20.0 |
| 1994 | 1,534.3 | 21.1 |
| 1995 | 1,715.4 | 22.5 |
| 1996 | 1,831.7 | 22.7 |
| 1997 | 2,009.6 | 23.4 |
| 1998 | 2,068.7 | 22.8 |
| 1999 | 2,241.4 | 23.3 |
| 2000 | 2,567.6 | 25.0 |
| 2001 | 2,417.2 | 22.8 |
| 2002 | 2,422.8 | 22.2 |
| 2003 | 2,575.5 | 22.5 |
| 2004 | 2,974.3 | 24.4 |
| 2005 | 3,331.6 | 25.6 |
| 2006 | 3,716.1 | 26.9 |
| 2007 | 4,040.2 | 28.0 |
| 2008 | 4,397.2 | 29.9 |
| 2009 | 3,560.4 | 24.6 |
| 2010 | 4,206.5 | 25.2 |
| 2011 | 4,785.5 | 30.8 |
| 2012 | 4,951.2 | 30.6 |
| 2013 | 5,037.6 | 30.0 |
| 2014 | 5,251.1 | 30.0 |
| 2015 | 5,053.4 | 27.7 |
| 2016 | 4,960.0 | 26.5 |
| 2017 | 5,288.8 | 27.1 |
| 2018 | 5,658.8 | 27.5 |

* "Total Trade" is goods and services exports plus goods and services imports, using "balance of payments" basis data to coincide with GDP data.
Source: U.S. Department of Commerce, Bureau of the Census, National Income and Product Accounts tables.

# Appendix B

## *Methodology*

We applied a multi-sector multi-country computable general equilibrium (CGE) model of the U.S. economy to estimate the impacts of trade on U.S. employment. CGE models use regional and national input-output, employment and trade data to link industries in a value-added chain from primary goods to intermediate processing to the final assembly of goods and services for consumption. Inter-sectoral linkages may be direct, like the input of steel in the production of transport equipment, or indirect, via intermediate use in other sectors (e.g., energy used to make steel that is used in turn in the transport equipment sector). Our CGE model captures these linkages by incorporating firms' use of direct and intermediate inputs. The most important aspects of the model can be summarized as follows: (i) it covers all world trade and production; and (ii) it includes intermediate linkages between sectors within each country.

### *The Model*

The specific model used was the Global Trade Analysis Project (GTAP) model (see Hertel 2013). The model and its associated data are developed and maintained by a network of researchers and policymakers coordinated by the Center for Global Trade Analysis at the Department of Agricultural Economics at Purdue University. Guidance and base-level support for the model and associated activities are provided by the GTAP Consortium, which includes members from government agencies (e.g., the U.S. Department of Commerce, U.S. Department of Agriculture, U.S. Environmental Protection Agency, and U.S. International Trade Commission, European Commission), international institutions (e.g., the Asian Development Bank, Organization for Economic Cooperation and Development, the World Bank, United Nations and the World Trade Organization), the private sector and academia. Dr. Francois is a member of the Consortium.

The model assumes that capital stocks are fixed at a national level. Firms are assumed to be competitive, and employ capital and labor to produce goods and services subject to constant returns to scale.[9] Products from different regions are assumed to be imperfect substitutes in accordance with the so-called "Armington" assumption. Armington elasticities are taken directly from the GTAP v. 10 database, as are substitution elasticities

[9] Compared to dynamic CGE models and models with alternative market structures, the present assumption of constant returns to scale with a fixed capital stock is closest in approach to older studies based on pure input-output modeling of trade and employment linkages. In the present context, it can be viewed as generating a lower-bound estimate of effects relative to alternative CGE modeling structures.

for value added.[10]

We are interested in the impact of trade on the U.S. and state economies given the U.S. wage structures in 2018 (i.e., given the prevailing wage structure of the labor force in a given year, how many jobs in the U.S. economy and in each state's economy were linked either directly or indirectly to trade?). As such, the model employs a labor market closure (equilibrium conditions) where wages are fixed at prevailing levels, and employment levels are forced to adjust. This provides a model-generated estimate of the U.S. jobs supported, at current wage levels, by the 2017 level of trade.

***Data***

The model incorporates data from a number of sources. Data on production and trade are based on input-output, final demand, and trade data from the GTAP database (see Aguiar, Narayanan & McDougall 2016). These data provide important information on cross-border linkages in industrial production, related to trade in parts and components. For the 2018 simulation, social accounting data are drawn directly from the most recent version of the GTAP dataset, version 10. Trade data (both exports and imports) exclude re-exports.[11] This dataset is benchmarked to 2014 and includes detailed national input-output, trade, and final demand structures for 140 countries across 56 sectors (see Table A-1). We have updated the trade and national accounts data to 2018.

The basic social accounting and trade data are supplemented with data on tariffs and non-tariff barriers from the World Trade Organization's integrated database and from the UNCTAD/World Bank WITS dataset. All tariff information has been concorded to GTAP model sectors within the version 10 database. For the purposes of the modeling exercise, the aggregation of the GTAP database includes 110 regions and 27 sectors.[12]

The GTAP model sectors were concorded to state-level employment data from the Commerce Department's Bureau of Economic Analysis (BEA). This allowed us to map nationwide effects to individual states. It is important to emphasize that we distribute the employment impacts of trade at the national level to employment at the state level. We are therefore reporting state-level employment related to trade nationally. We are not reporting the state level employment impacts of state-level trade. Based on the availability of employment data as well as the size of some of the sectors, we expanded some sectors (e.g., "Finance and Insurance" its "Finance" and "Insurance" components) and collapsed

[10] Technically we work with what is known as a "non-nested" version of the trade demand equation in the GTAP model. As such, in this case the model also corresponds analytically to a recent type of model known as an Eaton-Kortum model. See Bekkers et al (2017) for further technical discussion and derivations.

[11] See https://www.gtap.agecon.purdue.edu/databases/contribute/reexports.asp.

[12] The GTAP database includes relatively more detail in sectors, particularly in agricultural, primary production, and processed foods than we can use here when mapping model results by sector to state employment data by sector. State employment data for most of these sectors are not available.

others (e.g., individual food products into one sector, "Food Products," or individual transportation modes into one sector, "Transportation"). BEA does not disclose state-level employment data for certain sectors for confidentiality reasons. For some of these sectors, we were able to use Moody's Analytics state-level employment estimates to estimate the missing national employment to undisclosed sectors in these states. However, because we mixed employment data from two sources (BEA and Moody's), the sum of the employment effects for the states may not add perfectly to the total for the United States.

For purposes of the modeling exercise here, the 110 countries/regions in the standard GTAP model were placed in eight distinct groupings of trading partners for the purpose of examining the impact of U.S. trade with those countries: Canada, Mexico, China, Japan, Korea, the European Union (excluding the UK), the United Kingdom, India and rest-of-world. We also aggregated the standard GTAP model sectors into those shown in Table B-1.

**Table B1**
**Model Sectors**

| | |
|---|---|
| Primary agriculture | Electronic equipment |
| Forestry | Other machinery |
| Fishing | Other goods |
| Oil/gas, other mining | Construction |
| Processed Foods | Utilities |
| Beverages and tobacco | Air transport |
| Textiles | Water transport |
| Clothing | Other transport |
| Footwear, leather | Trade and distribution (Wholesale, retail, |
| Wood, paper | accommodation and food services) |
| Paper products, publishing | Communications (Information, postal, |
| Petroleum and coal products | delivery services) |
| Chemicals, rubber, plastics | Financial services |
| Primary metals | Insurance |
| Metal products | Business and professional services |
| Mineral products | Personal and recreational services (Arts, |
| Motor vehicles and parts | entertainment, and recreation services) |
| Other transport equipment | Other services (Education, health care, |
| | social assistance, government services) |

***Model-based Simulations***

The simulation conducted with the GTAP model involved imposing changes in U.S. trade, in this instance a hypothetical elimination of all U.S. exports and imports of goods and services by imposing prohibitive duties against goods trade with the United States across

the board, and prohibitive trade costs against services trade with the United States.[13]

Our results tell us how much U.S. and state output and employment would decline were the United States to cease exporting and importing goods and services, tracing changes at the border as they work through the U.S. economy. The net negative (or positive, in some cases) impacts on output and jobs from an absence of trade serve as a proxy for the opposite: the net positive (or negative) impacts on U.S. output and employment *because* of trade. We report the results from this second perspective in this paper.

## References

Aguiar, Angel, Badri Narayanan, & Robert McDougall. "An Overview of the GTAP 9 Data Base." Journal of Global Economic Analysis 1, no. 1 (June 3,2016): 181-208.

Bekkers, E., Francois, J. F. and Rojas-Romagosa, H. (2017), Melting Ice Caps and the Economic Impact of Opening the Northern Sea Route. *Economic Journal*. doi:10.1111/ecoj.12460

Hertel, T. (2013). "Global Applied General Equilibrium Analysis Using the Global Trade Analysis Project Framework," in P. B. Dixon and D. W. Jorgenson eds. *Handbook of Computable General Equilibrium Modeling*. Amsterdam: Elsevier, 815-76.

Reinert, K.A.. and D.W. Roland-Holst (1997), "Social Accounting Matrices," in Francois, J.F. and K.A. Reinert, eds. (1997), *Applied methods for trade policy analysis: a handbook*, Cambridge University Press: New York.

[13] We have modeled an extreme shock to the economy to show the extent to which sectors of the economy are tied to trade. We are not suggesting that a prohibitive tariff is a policy option that has been proposed by anyone. It is useful to understand the job impact of complete elimination of both exports and imports, in order to quantify the opposite scenario: the job impact of actual U.S. trade in the experiment years.

# Appendix C

***Employment Impacts by State and Country***

**Table C1**
**Net Number of U.S. Jobs Related to Trade with Canada, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +102.8 | Montana | +25.7 |
| Alaska | +20.3 | Nebraska | +50.9 |
| Arizona | +152.8 | Nevada | +74.4 |
| Arkansas | +62.5 | New Hampshire | +36.0 |
| California | +966.1 | New Jersey | +226.9 |
| Colorado | +146.8 | New Mexico | +40.4 |
| Connecticut | +92.3 | New York | +520.3 |
| Delaware | +24.2 | North Carolina | +241.4 |
| District of Columbia | +38.3 | North Dakota | +19.0 |
| Florida | +502.6 | Ohio | +274.2 |
| Georgia | +251.0 | Oklahoma | +74.6 |
| Hawaii | +38.5 | Oregon | +100.2 |
| Idaho | +39.4 | Pennsylvania | +305.5 |
| Illinois | +317.4 | Rhode Island | +26.6 |
| Indiana | +148.5 | South Carolina | +112.1 |
| Iowa | +79.0 | South Dakota | +23.1 |
| Kansas | +69.5 | Tennessee | +160.4 |
| Kentucky | +95.0 | Texas | +640.1 |
| Louisiana | +102.9 | Utah | +80.3 |
| Maine | +36.4 | Vermont | +17.3 |
| Maryland | +153.1 | Virginia | +212.1 |
| Massachusetts | +200.8 | Washington | +177.6 |
| Michigan | +220.2 | West Virginia | +32.4 |
| Minnesota | +150.0 | Wisconsin | +144.1 |
| Mississippi | +61.2 | Wyoming | +13.2 |
| Missouri | +147.4 | TOTAL | +7,848.0 |

Source: Authors' estimates.

**Table C2**
**Net Number of U.S. Jobs Related to Trade with Mexico, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +65.6 | Montana | +16.5 |
| Alaska | +9.3 | Nebraska | +31.4 |
| Arizona | +96.5 | Nevada | +46.5 |
| Arkansas | +39.9 | New Hampshire | +21.4 |
| California | +584.1 | New Jersey | +141.6 |
| Colorado | +97.9 | New Mexico | +29.2 |
| Connecticut | +58.6 | New York | +328.0 |
| Delaware | +15.4 | North Carolina | +150.7 |
| District of Columbia | +25.4 | North Dakota | +14.7 |
| Florida | +310.7 | Ohio | +171.1 |
| Georgia | +157.8 | Oklahoma | +60.1 |
| Hawaii | +23.6 | Oregon | +59.0 |
| Idaho | +24.1 | Pennsylvania | +194.9 |
| Illinois | +194.3 | Rhode Island | +16.1 |
| Indiana | +92.1 | South Carolina | +70.9 |
| Iowa | +47.2 | South Dakota | +13.9 |
| Kansas | +48.3 | Tennessee | +99.2 |
| Kentucky | +59.9 | Texas | +466.9 |
| Louisiana | +69.9 | Utah | +51.3 |
| Maine | +18.8 | Vermont | +10.4 |
| Maryland | +97.0 | Virginia | +135.9 |
| Massachusetts | +121.8 | Washington | +110.8 |
| Michigan | +136.6 | West Virginia | +24.3 |
| Minnesota | +91.3 | Wisconsin | +86.2 |
| Mississippi | +39.3 | Wyoming | +10.8 |
| Missouri | +91.8 | TOTAL | +4,961.1 |

Source: Authors' estimates.

**Table C3**
**Net Number of U.S. Jobs Related to Trade with China, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +103.5 | Montana | +28.9 |
| Alaska | +19.1 | Nebraska | +54.5 |
| Arizona | +147.3 | Nevada | +71.5 |
| Arkansas | +65.7 | New Hampshire | +29.4 |
| California | +888.2 | New Jersey | +211.9 |
| Colorado | +151.3 | New Mexico | +46.8 |
| Connecticut | +90.0 | New York | +493.8 |
| Delaware | +23.0 | North Carolina | +222.4 |
| District of Columbia | +38.9 | North Dakota | +25.4 |
| Florida | +491.4 | Ohio | +266.4 |
| Georgia | +241.7 | Oklahoma | +97.6 |
| Hawaii | +39.0 | Oregon | +93.5 |
| Idaho | +40.1 | Pennsylvania | +296.8 |
| Illinois | +266.2 | Rhode Island | +24.2 |
| Indiana | +144.1 | South Carolina | +107.9 |
| Iowa | +80.8 | South Dakota | +25.1 |
| Kansas | +80.6 | Tennessee | +158.8 |
| Kentucky | +102.0 | Texas | +689.4 |
| Louisiana | +112.4 | Utah | +76.7 |
| Maine | +31.2 | Vermont | +16.7 |
| Maryland | +148.4 | Virginia | +213.0 |
| Massachusetts | +176.2 | Washington | +184.9 |
| Michigan | +211.7 | West Virginia | +38.0 |
| Minnesota | +135.6 | Wisconsin | +133.6 |
| Mississippi | +64.0 | Wyoming | +17.4 |
| Missouri | +148.6 | TOTAL | +7,698.6 |

Source: Authors' estimates.

**Table C4**
**Net Number of U.S. Jobs Related to Trade with Japan, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +23.2 | Montana | +8.1 |
| Alaska | +5.3 | Nebraska | +14.7 |
| Arizona | +38.4 | Nevada | +18.4 |
| Arkansas | +17.3 | New Hampshire | +8.1 |
| California | +246.3 | New Jersey | +56.4 |
| Colorado | +41.0 | New Mexico | +13.1 |
| Connecticut | +20.7 | New York | +131.1 |
| Delaware | +6.2 | North Carolina | +58.8 |
| District of Columbia | +10.2 | North Dakota | +7.0 |
| Florida | +128.0 | Ohio | +59.4 |
| Georgia | +61.6 | Oklahoma | +26.1 |
| Hawaii | +10.4 | Oregon | +26.5 |
| Idaho | +11.5 | Pennsylvania | +75.4 |
| Illinois | +75.2 | Rhode Island | +6.2 |
| Indiana | +27.2 | South Carolina | +25.0 |
| Iowa | +21.0 | South Dakota | +6.8 |
| Kansas | +20.0 | Tennessee | +36.5 |
| Kentucky | +22.2 | Texas | +185.1 |
| Louisiana | +29.4 | Utah | +20.4 |
| Maine | +8.7 | Vermont | +4.6 |
| Maryland | +39.4 | Virginia | +54.1 |
| Massachusetts | +48.4 | Washington | +45.2 |
| Michigan | +41.3 | West Virginia | +9.7 |
| Minnesota | +37.8 | Wisconsin | +33.5 |
| Mississippi | +15.7 | Wyoming | +5.0 |
| Missouri | +37.2 | TOTAL | +1,976.8 |

Source: Authors' estimates.

**Table C5**
**Net Number of U.S. Jobs Related to Trade with Korea, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +13.2 | Montana | +4.3 |
| Alaska | +2.7 | Nebraska | +8.2 |
| Arizona | +21.2 | Nevada | +10.1 |
| Arkansas | +9.6 | New Hampshire | +4.4 |
| California | +136.1 | New Jersey | +30.8 |
| Colorado | +21.8 | New Mexico | +6.9 |
| Connecticut | +12.4 | New York | +71.2 |
| Delaware | +3.4 | North Carolina | +32.3 |
| District of Columbia | +5.5 | North Dakota | +3.7 |
| Florida | +69.6 | Ohio | +34.3 |
| Georgia | +34.2 | Oklahoma | +13.9 |
| Hawaii | +5.6 | Oregon | +14.3 |
| Idaho | +6.2 | Pennsylvania | +41.7 |
| Illinois | +42.2 | Rhode Island | +3.5 |
| Indiana | +16.2 | South Carolina | +14.4 |
| Iowa | +12.0 | South Dakota | +3.7 |
| Kansas | +11.7 | Tennessee | +21.0 |
| Kentucky | +13.0 | Texas | +98.7 |
| Louisiana | +15.6 | Utah | +10.9 |
| Maine | +4.8 | Vermont | +2.5 |
| Maryland | +21.2 | Virginia | +30.0 |
| Massachusetts | +26.3 | Washington | +26.5 |
| Michigan | +24.6 | West Virginia | +5.2 |
| Minnesota | +20.8 | Wisconsin | +19.3 |
| Mississippi | +9.0 | Wyoming | +2.6 |
| Missouri | +21.1 | TOTAL | +1,094.1 |

Source: Authors' estimates.

**Table C6**
**Net Number of U.S. Jobs Related to Trade with the EU (27), by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +80.5 | Montana | +22.9 |
| Alaska | +15.6 | Nebraska | +41.1 |
| Arizona | +120.2 | Nevada | +57.4 |
| Arkansas | +51.4 | New Hampshire | +27.4 |
| California | +761.2 | New Jersey | +170.4 |
| Colorado | +124.2 | New Mexico | +38.7 |
| Connecticut | +70.5 | New York | +405.9 |
| Delaware | +18.9 | North Carolina | +185.8 |
| District of Columbia | +32.1 | North Dakota | +19.8 |
| Florida | +390.3 | Ohio | +206.7 |
| Georgia | +190.3 | Oklahoma | +78.7 |
| Hawaii | +31.0 | Oregon | +81.2 |
| Idaho | +33.0 | Pennsylvania | +239.6 |
| Illinois | +236.7 | Rhode Island | +20.2 |
| Indiana | +107.5 | South Carolina | +84.6 |
| Iowa | +62.5 | South Dakota | +19.3 |
| Kansas | +61.2 | Tennessee | +121.3 |
| Kentucky | +75.5 | Texas | +557.3 |
| Louisiana | +88.9 | Utah | +62.6 |
| Maine | +26.8 | Vermont | +14.4 |
| Maryland | +121.2 | Virginia | +169.6 |
| Massachusetts | +152.7 | Washington | +144.1 |
| Michigan | +161.4 | West Virginia | +30.1 |
| Minnesota | +116.3 | Wisconsin | +108.9 |
| Mississippi | +49.6 | Wyoming | +14.1 |
| Missouri | +116.3 | TOTAL | +6,217.8 |

Source: Authors' estimates.

**Table C7**
**Net Number of U.S. Jobs Related to Trade with the UK, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +15.5 | Montana | +4.6 |
| Alaska | +5.8 | Nebraska | +7.5 |
| Arizona | +20.9 | Nevada | +11.1 |
| Arkansas | +10.1 | New Hampshire | +5.2 |
| California | +136.0 | New Jersey | +30.4 |
| Colorado | +22.1 | New Mexico | +7.4 |
| Connecticut | +11.0 | New York | +70.4 |
| Delaware | +3.2 | North Carolina | +34.8 |
| District of Columbia | +5.6 | North Dakota | +3.8 |
| Florida | +70.6 | Ohio | +38.9 |
| Georgia | +34.9 | Oklahoma | +14.8 |
| Hawaii | +6.2 | Oregon | +16.1 |
| Idaho | +6.4 | Pennsylvania | +44.4 |
| Illinois | +43.1 | Rhode Island | +3.9 |
| Indiana | +21.8 | South Carolina | +15.9 |
| Iowa | +11.7 | South Dakota | +3.7 |
| Kansas | +10.5 | Tennessee | +23.0 |
| Kentucky | +14.6 | Texas | +103.2 |
| Louisiana | +18.8 | Utah | +11.3 |
| Maine | +6.9 | Vermont | +2.7 |
| Maryland | +22.4 | Virginia | +30.1 |
| Massachusetts | +28.5 | Washington | +25.7 |
| Michigan | +30.8 | West Virginia | +6.0 |
| Minnesota | +21.6 | Wisconsin | +21.1 |
| Mississippi | +9.8 | Wyoming | +2.9 |
| Missouri | +21.0 | TOTAL | +1,148.6 |

Source: Authors' estimates.

**Table C8**
**Net Number of U.S. Jobs Related to Trade with India, by State, 2018**
**(Thousands)**

| | | | |
|---|---|---|---|
| Alabama | +21.6 | Montana | +5.5 |
| Alaska | +3.8 | Nebraska | +10.7 |
| Arizona | +31.2 | Nevada | +14.9 |
| Arkansas | +13.4 | New Hampshire | +7.2 |
| California | +193.9 | New Jersey | +45.0 |
| Colorado | +30.8 | New Mexico | +9.1 |
| Connecticut | +19.2 | New York | +105.1 |
| Delaware | +4.9 | North Carolina | +48.0 |
| District of Columbia | +7.9 | North Dakota | +4.6 |
| Florida | +100.3 | Ohio | +57.1 |
| Georgia | +49.9 | Oklahoma | +18.1 |
| Hawaii | +7.9 | Oregon | +20.7 |
| Idaho | +8.2 | Pennsylvania | +63.6 |
| Illinois | +64.5 | Rhode Island | +5.3 |
| Indiana | +31.3 | South Carolina | +22.6 |
| Iowa | +16.9 | South Dakota | +5.0 |
| Kansas | +15.6 | Tennessee | +32.6 |
| Kentucky | +20.4 | Texas | +137.0 |
| Louisiana | +21.6 | Utah | +16.2 |
| Maine | +6.9 | Vermont | +3.6 |
| Maryland | +30.7 | Virginia | +43.0 |
| Massachusetts | +39.7 | Washington | +37.0 |
| Michigan | +45.1 | West Virginia | +7.5 |
| Minnesota | +30.9 | Wisconsin | +30.2 |
| Mississippi | +13.0 | Wyoming | +3.2 |
| Missouri | +30.7 | TOTAL | +1,612.4 |

Source: Authors' estimates.

# EXHIBIT 22

# Contents

Introduction 3

Strong growth in US manufacturing, even as talent challenges persist 4

Changing workforce expectations affect hiring and retention 10

Applying customer focus to create a leading workforce experience 13

Taking an ecosystem approach to attract and upskill talent 14

Final thoughts: The road ahead 20

# Introduction

As the industry grows, manufacturers are actively investing in attracting and retaining employees, drawing on innovation and an ecosystem approach to help improve the worker experience.

**Key takeaways from the 2024 *Deloitte and The Manufacturing Institute Talent Study***

**01**

The US manufacturing industry has emerged from the COVID-19 pandemic on a strong growth trajectory and manufacturers studied indicated that, overall, they expect continued growth over the next 10 years as they work to meet evolving customer demands, de-risk their supply chains, and leverage government incentives and policies.

**02**

Deloitte and The Manufacturing Institute found that there could be as many as 3.8 million net new employees needed in manufacturing between 2024 and 2033, and that around half of these jobs (1.9 million) could remain unfilled if the talent conundrum is not solved.

**03**

Higher-level skills will likely be required as manufacturers continue their journey toward Industry 4.0, which could add to the skills gap. But tight labor markets have also created an applicant gap, which has challenged manufacturers' ability to fill roles across all skill levels.

**04**

Manufacturers seem to be commonly applying a "customer focus" to their workforce to help understand worker needs and design innovative solutions to create a better worker experience and improve retention.

**05**

Many manufacturers seem to be investing in partnerships and taking a regional ecosystem approach to build their talent pipeline and attract and upskill the workers that they need.

Source: 2024 Deloitte and The Manufacturing Institute talent study.

**About the 2024 *Deloitte and The Manufacturing Institute Talent Study***

In December 2023, Deloitte and The Manufacturing Institute embarked on their sixth manufacturing talent study in more than two decades (hereafter referred to as the "study"). The study involved an online survey of more than 200 US manufacturers, interviews with more than 10 senior executives from manufacturing organizations of all sizes and across all sectors, and an extensive collation of secondary data on labor supply and demand.

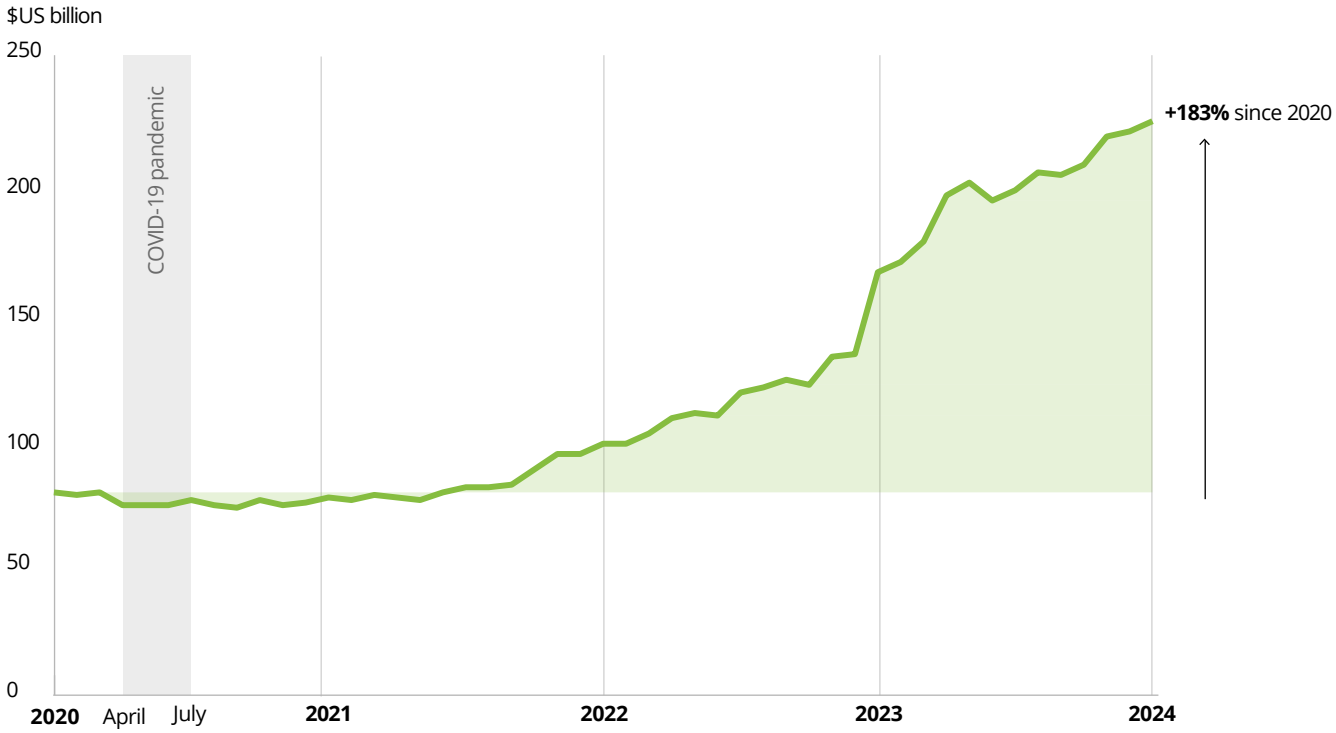
- Supported by Deloitte's economics team, the study conducted proprietary analysis on labor supply and demand data to explore the potential impact of unfilled jobs on the nation's economy.
- The study also includes extensive analysis of data comprising manufacturing job descriptions and analysis of growth trends.
- Research included a targeted analysis of over 80 manufacturing companies' annual reports and investor presentations.

# Strong growth in US manufacturing, even as talent challenges persist

The US manufacturing industry is experiencing strong growth. Manufacturing employment has surpassed pre-pandemic levels and stands close to 13 million as of January 2024.[1] The number of manufacturing establishments in the United States grew by more than 11% between the first quarter of 2019 and the second quarter of 2023, approaching 393,000 by the end of the period.[2] Construction spending in manufacturing—that is, dollars invested to build new or expand existing manufacturing facilities—has nearly tripled since June 2020 and was up 37% year over year in January 2024 when it reached a record high of US$225 billion (figure 1). Even as average lead times have declined since the pandemic,[3] the desire to de-risk supply chains and establish facilities closer to US customers has continued to drive investment from domestic and foreign manufacturers.[4]

Legislation and policy have also played a role. Deloitte analysis of government data as of September 2023 indicates that nearly 300 new clean technology and semiconductor and electronics manufacturing facilities have been announced and are planned for completion by 2031,[5] spurred in part by the Infrastructure Investment and Jobs Act (IIJA), the Inflation Reduction Act (IRA), and the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act. These projects represent over US$430 billion invested and include announcements of more than 234,000 new manufacturing jobs to be created.[6] The US Department of Defense launched its National Defense Industrial Strategy in January 2024 to guide investment and support the development of a modern and innovative defense industrial ecosystem. The overarching goals are to improve supply chain resiliency, enhance acquisition flexibility, develop the requisite workforce, and elevate the technological preparedness of the defense industrial base over the next three to five years.[7] These combined efforts seem to signal a positive outlook for the manufacturing sector, with potential implications for innovation, supply base expansion, job creation, and overall industry resilience in the United States.

**Figure 1. Total construction spending in manufacturing has grown significantly in recent years**




Source: Deloitte analysis of data from US Census Bureau.

### Workforce issues remain a leading concern for manufacturers: A skills gap and an applicant gap

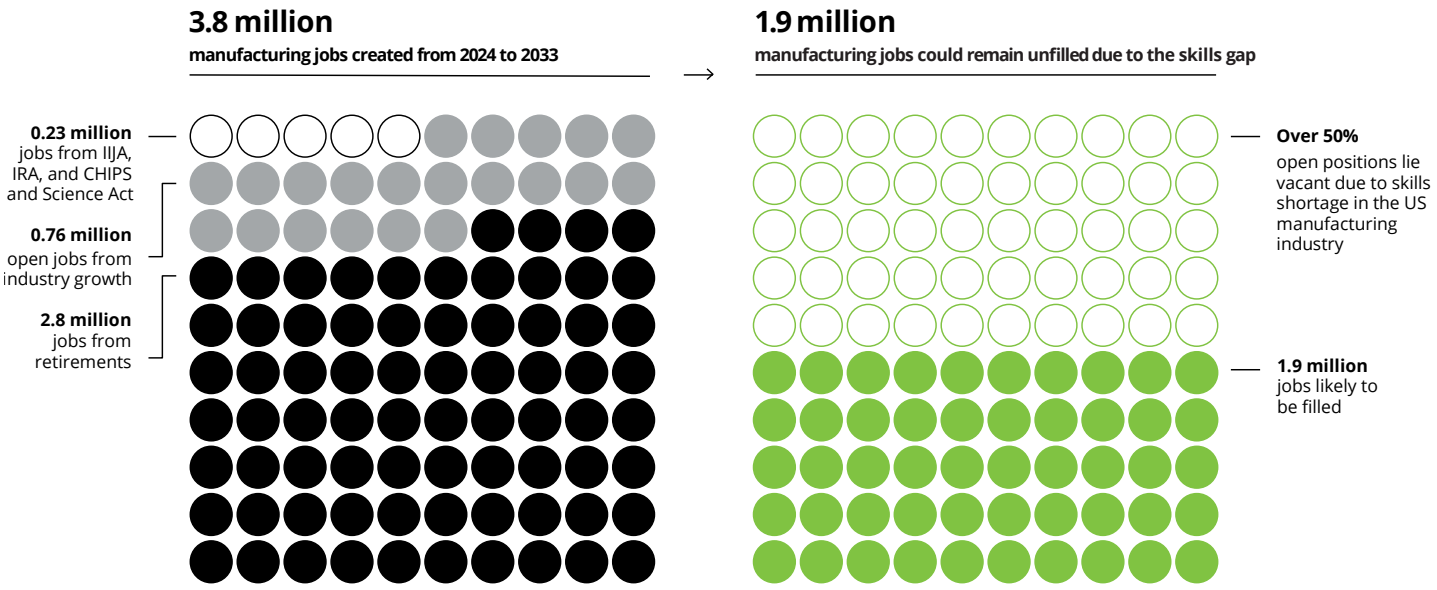
Alongside this potential growth, the 2024 *Deloitte and MI Talent Study* identified another trend: There is not just a skills gap, but notably a gap in applicants for open positions in manufacturing. Three important themes, in particular, stood out in the study:

1. Industry growth is driving the need for more workers of every type—from entry-level associates to skilled production workers to engineers.
2. Skill requirements are evolving and are spread between technical manufacturing skills, digital skills, and soft skills.
3. There is a shortage of potential candidates applying for positions—whether skilled or unskilled—and manufacturers need to retain the valuable talent they have.

Attracting and retaining talent is the primary business challenge indicated by over 65% of respondents in the National Association of Manufacturers' (NAM) outlook survey for the first quarter of 2024.[8] Workforce challenges have also been the top concern for manufacturers surveyed by NAM since the fourth quarter of 2017, with the exception of the pandemic.[9] This timing coincides with the first instance when total job openings in the United States exceeded the number of unemployed Americans.[10] This phenomenon is partly due to longer-term economic factors, such as the declining population growth rate and the decreasing labor force participation rate, which has trended lower on demographic factors, including increased retirements.[11] In addition, even though December 2023 quit-rate data suggests some improvement as they approach pre-pandemic levels, employee turnover rates remain elevated,[12] posing a challenge for manufacturers. This could be partly attributable to the increased caretaking responsibilities many Americans of working age are facing since the pandemic,[13] and also to the higher numbers of millennials and Generation Z workers joining the workforce,[14] who bring a different set of expectations.[15]

Even with some recent cooling, the labor market remains tight, and the resulting applicant gap may continue. This could impact the ability of manufacturers to fully capitalize on this recent growth in public and private investment. **The net need for new employees in manufacturing could be around 3.8 million between 2024 and 2033. And, around half of these open jobs (1.9 million) could remain unfilled if manufacturers are not able to address the skills gap and the applicant gap[16]** (figure 2).

**Figure 2. An estimated 1.9 million open positions may prove difficult to fill by 2033**




Source: Deloitte analysis of data from US Bureau of Labor Statistics and estimates of private investments from Invest.gov.

## Evolving skill requirements complicate the search for talent

This potential growth in the manufacturing sector appears to be creating demand for more employees across the board, even amid a historically tight labor market.[17] Moreover, the growth in construction jobs fostered by policy incentives may intensify competition for welders, electricians, and other trades, which could exacerbate the imbalance in labor supply and demand in manufacturing. Further complicating the picture is the evolving landscape of skill requirements and the rearchitecting of roles that is likely to be required as manufacturers continue their journey toward the smart factory and Industry 4.0.

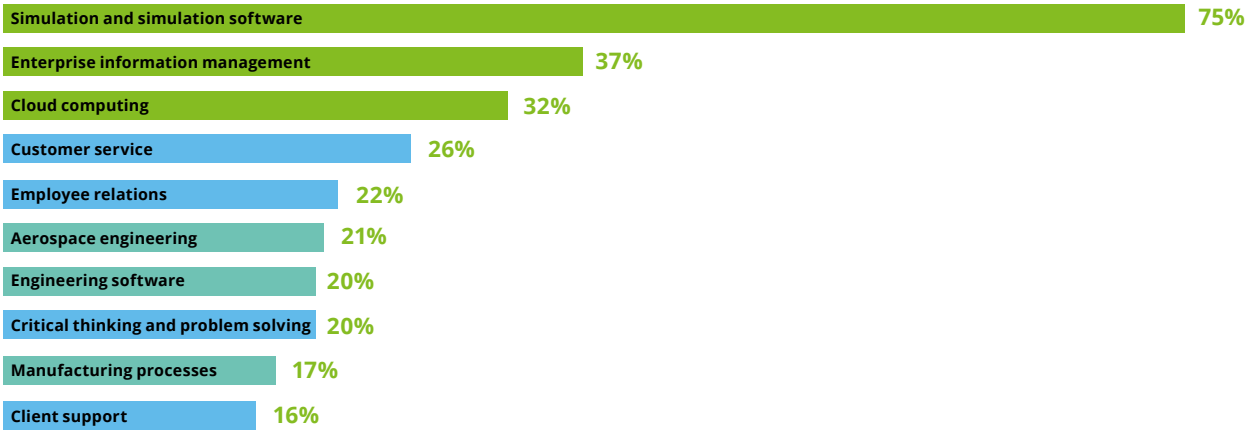
### *Evolving skill sets in manufacturing*

The World Economic Forum's 2023 *Future of Jobs* report highlights that 40% of the current skill requirements in advanced manufacturing will evolve over the next five years.[18] Manufacturers are prioritizing the development of these top three skills over the next five years: leadership skills, digital skills, and soft skills.[19]

To better understand the growing breadth of evolving skills that manufacturers are seeking, we analyzed the past five years of job posting data.[20] The research found a 75% increase in demand for simulation and simulation software skills, sought mostly for technology-enabled production or testing roles (figure 3).

**Figure 3. A combination of digital skills, soft skills, and high-level technical skills show the fastest compound annual growth rates in manufacturing between 2019 and 2023**

*Compound annual growth rates of fastest growing major skill categories*




*Examples of specific skills listed under each major skill category*

| Simulation and simulation software | Enterprise information management | Cloud computing | Customer service | Employee relations |
|---|---|---|---|---|
| Computer simulation | Corporate data management | Cloud administration | Customer engagement | Diversity programs |
| Digital twin | Enterprise content management | Cloud application development | Customer experience strategy | Employee engagement |
| Dynamic simulation | Information governance | Cloud engineering | Customer experience improvement | Employee satisfaction |
| Real-time 3D | Knowledge management | Cloud security | Rapport building | Employer brand marketing |
| Virtual prototyping | | | Customer relationship building | Cultural assimilation |

| Aerospace engineering | Engineering software | Critical thinking and problem solving | Manufacturing processes | Client support |
|---|---|---|---|---|
| Aerodynamics | CAD programs | Analytical skills | Additive manufacturing | Aftersales |
| Aerostructure | Civil engineering software | Analytical thinking | 3D printing | Client services |
| Aircraft design | Plant design systems | Brainstorming | Machining | Customer empowerment |
| Aircraft electronics | | Change agility | Manufacturing execution systems | Customer success management |
| Flight control systems | | Creative and complex problem-solving | Smart factory | Product support |
| | | Innovation | Process specification | Service quality management |
| | | Logical reasoning | | |
| | | Strategic thinking | | |

Source: Deloitte analysis of data from Lightcast database. Digital skills Soft skills High-level technical skills

Customer service and client support skills showed significant upticks in demand as well, and this trend is likely to continue as manufacturers increase digital interactions with customers and expand their aftermarket services. The growing focus on employee relations skills has likely resulted from manufacturers' efforts to develop a worker-friendly environment and a dedication to hiring from more diverse talent pools.[21] Manufacturing-specific skills, including those related to advanced processes like 3D printing, as well as cloud-based enterprise resource planning (ERP) solutions, have also experienced gains. The growth in demand for soft skills like critical thinking, problem-solving, and creativity tend to underpin many of the other skills that have shown the greatest gains, like customer service, simulation, and manufacturing processes.

**Digital skills are important according to surveyed manufacturers, but soft skills are a necessary complement**

One out of two respondents in our study indicated that it is "important" or "very important" for employees to have a high level of digital proficiency. Another 40% see it as "good to have," primarily for engineers and engineering technicians, operations personnel, and maintenance technicians. Manufacturers are integrating technologies such as computer numerical control, programmable logic controllers, sensors, advanced robotics, 3D printing, and others with artificial intelligence across functions.[22] This integration underscores the importance of having a digitally savvy workforce with skills such as machine learning, cybersecurity, data management, and data analysis. Meanwhile, network security and the ability to work with modern ERP systems and interconnected machines are increasingly becoming important.[23] Additionally, smart factory solutions are on the rise, requiring digital skills to design, implement, and operate.

The increased adoption of digital tools and technologies tends to bring soft skills such as adaptability, problem-solving, critical and cross-functional thinking, initiative and leadership to the fore. For example, critical-thinking skills are important to evaluate the outputs from AI tools, including generative AI, and to process data mined from interconnected machines. However, digital and soft skills alone are generally not enough—for employees to successfully apply these skills, it tends to be important to have a strong foundation in the fundamentals of manufacturing, especially in highly specialized sectors such as fabricated metal product manufacturing, and aerospace and defense. For example, to learn how to effectively operate welding robots, it can be helpful—and often necessary—for a worker to have welding experience in a manufacturing environment.

### *More manufacturing workers are likely to be needed for higher-skill roles*

According to occupation data from the US Bureau of Labor Statistics (BLS), some of the fastest growing manufacturing occupations projected until 2032[24] tend to be well-aligned with the skills in highest demand over the last five years. As operations and products become more complex and manufacturers look to integrate the information collected from their smart connected devices, equipment, and systems, highly skilled roles could grow the fastest between 2022 and 2032.[25]

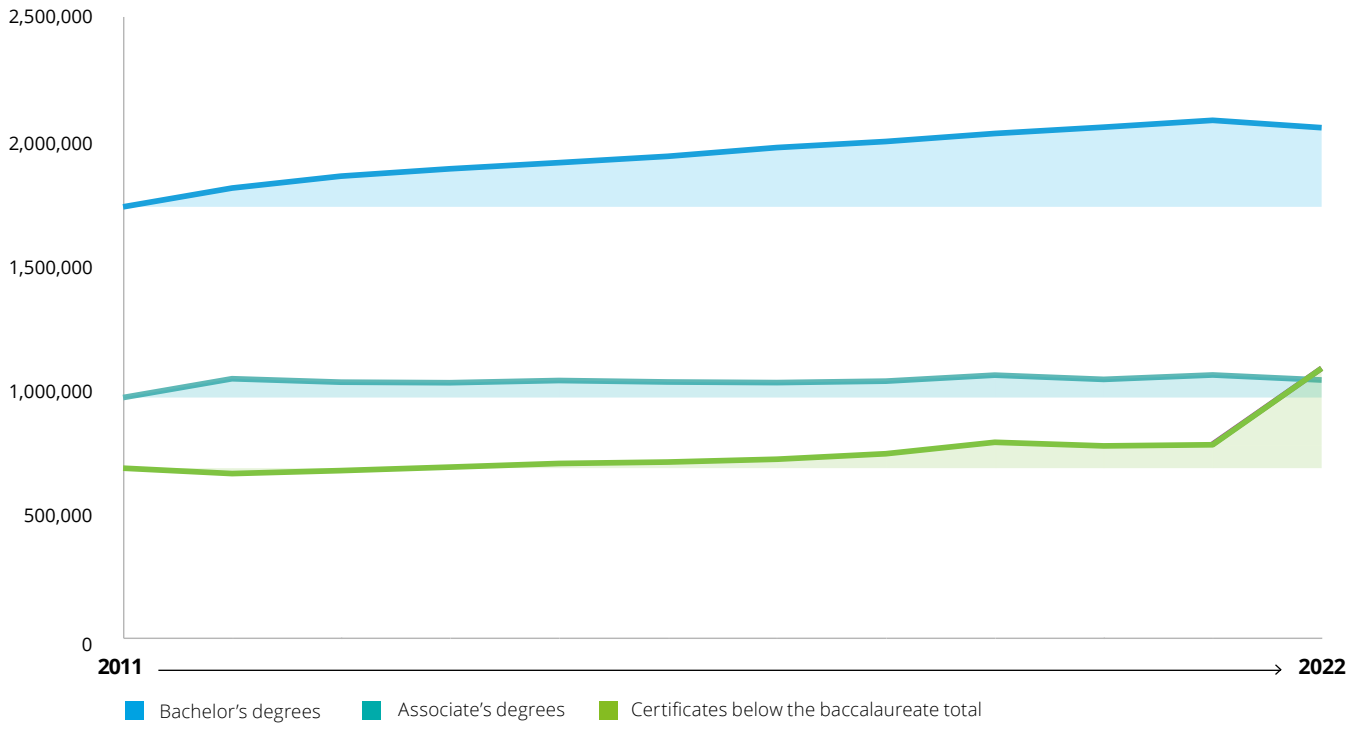
Industrial machinery maintenance technicians comprised over 270,000 employees in manufacturing in 2022 and these roles could grow as much as 16% by 2032.[26] Mechanical and industrial engineers combined to make nearly 370,000 employees in the sector and these occupations are each likely to expand by almost 11% over the same period.[27] Together, software and web developers, computer and information systems managers, and computer and information analysts constituted close to 243,000 manufacturing employees in 2022, and combined, they could increase by nearly 13% by 2032.[28] Although statisticians and data scientists currently make up a small portion of manufacturing employment (7,500), these roles may grow by close to 30% by 2032.[29]

Traditional production roles are likely to also continue to be important. According to BLS data, production-related occupations currently employ the largest number of people in the sector, and BLS also projects this to be the case in 2032.[30] However, the fastest growing production roles are likely to be those that require higher-level skill sets, such as semiconductor-processing technicians, machinists, first-line supervisors, welders, and electronics and electromechanical assemblers.[31] Gains are also likely for material-moving occupations such as laborers and material movers and industrial truck and tractor operators.[32]

### *Educational trends suggest a gap*

Graduation data from the National Center for Education Statistics suggests that traditional training methods may not be able to keep up. While the number of bachelor's degrees awarded in all fields of study from 2011 to 2022 has increased, the number of associate degrees—which tend to prepare graduates for high-skill trades—has remained stagnant (figure 4). The number of certificates awarded, which can offer foundational training for skilled trades, has experienced a moderate increase over the same period, and a significant jump from 2021 to 2022, even surpassing the number of associate degrees awarded.

**Figure 4. Bachelor's degrees climb while associates degrees stagnate in the US from 2011–2022 across all fields of study**




Note: Data includes all 38 fields of study reported by the National Center for Education Statistics, expanding beyond manufacturing roles.
Source: Deloitte analysis of data from National Center for Education Statistics.

For degree programs most relevant to manufacturing, there has been a substantial increase in graduates from programs such as computer and information sciences and engineering (figure 5) that typically require a bachelor's degree. There has also been growth in mechanic and repair technologies degrees, as well as precision production, fueled in large part, it appears, by substantial post-pandemic upticks from 2021 to 2022. However, growth has been slow in the remaining programs that prepare graduates for higher skilled roles like engineering technologists and skilled transportation and material moving positions. Our analysis also found that the average growth in certificates awarded was more than four times the growth in associate degrees for manufacturing-related programs over 2011 to 2022.

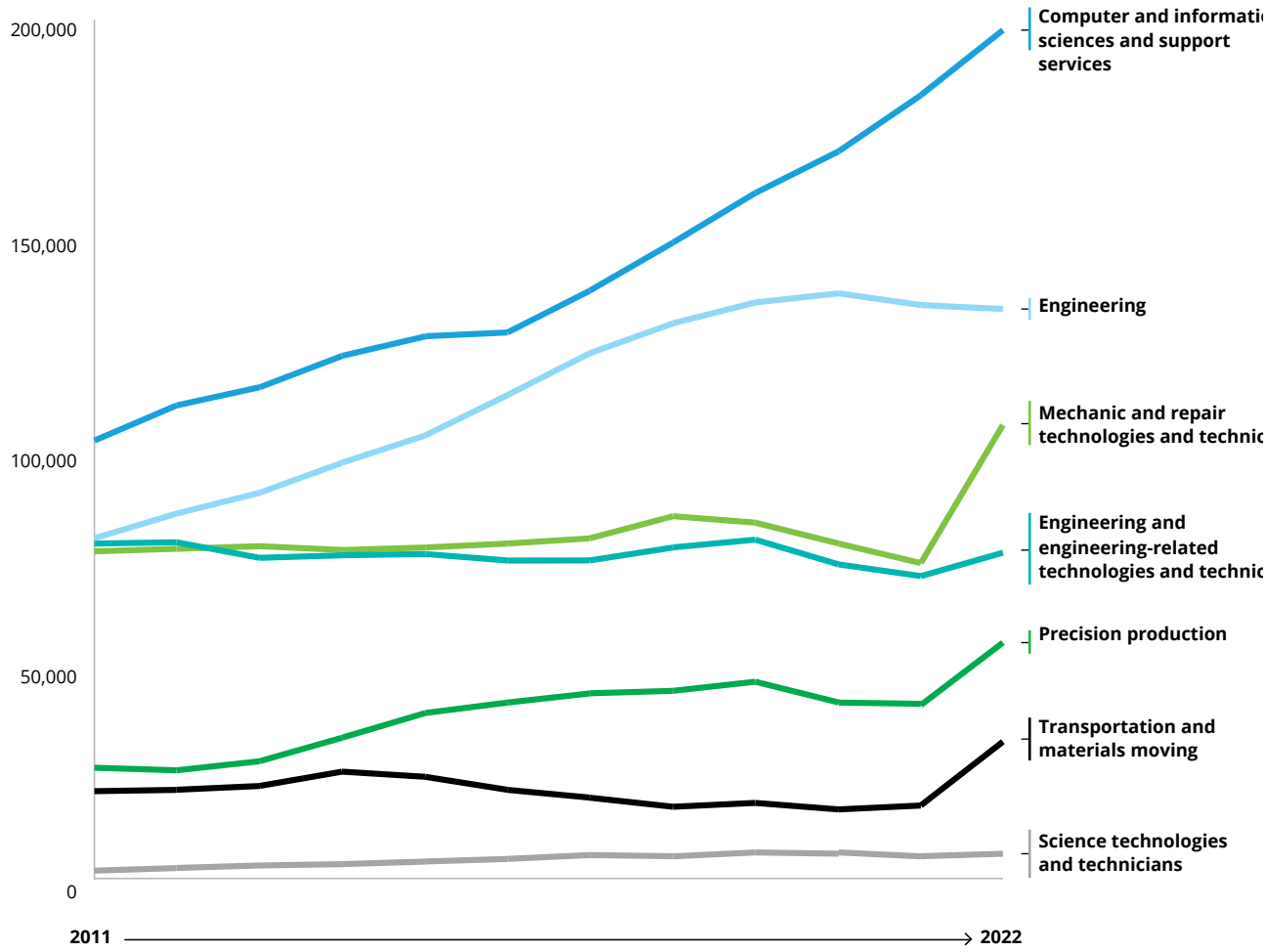
While this trend could help to grow a talent pool with the foundational knowledge companies can continue to build upon once workers are hired, it also suggests there may be a need to produce more highly skilled graduates with associate degrees. In general, if the number of people entering and graduating from degree programs that prepare them for high-skill manufacturing trades does not accelerate, the talent gap could widen.

Some manufacturers are taking an active role—and the lead—in addressing talent challenges

The key question becomes: Given the talent challenges, how can manufacturers build the workforce needed to seize the growth opportunity at hand? Our study found that there is a shift underway in the sector and, in general, companies are currently taking a more active approach to addressing both the skills gap and the applicant gap. Manufacturers seem to be focusing on investing in partnerships—and the worker pipeline and the work environment—to help create the workforce they need with the requisite skill sets and improve employee retention. Our study found that the following three approaches, when used in combination, are helping some manufacturers in overcoming the talent challenges they face:

1. Understanding changing workforce expectations
2. Applying a "customer focus" to workforce challenges to create a leading worker experience
3. Taking an ecosystem approach to attract and upskill talent

**Figure 5. Number of graduates for manufacturing jobs has varied by role**




Note: Graduate includes certificates, associates, and bachelor's degrees for selected (manufacturing-focused) courses.
Source: Deloitte analysis of data from National Center for Education Statistics.

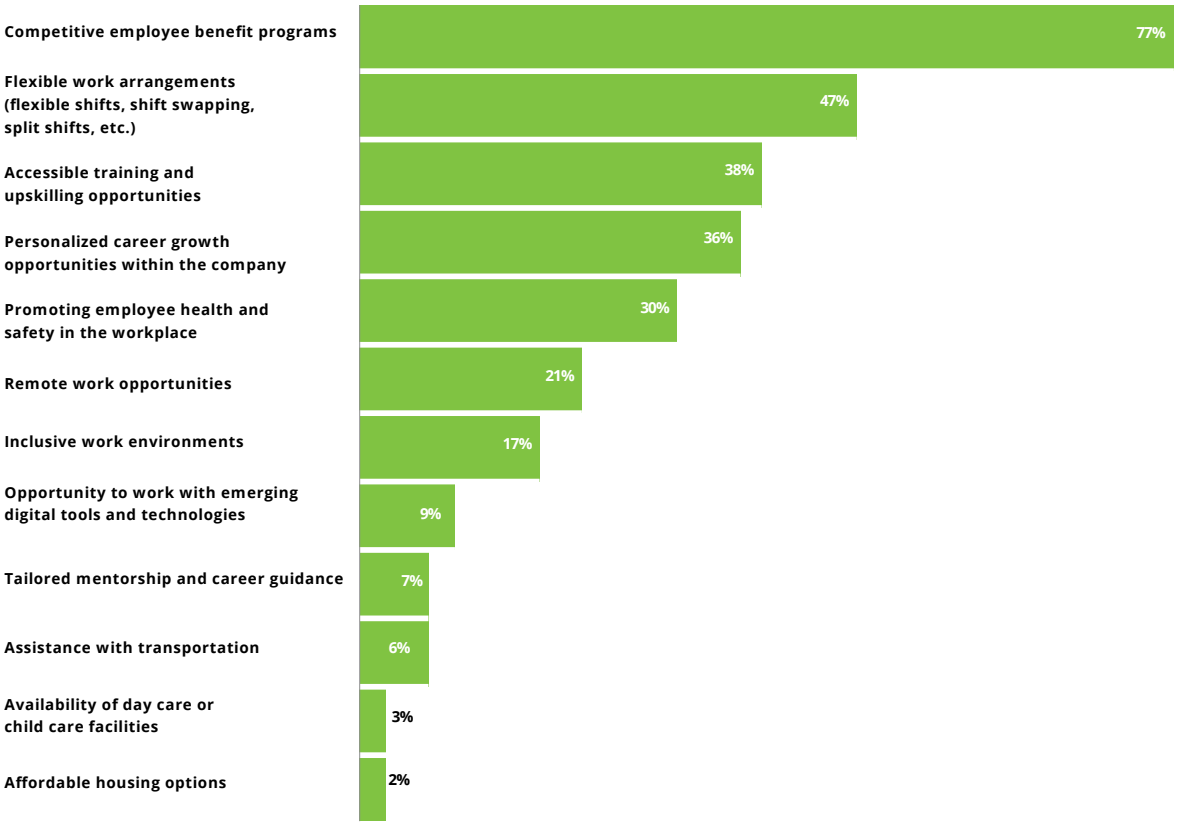
# Changing workforce expectations affect hiring and retention

As more baby boomers and Generation X workers move closer to or into retirement, the workforce may be made up more of millennials and Generation Z workers, who can have a different set of expectations when it comes to work culture and the working environment itself. In one recent survey, those respondents were found to be more prone to job switching, which can impact attraction and retention.[33] Generally, surveyed executives from our study reported that higher levels of flexibility, including remote-work options, seem to be among the most impactful strategies to attract and retain employees (figure 6), which can also be challenging with fixed work schedules and traditional in-person production team settings often seen in manufacturing.[34]

"The average tenure in our organization is reducing. So, we need to understand that even if we get a capable hire for two years, how do we then accelerate the capable hire's onboarding and distribution of knowledge across the larger organization and develop others quickly with the expectation that they're not going to stay with us for more than two years."

**—Interview with industry executive**[35]

**Figure 6. Most impactful strategies to attract and retain employees, according to survey respondents**




Source: Analysis of 2024 Deloitte and The Manufacturing Institute talent study.

### Providing the flexibility that workers want

Nearly half (47%) of respondents in our study indicated that flexible work arrangements (for example, flexible shifts, shift swapping, split shifts) is the strategy that their company has found to be most impactful for retaining employees (figure 6). Flexible work was second only to competitive employee benefit programs.

Some companies have piloted or implemented child care programs and have observed significant benefits. An executive from a distribution and logistics service provider told us that a pilot child care program run by an external organization was established adjacent to a warehouse and it was utilized by close to 80% of employees, who paid for the care. The executive reported a fourfold improvement in the turnover of this facility.[40]

An executive from an electric products manufacturer shared that the company developed a two-day per week part-time position that offers tuition assistance and pay without benefits that initially targeted university students.[41] The executive added that once the program was off the ground, "to our surprise, there were a lot of stay-at-home parents that wanted that—they came out of the woodwork to have a two-day workweek." They now have close to 400 employees in the successful program with good attendance and retention rates.

Some manufacturers are partnering with innovative temp agencies to provide the workforce and skills they need while providing workers the flexibility that they are looking for. Leveraging digital tools and apps, some temp agencies can provide part-time workers, including the semi-retired, college students, and caregivers, the opportunity to sign up for work slots and overtime, while providing the flexibility to cancel or swap shifts, with vacated spots being backfilled with another worker, with the help of AI tools.[42]

**A predicament to solve**

The hours spent on caretaking have increased for full-time workers since the pandemic; this includes child care but also care for parents and spouses.[36] According to BLS data, the average number of employees who missed work in the United States in 2023 due to child care stood at 47,000—42% above the pre-pandemic 2019 average of 33,000.[37] In a recent Manufacturing Institute study, 49.2% of women and 8.0% of men indicated that lack of child care support was their most significant labor-force challenge.[38] Yet in a previous Deloitte and Manufacturing Institute study, only 8% of surveyed manufacturing leaders said that their company offered new or additional day care options.[39]

### Taking a bigger role in skills development to attract and retain employees

The applicant gap seems to be prompting more employers to focus on training as a means to attract and retain employees. According to *Deloitte's Workforce Experience* research, employees who feel they can acquire necessary skills that are important for the future are 2.7 times less likely to leave their organization in the next 12 months.[43] Changing skill requirements have prompted some companies to employ a "skills-based" approach that focuses on employees' abilities and competencies rather than their job titles or formal qualifications, better aligning workers with work that fits their skills and capabilities (figure 7).

Manufacturers seem to recognize the value of upskilling and are using a variety of strategies to train employees, irrespective of role or function, to create an agile workforce. Internal training academies or programs were highlighted as instrumental in helping employees adapt to new technologies and processes.

Many companies are also leveraging e-learning platforms to facilitate flexible and self-paced learning opportunities and are sponsoring industry workshops, conferences, and seminars to help ensure employees are apprised of industry trends and leading practices. Some employers are conducting regular skills assessments of employees to track progress and refine training programs to meet evolving needs.

Mentoring, knowledge transfer, and rotational programs for new hires are gaining traction among manufacturers and are intended to enrich employees' experiences while helping to ensure well-rounded skill development. Such programs can encourage employees to gain experience across departments, which helps enable a versatile workforce.

### Providing additional support that employees seek

There is growing recognition that many job seekers need support services to help them meet the requirements of a full-time job, and these can range from help with the daily commute to finding affordable housing close to their job.[45] Reliable transportation to complete a daily commute can be a challenge for some employees, especially in rural areas with limited or no public transit.[46] An executive from an electric products manufacturing company mentioned that "[reliable] transportation was the number one reason people were leaving our roles."[47] The company partnered with a transportation service provider to offer subsidized rides to employees to and from work.[48] An automotive manufacturer in a rural area is collaborating with other companies and city and county government to investigate the local obstacles to transportation and devise pilot programs to improve transportation in the area.[49]

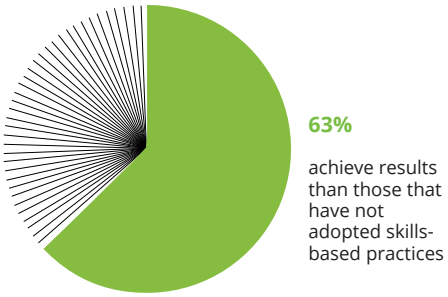
Finding affordable housing is also a challenge for some employees, especially given that the median home price in the United States increased by 37% between January 2019 and November 2023 and the average rental price in US cities rose by 26% over the same period.[50] Our interviews emphasized some manufacturers are working with a state or local government to investigate and develop affordable workforce housing options and opportunities.[51]

"STEM has been defined for years as science, technology, engineering, and mathematics. But STEM to us is soft skills, technical or technology skills, engagement, and motivation. Those are the skills we need. The rest of it can be taught all day long."

**—Interview with industry executive**[44]

**Figure 7. Surveyed skills-based organizations see results**

**Organizations that embed a skills-based approach are more likely to ...**



**63%** achieve results than those that have not adopted skills-based practices

**107%** place talent effectively

**98%** have a reputation as a great place to grow and develop

**98%** retain high performers

**79%** have a positive workforce experience

**57%** anticipate change and respond effectively and efficiently

**52%** innovate

**49%** improve processes to maximize efficiency

**47%** provide an inclusive environment

Notes: Skills-based organizations' ratio reflects the combined weighted ratios of the HR executive survey item, "Our organization's business and HR executives are aligned on the importance of skills in making decisions about work," and the worker survey items: "My employer treats workers as whole, unique individuals who can each offer unique contributions and a portfolio of skills to the organization," "My organization supports me in pursuing opportunities to create value through activities that are outside of the direct scope of my job," and "My organization makes it easy to apply my skills where they are most needed."; Results are defined as 11 business and workforce outcomes: meeting or exceeding financial targets, anticipating change and responding effectively and efficiently, innovating, achieving high levels of customer satisfaction, positively impacting society and communities served, improving processes to maximize efficiency, being a great place to grow and develop, placing talent effectively, providing workers with a positive workforce experience, providing an inclusive environment, and retaining high performers.
Source: Deloitte analysis of Deloitte skills-based organization survey, May–June 2022.

# Applying customer focus to create a leading workforce experience

Creating and improving products and processes is the core of what manufacturers do. They use a variety of strategies and frameworks to accomplish these objectives, such as "define, measure, analyze, improve, and control" (DMAIC)[52] and Design Thinking.[53] This focus on what the customer needs could be applied to creating innovative workforce solutions, especially when the optimal worker experience is a guiding principle. One executive emphasized that empowering talent organizations to be innovative is important, as "challenging them to be entrepreneurs and find new disruptive ways of doing things can bring great ideas."

Another executive said, "We want our customers to be first. We want our employees to be first. We want to meet them where they are, which means we adjust how we do things." According to a study on the American workplace, employees in the manufacturing industry seem to be less engaged when compared to other industries.[54] Actively disengaged employees are almost twice as likely to seek new jobs than engaged employees.[55]

### Creating a sense of purpose

According to The *Deloitte Global 2022 Gen Z and Millennial survey*, nearly 40% of millennials and Gen Zs have turned down a job because it didn't match their values. On the other hand, respondents who are happy with their company's impact on society and the environment are more likely to stay with the company for over five years.[56] Executive interviews indicated that providing a sense of purpose, emphasizing the importance of culture, and establishing clear leadership can provide motivation and help drive performance.

In particular, multiple executives highlighted that centering at least part of their mission statement on green products and projects and their benefit to the planet has helped them to attract and retain talent. An executive from a household electronics manufacturer expressed it this way: "This population cares about the planet and they want companies who are responsible in the way they manage their company. Sustainability is a very key part of what we do in our business—it's important to our associates and it's important to our customers."[58]

### Promoting a work environment focused on health, safety, and comfort

Several executives that we interviewed indicated that creating a comfortable working environment was important not only for attracting new talent but could also make the difference between keeping or losing employees to a competitor. As one executive summed it up, "We have to provide ways for people to feel safe and comfortable when they come to work. It's really important that employees feel like their companies care about them—that they see them—and that they believe that their employees' health and well-being are important." And the needed improvements can be as intuitive as better lighting in the parking lot or improving the cafeteria.

"People who have been here for a long time and new hires are seeking a sense of belonging and being part of something bigger. It's not a mantra that we just talk about with a certain level of employees—it's deep throughout the organization, and when they come to work, they know what they are coming to work for, and they sign up to that purpose."

**—Interview with industry executive**[57]

One executive indicated that before acquiring and completely renovating a 50-year-old manufacturing facility, their company surveyed employees to determine what was most important to them in a working environment. Improved lighting, including natural light, and air quality were at the top of workers' lists, and the renovated smart factory design was based on the feedback received.[59]

### Technology can help engage and empower workers—and make their jobs better, safer, and easier

Technology plays an important role in shaping the future of workforce development. It can act as a magnet in both attracting and retaining skilled individuals. As gleaned from our interviews, high-tech manufacturing environments seem to appeal to the workforce. Manufacturers that have built smart factories to enhance performance are also noting higher retention in these high-tech facilities.[60]

Deloitte Global's *Millennials and Gen Z Study* highlights that more than one-third of surveyed millennials and Gen Zs believe that AI and other technologies can augment jobs or various job functions over the next decade.[61] In another recent study, over half of the surveyed workforce believe it is important for manufacturers to focus on the consistent availability of technology to attract more people, whereas only 31% of manufacturing executives agreed to prioritize technology to attract employees.[62]

Enhanced employee engagement can be achieved by integrating technology into manufacturing processes. Digital tools including AI, generative AI, and automation can be used to augment mental and physical human capabilities to optimize production, make jobs easier, and provide autonomy by giving operators new channels to report production issues, which can enable efficient triage and rapid problem resolution. The integration of technology has also helped to revolutionize upskilling in the industry. Most companies we interviewed are exploring the potential of augmented or virtual reality (AR or VR) for comprehensive training, potentially allowing workers to acquire new skills using these tools. An executive mentioned that VR has reduced training time for welders at the company by 50% to 60%. The flexibility in technology-facilitated trainings can enable individuals to upskill at their convenience, helping to foster a more dynamic and efficient learning environment.

### Partnerships to build awareness of manufacturing careers and opportunities

Manufacturers across the nation open their doors on National Manufacturing Day to provide plant tours to the local community, including students, parents, teachers, and guidance counselors from K-12 schools.[69] A past Deloitte study has indicated tours of advanced manufacturing facilities for students can be an effective strategy for increasing interest in manufacturing jobs.[70] Several manufacturing executives indicated that company representatives regularly visit local K-12 schools to talk about the company, careers offered, and the high-tech environment in manufacturing facilities to inspire students to consider manufacturing careers.[71] Several companies have also donated manufacturing equipment to schools to spark interest and support skills development.[72]

In partnership with an engineering and construction firm and a welding equipment manufacturer, the American Welding Society offers nationwide grants to high school programs that do not currently have welding programs.[73] The grant provides a kit with a welding machine and other equipment to give students the opportunity to experience welding—many for the first time—and possibly inspire them to consider a career in the field. In another example, a flooring manufacturer implemented a work-based learning program in partnership with local high schools, which provides flexible and paid work experiences in several departments, as well as opportunities to advance into an apprenticeship program.[74] The company reported that, in 2023, it achieved 100% retention of graduating seniors and hired over 50 students from the program.[75]

### Partnerships to build, leverage, and support training programs

Some manufacturers are finding innovative ways to form partnerships to work with local technical colleges—as well as organizations throughout the talent ecosystem—to build the workforce that they need. Employer-led consortia to create programs that suit shared workforce development needs seem to have become more commonplace. Some consortia are even led by local workforce, government, or economic development agencies to build a workforce with the requisite skills to support a specific manufacturing sector in a region.[76]

Many states have implemented manufacturing career pathways from the National Career Clusters® Framework[77] to create programs that meet state needs, and an updated framework design is expected in fall 2024.[78] Strong workforce training programs can be important for attracting new businesses and keeping existing companies within a state.[79] In Georgia's QuickStart program, the Technical College System of Georgia partners with manufacturers to establish new facilities or expand in the state to develop and deliver customized training programs to create a skilled workforce ready to begin production.[80] Since its inception, QuickStart has trained over 1 million workers and companies often cite it as an important factor for choosing to set up new facilities or expand in Georgia.[81] The Virginia Talent Accelerator Program, a partnership between the Virginia Economic Development Partnership and the Virginia Community College System, offers recruitment and training services to greenfield or expanding facilities in the state of Virginia.[82] The Greater Wichita Partnership worked with Deloitte to develop an action plan to help the region build a workforce for the future. The plan emphasizes the need for collaboration among industry, education, and community stakeholders to drive inclusion, expand the talent pool, invest in skill development, and support innovation. Together, they can provide access to upskilling opportunities focused on high priority skills such as communication, computer literacy, and project management.[83]

Some manufacturers are partnering with community organizations. For example, a large automotive manufacturer partnered with Goodwill to administer credentialled training programs in local communities focused on developing digital skills, including IT support, and even training auto technicians.[84] Other companies have partnered with Goodwill to take advantage of the trained talent pool that they offer through the Talent Source program,[85] or the manufacturing services that they offer, including producing and packaging automotive components, and even manufacturing uniforms for the US military.[86]

Apprenticeships and programs for work study also appear to be on the rise. The number of apprentices in advanced manufacturing occupations increased to 59,500 in fiscal 2023, which is nearly triple the total in fiscal year 2021.[87] Nearly half (47%) of survey respondents in the *2022 Deloitte and The Manufacturing Institute Perceptions* study indicated that apprenticeships, work studies, or internships at manufacturing companies would be the most effective way to increase interest in manufacturing as a career choice.[88] The Manufacturing Institute's FAME program is one example that has helped to bolster the pipeline for maintenance technicians (see sidebar titled "FAME: Developing regional pools of maintenance technicians"). The Inflation Reduction Act offers tax credits to companies who hire employees from registered apprenticeship programs, which may increase the demand for apprenticeship programs and help expand training opportunities.[89]

**Partnerships that look beyond the traditional talent pipeline**

Manufacturers have focused efforts on increasing the size of their talent pool and created a more diverse and inclusive workforce by partnering with a variety of organizations to engage groups that may have unique barriers to entering or re-entering the workforce.

***Individuals that were formerly incarcerated who seek a "second chance"***

Several manufacturers have established a sense of purpose, given back to their local community, and even improved retention rates by providing work opportunities to applicants that were formerly incarcerated, who are reentering the workforce. A packaging manufacturer reported that almost 70% of its nearly 200-person workforce comprised second-chance individuals—and the company's attrition rate is 25 percentage points lower than the sector average.[94] In a recent study, 82% of managers reported that second-chance individuals may add even more value to their companies than those not part of the program.[95] Through the Workforce Opportunity Tax Credit, companies can also receive up to US$2,400 per employee.[96] However, people that were formerly incarcerated may face unique challenges related to transportation, housing, and job flexibility. Partnerships with local organizations can be essential for providing this support in cases where manufacturers don't have the expertise or resources in house (see sidebar titled "Resources supporting job-seekers that were formerly incarcerated").

***Refugees and immigrants***

Some companies have partnered with local organizations and resettlement groups to access a diverse talent pool of refugees and immigrant populations. A furniture manufacturer began hiring refugees nearly four decades ago and today they make up nearly half of the company's workforce.[100] Not only does it help to fill a need for workers, but it can also provide a sense of purpose as the company and workforce help community members. An executive from a large manufacturing company stated that new partnerships were needed to implement a similar program, but the benefits have been well worth it.[101] While a majority of companies that have implemented refugee hiring programs report higher retention rates and lower turnover, there are unique challenges to overcome, including language and cultural barriers.[102]

***Veterans***

According to the study, nearly one-third of surveyed manufacturers are partnering with organizations that support veterans. Their military experience often instills technical, leadership, and communication skills that are important for success in a manufacturing environment.[104] But transitioning into a civilian workplace is not without its challenges.[105] It can be difficult for veterans to communicate how the skills, traits, and work habits developed in the military align with those listed on job requisitions. Partner organizations that support veterans, and programs like The Manufacturing Institute's Heroes MAKE America,[106] can help manufacturers make these connections, provide veterans with access to manufacturing-specific training and certification, and help companies establish a pool of veteran candidates.[107]

"In the past, we said you had to be fluent in English, and we were missing out on a very hardworking, committed workforce. We teamed up with our local community partners and have been able to access a diverse group of refugees and immigrants from Afghans to Cubans, to other Spanish-speaking populations. It's been tremendously successful—the retention rate is significantly better than other populations—it's 76%. We are also developing an app so that they have access to translation available at their fingertips."

**—Interview with industry executive**[103]

**FAME: Developing regional pools of maintenance technicians**

One example of an innovative program to build regional pools of maintenance technicians—which are in high demand in advanced manufacturing environments—is the FAME program, which was started by an automotive manufacturer and transferred to The Manufacturing Institute to boost its national reach.[90] Students attend classes at a local community college two days a week and work three days for a local sponsoring manufacturer.[91] They are paid a competitive wage and engage in hands-on training and classroom education to develop technical and professional skills related to manufacturing. Graduates earn an associate degree and are certified as an Advanced Manufacturing Technician. The automotive manufacturer worked closely with its initial community college partners to tailor the program to meet its needs.[92] Today, the program has grown to nearly 40 employer-led chapters in 14 states, and it has produced over 1,800 graduates since 2012 who have benefitted from a 90% placement rate.[93]

**Resources supporting job seekers that were formerly incarcerated**

The Manufacturing Institute recently released its "Second Chance Hiring Toolkit for Local Communities," which leverages data from successful second chance programs across the United States. The toolkit recommends identifying a local hub organization to form partnerships between employers and community-based reentry organizations to build regional programs.[97] An example of a partnership model is the Beacon of Hope Business Alliance in Cincinnati, Ohio, which is operated by Cincinnati Works, a nonprofit organization whose mission is to provide workforce training and support services that people living in poverty need to become economically self-sufficient.[98] The goal of the alliance is to support job seekers that were formerly incarcerated, as they seek meaningful employment.[99] It is an ecosystem of partners that includes employers, community-based organizations that provide workforce training and support, a local government reentry and rehabilitation office, a nonprofit legal organization, and faith-based organizations.

### *Workplace accommodations*

Some people have unique abilities that can make them a good fit for certain manufacturing roles—including skilled production jobs like computer numerical control machine operators—that are generally difficult for manufacturers to fill.[108] There may be individuals with remarkable intellectual and visual abilities, as well as a high propensity to learn, who may also be neurodiverse and require additional accommodations in the workplace.[109] An automotive aftermarket parts supplier and a large heavy equipment manufacturer have formed innovative partnerships with organizations in their communities, which specialize in working with and training people with disabilities for the workforce.[110] These partnerships have led to the partner organization providing contract manufacturing services, as well as direct hiring of employees by the manufacturer. Moreover, individuals with physical limitations may be able to pursue additional employment opportunities with the advancement of digital technologies and robotics, as their qualifications and certifications could still enable them to engage in remote control monitoring of robotics, for example. The potential pool of talent is significant. Over 33 million working-age Americans were identified as having a disability in 2023—only 7.5 million are currently employed, and only 9.1% are employed in manufacturing.[111]

### A dedicated focus on the talent development team

It can take dedicated effort, and perhaps additional resources, including staff members with additional experience and skill sets, for talent organizations to take an ecosystem approach and focus on the many aspects of worker experience. An individual or group within the company should be responsible for getting out into the community and building relationships with the full spectrum of organizations within the ecosystem. Professionals with an economic development, business development, or sales background may be particularly well-suited for this role. On the other hand, experience performing research and analysis may be most helpful for benchmarking and comparing existing innovative talent programs. Partnering closely with plant managers, front-line supervisors, and other production leaders to offer training and support when implementing new and innovative talent programs may be necessary. Finally, new positions may be needed to support the needs of applicant groups.

# Endnotes


1. Deloitte analysis of data from: US Bureau of Labor Statistics, "The employment situation—February 2024," news release, March 8, 2024.
2. Deloitte analysis of data from: US BLS, "Quarterly census of employment and wages," accessed March 21, 2024.
3. Deloitte analysis of the purchasing managers' index (PMI) reports published by the Institute for Supply Management.
4. Reshoring Initiative, *Reshoring Initiative®—1H 2023 report: Geopolitical risk and industrial policy drive reshoring and FDI announcements*, accessed March 21, 2024.
5. Deloitte analysis of data from: The White House, "President Joe Biden: Investing in America," accessed March 21, 2024.
6. Ibid.
7. US Department of Defense, "DOD releases first-ever national defense industrial strategy," press release, January 11, 2024.
8. National Association of Manufacturers, *2024 First Quarter Manufacturers' Outlook Survey*, March 5, 2024.
9. *2024 Deloitte and MI Talent Study.*
10. Deloitte analysis of BLS' unemployment data from: US BLS, "Labor force statistics from the Current Population Survey," accessed March 21, 2024; and job openings data from: US BLS, "JOLTs database," accessed March 21, 2024.
11. Deloitte analysis of data from: The World Bank, "Population growth (annual %)—United States," accessed March 21, 2024; and US BLS, "Civilian labor force participation rate," news release graphic, accessed March 21, 2024.
12. Deloitte analysis of data from: US BLS, "Table 4. Quits levels and rates by industry and region, seasonally adjusted," news release graphic, accessed March 21, 2024.
13. Guardian, *Standing up and stepping in*, 2023, p.6.
14. Insights gleaned from interviews with industry executives conducted in January 2024.
15. Deloitte Insights and The Manufacturing Institute, *Competing for talent: Recasting perceptions of manufacturing*, 2022.
16. Deloitte analysis of data from: US BLS, "Labor force statistics from the Current Population Survey;" and estimates of private investments from: The White House, "President Joe Biden."
17. *2024 Deloitte and MI Talent Study.*
18. World Economic Forum, "Economy, industry, region, and skills profiles – Industry 'Advance Manufacturing'," accessed March 21, 2024.
19. Ibid.
20. Deloitte analysis of job posting data using the LightCast™ database.
21. Deloitte Insights and The Manufacturing Institute, *Beyond reskilling: Manufacturing's future depends on diversity, equity, and inclusion*, 2021.
22. *2024 Deloitte and MI Talent Study.*
23. Insights gleaned from interviews with industry executives conducted in January 2024.
24. Deloitte analysis of data from: US BLS, "Employment projections," accessed March 21, 2024.
25. Ibid.
26. Ibid.
27. Ibid.
28. Ibid.
29. Ibid.
30. Deloitte analysis of data from: US BLS, "Employment projections."
31. Ibid.
32. Ibid.
33. Deloitte Insights and MI, *Competing for talent*.
34. Insights gleaned from interviews with industry executives conducted in January 2024.
35. Interview with an industry executive, January 2024.
36. Guardian, *Standing up and stepping in*, 2023, p.6.
37. Deloitte analysis of US Bureau of Labor Statistics data.
38. Chad Moutray, *The manufacturing experience: Closing the gender gap*, The Manufacturing Institute, 2022.
39. Deloitte Insights and MI, *Competing for talent*.
40. Insights gleaned from interviews with industry executives conducted in January 2024.
41. Ibid.

# Endnotes


42. MyWorkChoice, "Bring flexibility to your workforce," accessed March 22, 2024.
43. Deloitte Digital, *Workforce Experience Research Study*, 2023.
44. Interview with an industry executive, January 2024.
45. Brookings, *The growing distance between people and jobs in metropolitan America*, 2015.
46. Deloitte Insights and MI, *Competing for talent*.
47. Insights gleaned from interviews with industry executives conducted in January 2024.
48. Ibid.
49. Ibid.
50. Deloitte analysis of data from: US Census Bureau, "New residential sales," accessed March 22, 2024; and: US BLS, "Consumer price index," accessed March 22, 2024.
51. Insights gleaned from interviews with industry executives conducted in January 2024.
52. American Society for Quality, "The Define Measure Analyze Improve Control (DMAIC) process," accessed March 22, 2024.
53. Interaction Design Foundation, "Design Thinking (DT)," accessed March 22, 2024.
54. Gallup, *State of the Global Workplace Report*, 2023.
55. Ibid.
56. Deloitte, *Striving for balance, advocating for change*, 2022.
57. Interview with an industry executive, January 2024.
58. Ibid.
59. Ibid.
60. Insights gleaned from interviews with industry executives conducted in January 2024.
61. Deloitte, *Striving for balance, advocating for change*.
62. Deloitte Insights and MI, *Competing for talent*.
63. Paul Wellener, Stephen Laaper, Ben Dollar, Heather Ashton, David Beckoff, "Accelerating smart manufacturing," Deloitte Insights, October 21, 2020.
64. Deloitte, "Resilient: Confronting the COVID-19 crisis—Episode 19: Enterprises and ecosystems: Fueling resilient recovery through innovation and collaboration," podcast transcript, July 2020.
65. Ibid.
66. National Association of Manufacturers, "Facts about manufacturing," accessed March 22, 2024.
67. *2024 Deloitte and MI Talent Study.*
68. Insights gleaned from interviews with industry executives conducted in January 2024.
69. Manufacturing Institute, "Manufacturing Day," accessed March 24, 2024.
70. Deloitte Insights and MI, *Competing for talent*.
71. Insights gleaned from interviews with industry executives conducted in January 2024.
72. Ibid.
73. Arc Welding, "AWS Foundation awards Light a Spark Grant to seven schools," news release, The Welder, November 6, 2023.
74. University of Georgia, "Building the future workforce: Mohawk's high school programs," accessed January 2024.
75. Ibid.
76. Strada Education Foundation, "Employer and community college partnerships," accessed March 22, 2024.
77. Advance CTE, "The National Career Clusters Framework," accessed March 22, 2024.
78. Advance CTE, "Advancing the framework," accessed March 22, 2024.
79. Steve Kaelble, "2023 top states workforce development programs," *Area Development*, 2023.
80. Georgia Quick Start/Technical College System of Georgia, "What we do," accessed March 22, 2024.
81. Georgia Department of Economic Development, "Workforce and education," accessed March 22, 2024.
82. Virginia Economic Development Partnership, "Virginia Talent Accelerator program," accessed March 22, 2024.
83. Greater Wichita Partnership, "The talent roadmap—A way forward," accessed March 22, 2024.
84. Goodwill Industries International, "Goodwill® and General Motors launch GoodProspects® for careers," press release, October 4, 2018.

# Endnotes


85. Goodwill of Central and Southern Indiana, "Goodwill TalentSource™," accessed March 22, 2024.
86. Goodwill of Central and Southern Indiana, "Global forming," accessed January 2024; Goodwill South Florida, "Two of South Florida's largest employers join forces to provide jobs while producing US Military uniforms and veteran interment flags," May 14, 2019.
87. Apprenticeship USA, *Advanced manufacturing*, October 2023.
88. Deloitte Insights and MI, *Competing for talent*.
89. Michelle Meisels, Misha Nikulin, Kate Hardin, Matt Sloane, and Kruttika Dwivedi, "2024 engineering and construction industry outlook," Deloitte Insights, accessed March 22, 2024.
90. FAME USA, "Home," accessed March 22, 2024.
91. Ibid.
92. Dave Tobenkin, "Employers partner with community colleges to fill the talent pipeline," Society for Human Resource Management, accessed March 22, 2024.
93. FAME USA, "Change your life with FAME USA," accessed March 22, 2024.
94. Micah Solomon, "How second chance employees can boost a bottom line: The Nehemiah Manufacturing success story," *Forbes*, August 9, 2021.
95. National Association of Manufacturers, "Second chance hiring strengthens manufacturing," news release, May 20, 2021.
96. Internal Revenue Service, "Work opportunity tax credit," accessed March 22, 2024.
97. The Manufacturing Institute, "Second chance hiring toolkit for local communities," accessed March 22, 2024.
98. Cincinnati Works, "A job is just the beginning," accessed March 22, 2024; Beacon of Hope Business Alliance, "Creating a fair chance for decent work," accessed January 2024.
99. Ibid.
100. Bobby Dalheim, "Hiring refugees is good for people, good for business, says Stickley CEO," *Furniture Today*, August 15, 2023.
101. Insights gleaned from interviews with industry executives conducted in January 2024.
102. Theresa Agovino, "US companies step up to Hire Afghan and Ukrainian refugees," accessed March 22, 2024.
103. Interview with an industry executive, January 2024.
104. Helen Sydney Adams, "Why veterans make an excellent fit in manufacturing," *Manufacturing Digital*, June 9, 2023; Lindsay Gilder, "Veterans make great industrial employees—Here's how to recruit them to join your team," *Thomas Publishing Company*, May 22, 2023.
105. Ibid.
106. The Manufacturing Institute, "Heroes MAKE America," accessed March 22, 2024.
107. The Manufacturing Institute, *Transitioning military-affiliated talent into manufacturing*, February 2024.
108. Catherine Ross, "Embracing the skills of individuals with autism for machining," *Industrial Supply Magazine*, October 25, 2023.
109. Ibid.
110. Pride Industries, "Solve the manufacturing skills gap with people with disabilities," October 9, 2023; Caterpillar, "Community partnerships to enable the work that matters," April 14, 2021.
111. US BLS, "Persons with a disability: Labor force characteristics—2023," news release, February 22, 2024.

# Authors


### John Coykendall | jcoykendall@deloitte.com

John Coykendall is a vice chair, Deloitte LLP, and the leader of the US Industrial Products & Construction practice. John has more than 25 years of consulting experience focusing on global companies with highly-engineered products in the Aerospace and Defense, Industrial Products and Automotive industries. Coykendall advises senior executives on driving impactful and sustained performance improvement, through both top-line growth and margin improvement initiatives. He has led large-scale transformation efforts to help businesses with strategic cost transformation and operations/supply chain initiatives. Coykendall has an undergraduate degree from Lafayette College in Business & Economics and Government & Law and an MBA from Duke University.

### Victor Reyes | vreyes@deloitte.com

Victor Reyes is a managing director in Deloitte's Human Capital practice, focused on helping organizations reimagine their people strategies and HR capabilities to deliver business results, enhance talent experience, and anticipate and embrace future workforce challenges. He serves as Deloitte's Human Capital consulting leader for the Industrial Products & Construction sector. In his more than 23 years as a management consultant, he has designed and implemented programs that include talent strategy, acquisition, and development; HR technology strategy and deployment; global shared services and outsourcing; mergers, acquisitions and divestitures; and workforce analytics. Reyes holds an MBA from Harvard Business School and a BA in Government from Harvard College.

### Kate Hardin | khardin@deloitte.com

Kate Hardin, Executive Director of Deloitte's Research Center for Energy and Industrials, has worked in the energy industry for 25 years. She currently leads Deloitte's research on the impact of the energy transition on the energy and industrial manufacturing sectors. Before that, Hardin led IHSMarkit's integrated coverage of transportation decarbonization and the implications for automotive and energy companies. Hardin has served as an expert in residence at Yale's Center for Business and Environment, and she is also a member of the Council on Foreign Relations. Hardin has an MBA from the Yale School of Management and a MA in Russian studies from Yale University.

### John Morehouse | jmorehouse@deloitte.com

John Morehouse is the research leader for industrial products manufacturing in the Deloitte Research Center for Energy & Industrials. He has over 25 years of experience in manufacturing-related roles in industry, academia, and government.

### Gardner Carrick | gcarrick@nam.org

Gardner Carrick is the Chief Program Officer for The Manufacturing Institute, the non-profit affiliate of the National Association of Manufacturers. Mr. Carrick leads the Institute's efforts to create a world class workforce for the U.S. manufacturing sector. He oversees all of the MI's program activities, including the Institute's FAME education program, Heroes MAKE America program, Women MAKE America team and workforce initiatives. As a widely respected resource and advisor across the workforce development ecosystem, he is also creating a new national recognition program for the industry-based credentials used in most manufacturing education programs.  And he is leading a public-private partnership to determine the outcomes of manufacturing education programs and develop solutions to improve their results.

# Acknowledgments

The authors would like to thank **Kruttika Dwivedi** and **Anuradha Joshi** for their key contributions to this report, including research, analysis, and writing.

The authors would like to thank **Luke Monck**, **Misha Nikulin**, **Simona Savitt**, and **Lindsey Berckman**, the members of the 2024 Talent Study Deloitte Advisory Board.

The authors would like to thank **Carolyn Lee**, the Advisor from The Manufacturing Institute.

The authors would like to thank **Zack Pu**, **Asi Klein**, **Trey Howard**, and **Ram Iyer** for their subject-matter inputs.

The authors would like to acknowledge the support of **Clayton Wilkerson** for orchestrating resources related to the report; **Narasimham Mulakaluri** and **Akshay Jadhav** for their data expertise; **Daniel Bachman** for his subject-matter inputs; **Heather Ashton Manolian** for managing Deloitte's relationship with The Manufacturing Institute and providing subject-matter inputs; **Kimberly Prauda** and **Neelu Rajput** who drove the marketing strategy and related assets to bring the story to life; **Alyssa Weir** for her leadership in public relations; and **Rithu Thomas** and **Preetha Devan** from the Deloitte Insights team who supported the report's publication.

Cover image by: **Rahul B**

# Contact us

*Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.*

**Industry Leadership**

**John Coykendall**
Vice Chair
US Industrial Products and Construction leader
Deloitte LLP
jcoykendall@deloitte.com
+1 203 905 2612

John Coykendall is a vice chair, Deloitte LLP, and the leader of the US Industrial Products & Construction practice. John has more than 25 years of consulting experience focusing on global companies with highly-engineered products in the Aerospace & Defense, Industrial Products, and Automotive industries.

**Deloitte Research Center for Energy & Industrials**

**Kate Hardin**
Executive director
Deloitte Research Center for Energy & Industrials
Deloitte Services LLP
khardin@deloitte.com
+1 617 437 3332

Kate Hardin has over 25 years experience at the intersection of energy and industry, and is the executive director of the Deloitte Research Center for Energy & Industrials.

# EXHIBIT 23

COALITION OF SERVICES INDUSTRIES

# *White Paper 1: Services and Digital Trade Are Critical to U.S. Competitiveness and Middle-Class Job Creation*

## Introduction

Services and digital trade are fundamental to the health of the American economy. U.S. services and digital firms support every economic sector and are a major source of good, high-quality U.S. jobs. They are world-class innovators and competitors, providing the advanced products and technologies used in advanced manufacturing, climate change remediation, more productive and sustainable agriculture, expanded educational opportunities and greater economic inclusion.

U.S. services and digital industries need cross-border trade and investment to maintain their ability to innovate and compete and thereby continue to grow. Domestic demand alone will not generate sufficient revenue to support the R&D and the high levels of capital investment needed to maintain a globally competitive edge. It is even more important for the U.S. to pursue a robust services and digital U.S. trade agenda now given the rising tide of foreign services restrictions and digital protectionism that threatens American services firms.

This White Paper discusses how a strong U.S. services and digital trade and investment agenda promotes the interests of the American middle class by creating better jobs, promoting U.S. competitiveness, and supporting important goals such as combatting climate change and addressing inequality. The paper also details some of the international trade and investment issues that are undermining the competitiveness of CSI members and their ability to create new U.S. jobs and drive the economic recovery.

## U.S. Services and Digital Sectors Create Good U.S. jobs

Services facilitate and are integrated into all sectors of the economy. Services are both digitally enabled themselves (for example, online shopping) and overall enablers of the digital economy in combination with software, digital technologies, and data flows (e.g., in “smart” products that contain embedded sensors or chips allowing for ongoing data transfers). Digital services are increasingly integrated into the production and sale of finished manufactured goods.

Millions of jobs are involved. According to the most recent Department of Commerce assessment, the digital economy alone directly supports 8.8 million jobs, accounting for 5.7% of

total jobs.[1] More broadly, estimates of direct and indirect jobs associated with digital services are higher: one recent study finds that 19.1 million U.S. jobs are supported by the internet sector.[2] Overall, more than 109 million workers were employed in services-producing sectors of the economy in 2019, 83% of total private sector employment.[3]

## Services and Digital Trade Sectors Create High-Income U.S. Jobs

The U.S. services and digital sectors are creating the higher wage jobs that American workers need—both high school and college educated.

**52 million**

Workers in services occupations earn middle class salaries.

U.S. Government 2019 employment data show that firms employed nearly 52 million workers in services occupations earning middle class wages as defined by Pew Research Center.[4]

- Most American households today "sustain a middle-class living through work in areas outside manufacturing, especially in services sectors where the United States has comparative advantages."[5]
- The Bureau of Labor Statistics projects the number of jobs in these occupations will increase by 6% (+3.1 million jobs) over the next 10 years.[6] Some of the fastest-growing occupations include software developers and testers, registered nurses, general and operations managers, and financial managers.
- It is worth noting that services workers play a key role addressing climate issues. Just one segment of this sector, energy efficiency services, employs more than 3 million, with more than 50% in construction, 20% in professional services, and 14% in manufacturing.[7]

Increasing the competitiveness of U.S. services and digital trade firms in global markets will in turn help expand these jobs.

## The Services Sector Provides Nearly Half of All U.S. Manufacturing Sector Jobs

**49%**

Share of manufacturing sector employment in services occupations.

To date, efforts to create good new jobs for American workers have focused largely on the manufacturing sector, based on the mistaken assumption that traditional production jobs pay better than other occupations. The emphasis on production work is misplaced,

---

1 Jessica R. Nicholson, "New Digital Economy Estimates," U.S. Department of Commerce, Bureau of Economic Analysis, August 2020. This paper notes that BEA is "actively working to develop methodology for estimating the components of the digital economy for which estimates are missing."

2 Internet Association, "Measuring the U.S. Internet Sector: 2019," September 26, 2019.

3 U.S. Department of Commerce, Bureau of Economic Analysis, "Table 6.4D: Full-Time and Part-Time Employees by Industry."

4 Bureau of Labor Statistics, Employment Projections program, Table 1.1, "Employment by major occupational group, 2019 and projected 2029," and Pew Research Center, "Are you in the American Middle Class? Find out with our income Calculator," Factank, July 23, 2020. Pew defines the middle class in 2018 as three-person households earning between $48,500 and $145,500.

5 Carnegie Endowment for International Peace, Making U.S. Foreign Policy Work Better for the American Middle Class, September 23, 2020.

6 Bureau of Labor Statistics, Employment Projections program.

7 Environmental and Energy Study Institute, "Fact Sheet: Jobs in Renewable Energy, Efficiency, and Resilience (2019)," July 23, 2019.

overlooking the major role that services play in creating good jobs in the manufacturing sector.

**Table 1. Portion of Manufacturing Sector Employment in the Services Sector**
**Manufacturing Sector Employment by Occupation, 2019**

| Occupation | Number of Jobs | Typical Entry-Level Educational Requirement | Average Annual Wage (USD) |
|---|---|---|---|
| Production Occupations | 6,466,390 | High School | 40,140 |
| Transportation and Material Moving Occupations | 1,095,620 | High School | 37,920 |
| Office and Administrative Support Occupations | 1,031,950 | High School | 41,040 |
| Architecture and Engineering Occupations | 829,320 | College | 88,800 |
| Management Occupations | 718,560 | College | 122,480 |
| Installation, Maintenance, and Repair Occupations | 648,670 | High School | 50,130 |
| Business and Financial Operations Occupations | 526,720 | College | 78,130 |
| Sales and Related Occupations | 426,650 | High School | 43,060 |
| Computer and Mathematical Occupations | 307,140 | College | 93,760 |
| Construction and Extraction Occupations | 203,890 | High School | 52,580 |
| Life, Physical, and Social Science Occupations | 146,330 | College | 77,450 |
| Arts, Design, Entertainment, Sports, & Media Occ. | 91,520 | Various | 61,960 |
| Food Preparation and Serving Related Occupations | 79,420 | None | 26,670 |
| Building & Grounds Cleaning & Maintenance Occ. | 65,540 | None | 31,250 |
| Farming, Fishing, and Forestry Occupations | 35,450 | Various | 31,340 |
| Protective Service Occupations | 13,070 | High School | 49,880 |
| Healthcare Practitioners and Technical Occupations | 10,790 | College | 83,640 |
| Legal Occupations | 7,390 | College | 109,630 |
| Personal Care and Service Occupations | 1,340 | High School | 31,260 |
| Healthcare Support Occupations | 1,080 | High School | 31,010 |
| Educational Instruction and Library Occupations | 600 | College | 57,710 |
| Community and Social Service Occupations | 400 | College | 50,480 |
| Total Occupations | 12,707,840 | | |

* These data reflect the averages for the occupation generally, not specifically to that occupation within manufacturing. The latter data are not available.
Source: Bureau of Labor Statistics, Occupational Employment Statistics, 2019 National Occupational Employment and Wage Estimates, United States.

A review of the U.S. Bureau of Labor categories of occupations involved in the manufacturing sector listed in Table 1 reveals that *in 2019, 49% of all employees classified as working for a manufacturing firm (and thus counted in "manufacturing sector" employment) actually held services occupations.*[8] *Moreover, 13 of these services occupations pay wages that would put families of the job holder in the middle class, as defined by Pew Research Center, and four of them are available to individuals with only a high school education.*[9]

### American Workers Need Training to Take Advantage of New Services and Digital Jobs

**2/3**

Share of new jobs created over the last 10 years that required digital skills.

Many of the services jobs that are being created require digital skills. Over the last decade, two-thirds of the 13 million U.S. jobs created required medium to advanced levels of digital skills.[10]

As the American Leadership Initiative recently noted, a large number of jobs available before the pandemic were unfilled because workers did not have the digital skills needed.[11] Many services and digital trade firms have already implemented programs to train high-school graduates and re-skill workers for career-track jobs in the services sector. More must be done, with government in partnership, to expand worker training and re-skilling programs that connect high school graduates and unemployed or underemployed Americans to well-paying, 21st century jobs.

## Services and Digital Sectors Make U.S. Manufacturing and Small Businesses More Competitive

### Services Support the Competitiveness of U.S. Manufacturing

Services are essential to the competitiveness of American manufacturers. As advances in information technology accelerate, U.S. manufacturers are using services – notably digitally-enabled products and services – not only to make products (e.g., through automation and robotics) but also to better differentiate and customize their offerings. An International Trade Commission survey of research found that access to a wide variety of high-quality services promotes manufacturing competitiveness: "[p]roducts that make greater use of services inputs exhibit higher product quality and higher export prices."[12]

For example, GM offers OnStar Guardian customer support in many of its vehicles as a premium feature. Semiconductor chip manufacturers use "big data" analytics to estimate the performance of a range of product variations.[13] Software enabled services help medical device manufacturers with "each step of the value chain, from designing a new product to helping firms comply with regulations."[14]

---

8 Calculated by The Trade Partnership from data in Table 1.

9 *Ibid*.

10 American Leadership Initiative, *A Global Digital Strategy for America*, February 2021, p. 9.

11 *Ibid*., p. 10.

12 *Ibid*., p. 3-14.

13 U.S. International Trade Commission, *Economic Effects of Significant U.S. Import Restraints*, Eighth Update 2012, Special Topic: Services' Contribution to Manufacturing, Inv. No. 332-325, December 2013, p. 3-7.

14 *Ibid*.

### Services Support the Competitiveness of U.S. Small Businesses

**90%**

Share of total minority-owned small businesses that are services firms.

Digital tools are also increasingly enabling small businesses to export. Particularly during the pandemic, internet platforms afforded small businesses new opportunities to offer their goods and services globally, and software and services enabled small businesses to operate more competitively and efficiently. A study that surveyed U.S. small businesses found that 92% that export use digital tools such as online payment processing tools, online productivity tools, e-commerce websites, online marketing and other tools.[15] That same study found that exporting accounts for a growing share of small business services firms' revenues, reaching 25% in 2018, and nearly 6 million export-related jobs nationally.

Though small businesses tend to be short on financial resources and international sales experience, digital tools can help them gain access to new foreign markets. This is important to consider amid efforts to address economic and racial inequality: in 2018, 90% of all minority-owned small businesses were services firms.[16]

## Services and Digital Trade Providers Are Key Partners in Efforts to End the Pandemic, Address Environmental Issues and Advance Racial Equity and Underserved Communities

In addition to helping the Administration grow high-quality jobs in all sectors of the U.S. economy, a partnership with services and digital trade providers will help the Biden administration reach its goals of getting past the pandemic, addressing environmental issues, and advancing racial equity and underserved communities. Services and digital trade providers are already active on these issues.

### Services and Digital Trade Providers Stepped Up to Get the Economy Moving during the Pandemic

Services helped the U.S. economy stay resilient in the face of sudden, severe disruptions from the pandemic.

- Millions of workers had to figure out ways to work or go to school from home, and the internet and other digital services made that possible.
- Digital services also enabled hundreds of thousands of small businesses to become digital virtually overnight, sustaining their businesses through the pandemic. One-third of small businesses state that they would not have survived the pandemic without access to digital tools.[17]

---

15 United States Chamber of Commerce and Google, *Growing Small Business Exports: How Technology Strengthens American Trade*, October 2019.

16 Excludes "construction" from "services." U.S. Census Bureau, "Annual Business Survey: Employment Size of Firm Statistics for Employer Firms by Sector, Sex, Ethnicity, Race, and Veteran Status for the U.S., States and Metro Areas: 2018."

17 Connected Commerce Council, "Digitally Empowered."

- Financial services firms made it possible for people to bank from home at the same time banks developed new digital technologies to assist the unbanked. They also supported thousands of companies in getting PPP loans.
- Digitally connected supply chains eventually enabled manufacturers to restock their customers. Transportation and warehouse workers kept supplies moving, particularly of PPE goods needed to fight the pandemic.
- Cross-border sharing of research and data supported the development of vaccines. The health care industry pivoted to telemedicine.
- Some service sectors were declared "essential" and allowed to continue operating outside the quarantine restrictions, including transportation and construction.

Services are also key to getting the U.S. past the pandemic in the months ahead, helping accelerate a recovery.

## Services and Digital Trade Providers Are Partners in Addressing Environmental Issues

U.S. environmental services and technologies are world class and have a critical role to play in combatting climate change. Digital technologies such as cloud services are already fundamental to promoting more sustainable forms of agriculture. Farmers are using artificial intelligence and machine learning to track supplies, use appropriate levels of inputs like fertilizers and water, and increase yields in environmentally sustainable ways. For example, some farm tractors come equipped with soil probes and sensors that send information to an online portal which aggregates the tractor's data with other data, helping farmers to better plan and manage resources in environmentally responsible ways.[18]

Others are seeking to lower their carbon footprint. A leading technology company is using a combination of artificial intelligence, hybrid cloud and quantum computing to apply science to complex climate-related problems, such as the growing global carbon footprint of cloud workloads and data centers, methods to accurately model and assess the risk of changing environments and climate patterns, and the development of new polymers, membranes and materials that can capture and absorb carbon at the origin of emission.[19]

Finally, AI can help support more sustainable harvesting practices. Studies show that 90% of major fish stocks globally are either overfished or fully exploited – which is a trade problem in a world where over 3 billion people rely on fish for their main protein. Global negotiations on fishery subsidies are underway at the World Trade Organization, but with over 200,000 commercial fishing vessels around the world, there is a need to promote responsible fishing on a cross-border basis. Through a partnership with another leading technology company, two NGOs developed a tool called Global Fishing Watch to apply a data-driven approach to the issue of overfishing.[20] These researchers apply AI to publicly available broadcast signals from commercial vessels to detect "zigzag" patterns associated with fishing vessels, and then follow these vessels on a public map to understand when and where they are fishing.

---

18 Ofir Schlam, "4 ways big data analytics are transforming agriculture," July 15, 2019.

19 IBM, "IBM Commits To Net Zero Greenhouse Gas Emissions by 2030," Press Release, February 16, 2021.

20 Google, "Oceans of data: tracking illegal fishing over 1.4 billion square miles," September 2018

### *Services and Digital Trade Firms Are Focused on Advancing Racial Equity and Underserved Communities*

As major employers of people of color, services and digital trade providers have an important role to play in overcoming racial inequities that stand in the way of access to good jobs, financial resources, education and healthcare. Indeed, many have already announced new initiatives, including efforts to:[21]

- Provide greater access to low-cost financial products to help those who do not use banks or do not use them effectively, and expand their access to credit to start or build new businesses.
- Expand access to digital services like speedy and reliable connection to the internet, in particular for those living in rural areas, older workers, and African Americans, Hispanics, and other underserved communities.
- Provide training that workers of the future will need to excel in the jobs of the future, which will increasingly be technology-intensive. Numerous leading services and digital trade firms already have and are enhancing firm apprentice programs and offering college tuition support, for example.[22] As suggested by the American Leadership Initiative, new public-private partnerships will be necessary to do more.
- Promote diversity in services firms' supply chains.[23]

## To Remain Competitive and Create Good U.S. Jobs, Services and Digital Firms Need Expanding Trade and Investment

Expanding U.S. services and digital trade and investment will enable U.S. services and digital sectors to remain competitive and strengthen the American middle class by providing a source of high-wage jobs. U.S. services and digital trade firms and workers need a global customer base that provides growing demand for new products and services. They sell to these customers through exports as well as through in-country investments. As explained below, while the cross-border exports of banking and insurance firms are limited pursuant to regulatory requirements, finance firms engaged in global securities trading are also among the largest exporters of services from the United States.

Millions of jobs are at stake. More than 4 million American jobs were tied to services exports in 2016,[24] with up to 2.4 million U.S. jobs linked to digital trade.[25] Every billion dollars of services exports supports over 6,700 jobs.[26]

---

[21] Microsoft is implementing programs that address several of the initiatives listed below. See "New ideas and energized employees fuel Microsoft's ongoing efforts toward racial equity," March 10, 2021.

[22] For example, the Entertainment Software Association is working with Black Girls CODE to teach coding and technology skills to 1 million girls and young women by 2040. Entertainment Software Association, "The Entertainment Software Association Announces $1 Million Initiative to Support Black Girls Code Through Its Philanthropic Foundation."

[23] Two examples of many are MetLife's *2019 Sustainability Report*, and FedEx, "Diversity & inclusion: Our values in Action."

[24] Chris Rasmussen, "Jobs Supported by Exports 2016: An Update," U.S. Department of Commerce, August 2, 2017.

[25] Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, The Brookings Institution, Working Paper 79, October 2014.

[26] Rasmussen, *op. cit*.

U.S. exports of digital services have surpassed $500 billion, accounting for more than half of all U.S. service exports and generating a U.S. digital trade surplus in excess of $200 billion.[27] Likewise, U.S. exports of aircraft, automobiles, machinery, telecommunication equipment and other connected devices that incorporate significant services functionality exceed $500 billion. Digital services play a major role in supporting commerce in all sectors: Over 75 percent of the value of cross-border data transfers accrues to industries like agriculture, manufacturing, and logistics.[28]

Digital services support millions of American jobs. For example, software alone supports over 14 million American jobs[29] – jobs that not only pay more than twice the average annual wage for all U.S. occupations, but also are often accessible without a costly four-year college degree. As a dynamic and innovative economy, the United States is primed for continued growth in these strategic export sectors. With over 1 million software and digital jobs[30] across manufacturing and service facilities going unfilled across the country, there is continued room to grow the economy through digital services trade.

## Services Exports Matter to High-Wage Jobs, Manufacturing

**+18%**

How much extra blue-collar workers in services exporting firms earn compared to non-exporting firms.

### *Services Firms That Export Pay Higher Wages to both Blue- and White-Collar Workers*

Export-intensive services firms pay higher wages than services firms that are not export intensive. Workers at export-intensive services firms earn 15.5% more than workers in other services firms. The wage premium is even stronger for blue-collar workers: they earn 18% more than their white-collar colleagues (12.0%).[31]

### *U.S. Data Understates the Value of Services Exports and Importance to Manufacturing*

The low levels of U.S. direct services exports compared to goods exports greatly understates the actual level of services trade flows to global markets. This is due to the poor quality of services data: U.S. goods exports contain a large percentage of services input that has only recently begun to be tracked by BEA and the OECD. As a result, the positive impacts of the U.S. services sector on jobs and wages, particularly in manufacturing, is not sufficiently recognized (see the Appendix for a discussion of some of these data issues).

In fact, services and digital trade exports matter to U.S. manufacturers and their workers. U.S. manufacturing firms (particularly chemical manufacturers and computer and electronics parts manufacturers) are among the largest exporters of services (primarily income they receive for

---

27 United States, Congress, House Digital Trade Caucus co-chairs letter to Ambassador Katherine Tai, March 29, 2021, https://insidetrade.com/sites/insidetrade.com/files/documents/2021/mar/wto2021_0148a.pdf

28 Global Data Alliance, Facts and Figures, accessed April 8, 2021, https://globaldataalliance.org/downloads/gdafactsandfigures.pdf

29 "Software: Growing US Jobs and the GDP," Software.org, BSA Foundation, accessed April 8, 2021, https://software.org/wp-content/uploads/

30 "A Policy Agenda to Build Tomorrow's Workforce," BSA, accessed April 8, 2021, https://www.bsa.org/files/policy-filings/05022018BSAWorkforceDevelopmentAgenda.pdf

31 David Riker, "Export-Intensive Industries Pay More on Average: An Update," U.S. International Trade Commission, Office of Economic Research Note, No. 2015-04A, April 2015.

use of intellectual property, R&D and consulting services).[32] The incorporation of services with finished advanced manufactured goods makes those products highly sought after by global customers and enables manufacturers to charge higher prices, and represents indirect, and unmeasured, exports of services.

## Services Investment Supports U.S. Jobs and Growth

### *Inbound and Outbound Services Investment Supports U.S. Jobs*

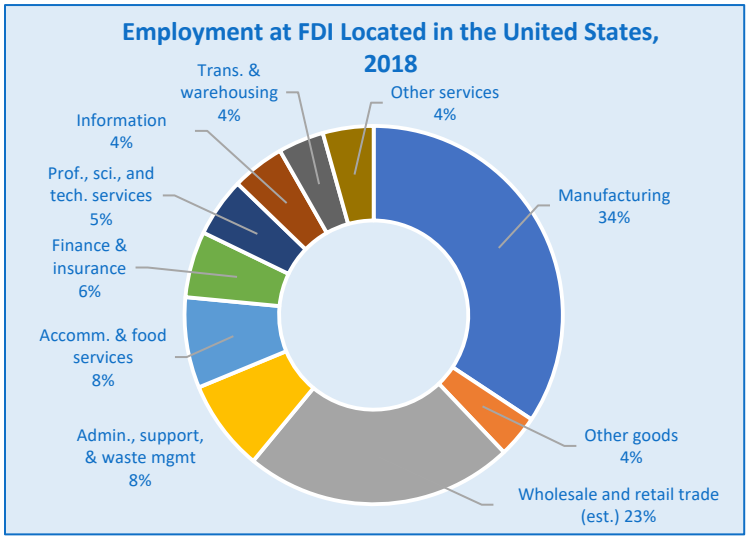
Foreign services firms account for

**62%**

Of U.S. FDI employment.

Services investments, both inbound and outbound, are a growing source of American middleclass jobs. Foreign services firms employed 8.6 million workers in the United States in 2018--more than 62% of all workers employed by foreign firms located in the United States that year. Inbound investment in services sectors grew at an average annual rate of 6% from 2015-2018.[33]

These are high-paying jobs. Compensation per employee in 2018 placed such workers well into the American middle class: finance and insurance, $199,107; company management, $126,970; professional, scientific, and technical services, $120,279; information services, $94,823; real estate and rental and leasing, $87,851; health care and social assistance, $62,199; and transportation and warehousing, $55,656.




Source: Bureau of Economic Analysis, "Foreign Direct Investment in the U.S., All U.S. Affiliates."

Research into the U.S. employment (and other) impacts of outward U.S. investment has concluded that U.S. foreign affiliate activity tends to complement, not substitute, for U.S. activity, including employment. The global work of American multinational companies is concentrated in the United States, not in their affiliates abroad. More company-wide employment is located in the United States – i.e., 2.2 employees for every one foreign employee.[34]

For example, industry experts estimate that more than 32,000 domestic jobs are created as a result of international property and casualty insurance trade, resulting in more than $3 billion in U.S. payroll and employment benefits. That payroll, in turn, produces hundreds of millions of dollars in federal, state, and local payroll and sales taxes for the U.S. economy.[35] By expanding

---

32 Jennifer Bruner and Alexis Grimm, "A Profile of U.S. Exporters and Importers of Services, 2017," *Survey of Current Business*, December 2019.

33 Based on data for seven services sectors for which a complete time series were available for the 2015-2018 period. 2018 is the latest year data are available. Bureau of Economic Analysis, "Foreign Direct Investment in the U.S., All U.S. Affiliates."

34 Matthew J. Slaughter, "How U.S. Multinational Companies Strengthen the U.S. Economy: Data Update," prepared for Business Roundtable and United States Council for International Business, March 2010.

35 American Property and Casualty Insurance Association, unpublished data.

sales for U.S. services (and other sectors) through foreign affiliate sales, U.S. parent companies can increase employment in the United States.

Finally, U.S. foreign direct investment enhances U.S. influence abroad in promoting American values such as rule of law, greater transparency, and respect for human rights and the environment.

### *Foreign Investment Plays a Much Greater Role Than Exports in Generating Services Sector Growth*

Despite the growing importance of digitally enabled cross-border services trade, the primary means for the global supply of services is investment. In 2018, two-thirds ($1.7 trillion) of U.S. sales of services to foreign customers were supplied by U.S. services companies through their foreign affiliates; one-third were supplied through cross-border exports.[36]


This reliance on foreign investment is due to several factors. First, and perhaps most important: many services such as financial services, telecommunications, and to a lesser extent, professional services are heavily regulated in most countries. For example, financial services are subject to local prudential and other regulatory requirements such as establishment of legal presence, investment of capital assets, and local licensing in order to supply a service in a local market. Such requirements can only be fulfilled by local establishment.

Second, the provision of many services requires proximity to local customers to make sales and provide ongoing customer service and after sales services. Retail or wholesale distribution services and logistics are both examples of services that require in-country presence and proximity to customers. In the case of retail, while online shopping has become widespread, a brick-and-mortar presence in local markets as well as online, referred to as an "omni-channel" model, is still often preferred by local customers and local establishment may also be required by regulators.

### Services Trade and Investment Commitments Impact Direct Services Exports

While the market access commitments under the World Trade Organization (WTO) General Agreement on Trade in Services (GATS) and U.S. free trade agreements (FTAs) provide for some opening in foreign markets, these multilateral and bilateral agreements do not eliminate all services trade restrictions, particularly with respect to cross-border trade. Furthermore, GATS services market access commitments are particularly weak as they are based on a "positive list" approach in which WTO members are only required to provide market access in those sectors and modes of services supply where they choose to do so. Thus, out of the 160 possible

[36] Bureau of Economic Analysis, "International Services (Expanded Detail)."

services sub-sectors in which services commitments can be made, the average number of sectors covered in WTO members' GATS schedules is only 55.[37]

In addition, in the case of financial services, cross-border commitments in banking and insurance are specifically limited and thus only a relatively narrow sliver of the services in those sectors are exported. During the WTO Uruguay Round Financial Services negotiations, a group of WTO members developed the Understanding on Commitments in Financial Services (Understanding) which was intended to be a model for how WTO members should schedule their financial services commitments.[38] The Understanding provides a closed list of specific insurance and banking sector services that should be subject to WTO member cross-border commitments. Pursuant to the Understanding, in the banking sector cross-border commitments should be made only with regard to transfer of information, information processing and advisory services. In insurance, the Understanding limited cross-border commitments to marine, aviation and transportation insurance, goods in-transit, reinsurance and retrocession, and services auxiliary to insurance. The United States and many other WTO members, particularly developed countries, incorporated the practice of limiting financial services cross-border commitments to the specific lists provided in the Understanding in their FTAs.[39] In U.S. FTAs , these cross-border financial services commitments have been broadened to include portfolio management and electronic payment services, but they still remain relatively narrow. The ITC found that U.S. property and casualty insurance exports would increase by 48% if all of the examined countries were to fully liberalize cross-border insurance trade rules, and U.S.-based jobs would increase.[40]

### Services and Digital Trade and Investment Barriers Are Increasing

A robust U.S. trade agenda for services and digital trade is especially important now because foreign barriers to services and digital trade and investment are increasing. The Organization for Economic Cooperation and Development found that the services regulatory environment, particularly for foreign investment, became more restrictive in 2020 and the pace of tightening has accelerated.[41] Digital fragmentation is on the rise: as the OECD recognized, "rules and regulations remain fragmented by borders," and the resulting "regulatory divergences" are raising cross-border costs "as activities need to be aligned across multiple regulatory frameworks."[42]

These barriers negatively impact not only services and digital trade providers and their U.S. workforce, but the range of other U.S. industries that are integrated with them, notably manufacturing. The ITC found that by reducing costs and increasing the variety of services available to U.S. manufacturers, services liberalization could serve as "an important component

---

37 World Trade Organization, *Trade in Services Rules To Consider*, February 20, 2019; A. Breckenridge, *GATS: The WTO Framework for Services*, Trade Knowledge Framework,(2018); Thornberg and Edwards, "Failure of Trade Liberalization: A Study of the GATS Negotiation," *Journal of International Business and Law*, Volume 10/Issue 2 (2011).

38 World Trade Organization, *Understanding on Commitments in Financial Services*, 1999.

39 U.S.-Mexico-Canada Agreement, Chapter 17, "Financial Services;" Annex 17-A, "Cross-Border Trade."

40 U.S. International Trade Commission, *Property and Casualty Insurance Services: Competitive Conditions in Foreign Markets*, Inv. No. 332-499, March 2009.

41 Organization for Economic Cooperation and Development, *OECD Services Trade Restrictiveness Index: Policy trends up to 2021*, February 2021.

42 Organization for Economic Cooperation and Development, *op. cit*

of efforts to boost manufacturing competitiveness," in particular for motor vehicles.[43] They also impact the success of the Administration's efforts to get past the pandemic and address climate issues. Many of these growing barriers interfere with the efficient global development of vaccines to treat the coronavirus and other deadly diseases. Tariffs on goods and regulatory and other restrictions on environmental services make addressing climate change costlier around the world, and in particular the development of new services and technologies that get economies to net zero carbon emissions.

## Conclusion

CSI members support efforts to increase middle class jobs, particularly for communities left behind, to recover from the pandemic, to address environmental issues and climate change, and to promote inclusive prosperity for all segments of the workforce. To do this, however, we need the Administration's assistance in accessing global markets for American services and digital trade products. Such access makes our firms and workers globally competitive and better able to develop the innovative products and services that will employ more workers at higher wages in the United States.

[43] ITC, op. cit., p. 3-14-15.

# Appendix

## Services and Digital Trade Data Significantly Understate the Importance of that Trade to the American Economy

It is widely acknowledged that official government data reporting U.S. exports, imports and investment related to services and digital trade is incomplete and dated. It does not measure all the ways in which services from the United States cross borders or U.S. services traded between domestic and foreign affiliates impact U.S. operations and employment. As such, it significantly understates the importance of that trade to the American economy.

An assessment by McKinsey Global Institute of just three deficiencies in services and digital trade data collection demonstrates that, if those deficiencies were corrected, the value of services and digital trade would be considerably greater than policy makers currently believe.[44] Globally, McKinsey concluded that if three additional channels for services delivery were counted, **the total value of services trade flows would exceed that for goods**.

According to McKinsey:

- Trade statistics do not fully report the value of services that go into the production of traded goods, such as design, marketing, R&D, and other types of intellectual property. This services value is largely counted in the value of goods exports in official government trade data. These "hidden" services exports amount to a lot. When value added trade data are used, one finds that services represent 31% of the value of goods trade (2014).
- Intangibles like design, brands, software, organizational capital, and training for example, are increasingly important features of traded goods, but they are hard to measure and not always reported in trade data as such if they do not cross borders as discrete transactions (a growing exception is when intangibles are patented or trademarked and recognized as royalty payments in services trade data). McKinsey estimated that if these services were captured in trade data, they would cut the U.S. trade deficit by almost one third.
- Free digital services like email, social media, mapping and search engines are not counted in statistics. McKinsey estimated the estimated value of free services could add as much as $3.2 trillion to global trade in services.

Again, these are just three of the problems with services and digital trade data. Statisticians are aware of many more and are expanding their data coverage little by little, as their budget resources allow and as they are able to overcome measurement and data collection roadblocks. But we have a long way to go. In the interim, policy makers should not underestimate the value of international services and digital trade, and the potential benefits of increasing that trade and investment through trade policies, judging from its size relative to goods trade as currently reported in official statistics.

---

[44] The estimates that follow are from McKinsey Global Institute, McKinsey & Company, *Globalization in Transition: The Future of Trade and Value Chains*, January 2019, Chapter 2.

# EXHIBIT 24

# *White Paper 2:*
# *Addressing Foreign Services Trade and Investment Barriers Benefits American Workers and Must Remain a Priority*

## Past Liberalization of Services and Investment Barriers Has Been Good for American Workers

U.S. free trade agreements (FTAs) have covered services since the U.S.-Israel Free Trade Agreement. Over time, the scope and sophistication of that coverage has expanded to reflect economic, environmental and technological developments. Provisions affecting digital trade have been included in all U.S. FTAs since the agreement with Jordan.

These services provisions of U.S. FTAs have been good for American workers. A 2021 ITC study found that U.S. bilateral or regional FTAs have had a net positive impact on services sector output and jobs. As a result of increases in U.S. output, FTAs expanded U.S. employment in services sectors covered by FTAs by a net of 323,970 workers, the most of any sector. [1] Workers in other services sectors (those not directly affected by provisions in FTAs, like construction) also benefited from FTA-related increases in U.S. output, by 121,520 jobs.[2] About 82,000 of these jobs were held by workers with up to a high school level of education.[3]

**+324,000**

Increase in U.S services sector employment as a result of U.S. FTAs

U.S. trade agreements recognize the importance of giving domestic regulators at the national, state and local levels the discretion to implement legitimate public policy objectives through domestic regulation. Recognition of the right to regulate is a core principle of U.S. FTAs and is noted in the Preamble to the General Agreement on Trade in Services (GATS). Pursuing new services trade liberalizing opportunities does not undermine this regulatory prerogative. Indeed, for example, provisions should be included that ensure that parties can protect consumers from fraud and deception when they engage in digital trade, and that their personal data and privacy are protected.

---

[1] United States International Trade Commission, *Economic Impact of Trade Agreements Implemented under Trade Authorities Procedures, 2021 Report*, p. 100. Due to historical data constraints, the ITC did not consider the impacts of the Uruguay Round Agreements, the U.S.-Israel FTA, nor the U.S.-Mexico-Canada Agreement as it had only recently gone into effect.

[2] United States International Trade Commission, *Economic Impact of Trade Agreements Implemented under Trade Authorities Procedures, 2021 Report*, p. 100.

[3] United States International Trade Commission, *Economic Impact of Trade Agreements Implemented under Trade Authorities Procedures, 2021 Report*, p. 103.

## A Rising Tide of Services and Digital Trade Barriers Threatens These Benefits

A robust U.S. trade agenda for services and digital trade is especially important now because foreign barriers to services and digital trade and investment are increasing. These barriers disadvantage not only U.S. services sector workers, but also American manufacturing workers and those employed by small- and medium-sized firms. The Organization for Economic Cooperation and Development found that the services regulatory environment, particularly for foreign investment, became more restrictive in 2020 and the pace of tightening has accelerated.[4] The Information Technology and Innovation Foundation found that the number of countries that have enacted data localization requirements has nearly doubled from 35 in 2017 to 62 in 2021.[5]

### Core Principles for Digital Trade Agreements

1 Prohibit digital customs duties
2 Secure basic non-discrimination principles
3 Expand market access for investment and cross-border services, including those delivered digitally
4 Enable cross-border data flows
5 Prevent localization barriers
6 Ban forced tech transfers and protect critical source code and algorithms
7 Foster innovative encryption products
8 Ensure technology choice
9 Promote a free and open Internet
10 Support data innovation
11 Advance strong and balanced protection of IP rights
12 Promote transparency and stakeholder participation in the development of regulations and standards
13 Encourage exports of goods sold online with higher tax-free and tariff-free thresholds
14 Advance innovative authentication methods
15 Enable paperless trade
16 Require cross-border interoperability of e-invoicing systems
17 Enhance secure and interoperable e-payment systems
18 Foster digital trade through international standards
19 Deliver enforceable consumer protection
20 Ensure adequate protection of personal data
21 Promote cooperation on cybersecurity
22 Create a safe online environment
23 Develop ethical and government frameworks for the use of AI technologies
24 Increase trade and investment opportunities for SMEs and create jobs for workers
25 Increase access to retraining and digital skills
26 Cooperate on digital capacity building
27 Encourage recognition of labor rights
28 Recognize digital inclusion as a driver of economic and social development
29 Ensure mutual recognition of digital identities
30 Promote equality of opportunity in digital economies

The United States needs to lead global efforts to remove these costly barriers to services and digital trade. For trade policy to align with the realities of today's services trade, the Administration's agenda should include a commitment to update World Trade Organization (WTO) General Agreement on Trade in Services (GATS) by expanding services market access commitments and adopting strong rules on digital trade, whether that takes place multilaterally through WTO e-commerce negotiations, regionally through an Asia-Pacific digital-trade agreement, another form of trade pact, or some combination of these. "Advancing U.S. digital governance, which promotes democracy, rule of law, and transparency in the region, is a key part of a global strategy to counter China, as well as to expand U.S. markets to support U.S. workers," concluded an American Leadership Initiative

[4]Organization for Economic Cooperation and Development, *OECD Services Trade Restrictiveness Index: Policy trends up to 2021*, February 2021.
[5] Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, p.3.

report highlighting the benefits of a Pacific Digital Agreement.[6]

**The world is not waiting for us.** For example, Singapore and Australia signed a digital economy agreement in 2020, and Singapore, New Zealand and Chile signed the Digital Economy Partnership Agreement, also in 2020; Korea plans to join this agreement. The European Union plans to seek digital partnership agreements with Japan, Korea and Singapore as part of its Indo-Pacific strategy. These agreements would set interoperability of standards for emerging technologies like artificial intelligence that will influence supply chains for years to come.

**A trade deal would align with administration China policy.** A high-standard trade agreement on services and digital trade in the Asia-Pacific would strengthen ties with allies and complement the Biden-Harris administration's foreign policy objectives. By codifying rules to create an open and non-discriminatory framework for digital commerce, the United States would help protect what has essentially become critical infrastructure for global trade.

Services and digital trade are also central to supporting manufacturing and maintaining U.S. economic competitiveness. By reducing trade barriers and streamlining access to digital goods and services – including e-payments and financing -- a high-standard agreement would aid the small businesses that typically have more trouble navigating overseas markets.

## Reducing Services Trade and Investment Barriers Benefits American Workers

As U.S. services and digital trade grows with the elimination of foreign barriers, the number of these good jobs can be expected to increase, with positive ripple effects through the economy. A $1 million increase in final demand for professional, scientific and technical services generates 4.3 direct jobs and another 15.3 indirect jobs throughout the economy; management of companies, 3.6 direct and 12.4 indirect; finance and insurance, 2.0 direct and 10.8 indirect, and information, 2.0 direct and 10.9 indirect.[7]

---

[6] *American Leadership Initiative, Next Steps for U.S. Digital Leadership: Advancing Digital Governance with the Pacific and Europe*, July 2021, p. 9.

[7] Josh Bivens, Economic Policy Institute, "Updated Employment Multipliers for the U.S. Economy," Table 2, January 23, 2019, https://www.epi.org/publication/updated-employment-multipliers-for-the-u-s-economy/?fbclid=IwAR3ZC293MrtIq2z_4T40uJtCEXCkh21gn_HEheq-rQaSjxxbSo8GVWe3gwA,

**It helps workers earning middle class wages, many with no college degrees.** U.S. Government 2019 employment data show that firms employed nearly 52 million workers in services occupations earning middle class wages as defined by Pew Research Center.[8] Most American households today "sustain a middle-class living through work in areas outside manufacturing, especially in services sectors where the United States has comparative advantages."[9] An increase in services exports expands these job opportunities for American workers.

**52 million**

Workers in services occupations earning middle class salaries

At the same time, U.S. companies and government must coordinate to expand training and reskilling programs, so American workers can take better advantage of new opportunities in overseas markets. To learn more about work force development programs in the services and digital trade industries, read CSI paper here.

**It helps manufacturing workers.** The benefits of reducing trade and investment barriers accrue not just to services sector workers, but in those in manufacturing as well. U.S. manufacturers have historically relied on services such as finance, marketing, payments, insurance, logistics, and distribution to produce and ship their products to international markets, all of which are now digitally enabled in important ways. In addition, with the growing availability of digital services, manufacturers have come to rely even more on services in the form of e-payments, social media-based marketing and cloud storage, to take a few examples. The ITC found that by reducing costs and increasing the variety of services available to U.S. manufacturers, services trade liberalization could serve as "an important component of efforts to boost manufacturing competitiveness," in particular for motor vehicles.[10]

**It helps blue-collar workers.** Export-intensive services firms pay higher wages than services firms that are not export intensive. Workers at export-intensive services firms earn 15.5% more than workers in other services firms. The wage premium is even stronger for blue-collar workers: they earn 18% more than their white-collar colleagues (12.0%).[11] An expansion of services trade flowing from barrier reduction increases job opportunities for these workers.

**+18%**

How much extra blue-collar workers in services exporting firms earn compared to non-exporting firms.

**It helps women and minority workers.** Women account for 53% of all private sector services jobs.[12] Minorities account for 29% of total private sector services

---

[8] Bureau of Labor Statistics, Employment Projections program, Table 1.1, "Employment by Major Occupational Group, 2019 and Projected 2029," and Pew Research Center, "Are You in the American Middle Class? Find Out with Our Income Calculator," Factank, July 23, 2020. Pew defines the middle class in 2018 as three-person households earning between $48,500 and $145,500.

[9] Carnegie Endowment for International Peace, Making U.S. Foreign Policy Work Better for the American Middle Class, September 23, 2020.

[10] ITC, op. cit., p. 3-14-15.

[11] David Riker, "Export-Intensive Industries Pay More on Average: An Update," U.S. International Trade Commission, Office of Economic Research Note, No. 2015-04A, April 2015.

[12] Bureau of Labor Statistics, 2020 data extracted September 13, 2021, https://www.bls.gov/ces/data/.

employment.[13] An expansion of U.S. services output related to the reduction or elimination of foreign barriers to U.S. services exports will have a positive impact on these workers.

**It helps small businesses.** Digital tools increasingly enable small businesses to export. Internet platforms afford small businesses new opportunities to offer their goods and services globally, and software and services enable small businesses to operate more competitively and efficiently. The challenges imposed by barriers to services trade are especially acute for smaller firms. In a national survey of over 3,800 small companies, small business owners listed their top export barriers as foreign regulations (such as taxes, data localization requirements, privacy rules, and liability risks), tariffs and customs procedures, payment collection, company resources, and risk and infrastructure.[14] That study estimated that improving market access would boost small business sales abroad by over 14% over the ensuing three years. That would in turn increase U.S. economic output by $81 billion and add 900,000 American jobs.

**90%**

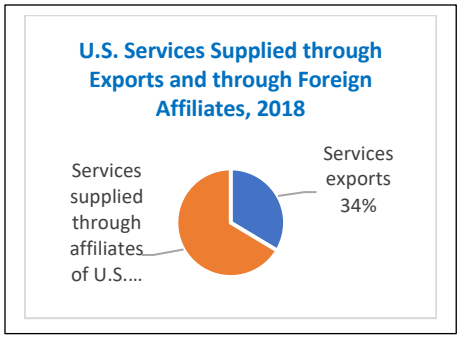
Share of total minority-owned small businesses that are services firms

## Addressing Trade Barriers Will Not Promote Offshoring and a "Race to the Bottom"

Decisions by U.S. services firms on where to locate their operations and how to access foreign markets differ from their manufacturing counterparts in several respects. First, many services sectors such as financial services, telecommunications, and some professional services, are heavily regulated and therefore are required to establish a presence in foreign markets in order to offer their services there. Second, many of these services as well as others such as distribution and transportation must be close to their customers in order to provide them with services and must therefore have foreign affiliates to operate in foreign markets. In 2018, two-thirds of the value of services provided internationally by U.S. firms was delivered through U.S. affiliates located abroad.[15] Nearly three-quarters of that investment was located in developed markets.[16]

---

[13] Bureau of Labor Statistics, 2019 data extracted September 13, 2021, https://www.bls.gov/cps/demographics.htm#race.
[14] U.S. Chamber of Commerce and Google, *Growing Small Business Exports: How Technology Strengthens American Trade*, 2019, p. 8.
[15] Shari A. Allen, Alexis N. Grimm, Christopher Paul Steiner, and Rudy Telles Jr., "Trade in Services in 2019 and Services Supplied Through Affiliates in 2018," *Survey of Current Business*, October 2020, https://apps.bea.gov/scb/2020/10-october/1020-international-services.htm.
[16] Bureau of Economic Analysis, "Balance of Payments and Direct Investment Position Data, 12019," extracted September 14, 2021.




Establishing abroad in order to meet local regulatory requirements and to meet customer needs in person does not come at the expense of U.S. workers. In fact, services providers operating through investments in foreign markets employed more than 20 million workers at headquarters and other U.S.-based locations to support these foreign operations.[17] The global work of American multinational companies is concentrated in the United States, not in their affiliates abroad. For example, industry experts estimate that more than 32,000 domestic jobs are created as a result of international property and casualty insurance trade, resulting in more than $3 billion in U.S. payroll and employment benefits. That payroll, in turn, produces hundreds of millions of dollars in federal, state, and local payroll and sales taxes for the U.S. economy.[18] By expanding sales for U.S. services (and other sectors) through foreign affiliate sales, U.S. parent companies can increase employment in the United States.

Trade agreements can eliminate barriers that force companies to set up operations in foreign countries to have a commercial presence. For example, elimination of requirements that telecom/media services require a commercial presence could drive more of those services to be delivered as exports from the United States.[19]

## Conclusion

In conclusion, a substantial body of U.S. government research has documented the benefits that accrue to U.S. workers from expanded services trade and investment commitments. Liberalized services trade has been shown to boost U.S. employment, while blue-collar workers in export-oriented services jobs earn higher wages. A reduction in trade barriers would also benefit small business through expanded export opportunities. Amid a growing wave of protectionism in foreign markets, there is a compelling rationale for the U.S. to pursue an ambitious services and digital trade agenda.

[17] Bureau of Economic Analysis, "Selected Operating and Financial Data of U.S. Parents, by Industry of U.S. Parent, 2018," extracted September 14, 2021.

[18] American Property and Casualty Insurance Association, unpublished data.

[19] However, not all "offshored" jobs can be brought back to the United States. Some U.S. workers have little interest in doing some of these jobs; others would more likely be performed by local workers in any event.

# EXHIBIT 25

## CSI Member

# *Services and Digital Trade*
# *Workforce Development Programs*

As services and other jobs increasingly demand a high level of professional skills and digital literacy, both government and industry must do more to equip individual workers with the requisite training. The success of individual American workers and U.S. global competitiveness are closely intertwined.

A study by Brookings found that nearly two thirds of the new jobs created between 2010 and 2016 required at least a moderate level of digital skills. [1] The same report found that nearly a quarter of workers were already engaged in occupations with a high level of digital content. It also concluded that holding education constant, workers with better digital skills tended to earn higher wages than those with lower skills.

Government and companies should collaborate to improve education and training programs. Below we offer examples of how CSI members are upskilling workers and helping them prepare for more professionally intensive and digitally demanding work.

- **IBM**

IBM's **"new collar" initiative** is a pioneering registered apprenticeship program established in 2017. IBM coined the term "new collar" jobs to describe in-demand, well-paying roles where skills matter more than having specific degrees. In the last five years, new collar IBMers have accounted for around 15 percent of the company's total annual U.S. hiring.

The new collar initiative is based on IBM's existing **P—TECH** program, which started in 2011. P-TECH enables students to earn both their high school diploma and a two–year associate degree linked to growing, competitive STEM fields. The program has expanded over time to encompass 600 industry partners and 260 school partners, and now operates in 26 countries.

The P-TECH education model has five key elements:
• Open enrollment – no testing for admission, with a focus on underserved communities, cost-free (including degree, textbooks, and transportation)
• Mentors for all students from the employer partners
• Alignment of the program of study for grades 9-14 with the skills needed by an employer – which has helped the program become a common pathway for students to obtain subsequent STEM degrees and certifications
• Seamless pathway – considered part of the college community as soon as a student starts at P-TECH, without obstacles such as college admissions requirements, SAT tests, or FAFSA applications
• Paid internships for students from the employer – Community college education is embedded directly into the fabric of the P-TECH model, because it serves as an accelerator that can propel students into well-paying careers as well as a launch pad toward a bachelor's degree.

---

[1] Mark Muro, Sifan Liu, Jacob Whiton, and Siddharth Kulkarni, Brookings, *Digitalization and the American Work Force*, November 15, 2017, p. 15.

IBM also offers free, digital learning through **Open P-TECH**, which introduces students and educators to emerging technologies such as artificial intelligence, cloud computing, and cybersecurity.

In addition, to help prepare more American students and workers vital roles in cybersecurity, IBM recently pledged to train more than 150,000 people in cybersecurity skills over the next three years through a range of programs, such as SkillsBuild. IBM also will partner with more than 20 Historically Black Colleges & Universities to establish Cybersecurity Leadership Centers to build a more diverse U.S. cyber workforce.

IBM believes that this exciting new era of technology – powered by the cloud, AI, and quantum computing – must be an inclusive era. By helping make community college accessible to a broader population of students, IBM can support the critical role these educational institutions play in building back a more equitable economy.

- **Amazon**

Through the **Upskilling 2025 program**, Amazon committed $700 million to provide 100,000 employees with access to upskilling programs through 2025. Upskilling programs prepare employees with in-demand skillsets and propel them into new careers. The training programs offered through Upskilling 2025 support Amazonians as they gain critical skills to move into higher skill, better paying, technical or non-technical roles within Amazon and beyond. Amazon is focused on creating pathways to careers in areas that will continue growing in years to come, like medicine, cloud computing, and machine learning. As part of Upskilling 2025, Amazon is continuing to announce new training opportunities and expanding on existing programs for employees across the U.S., including:

**Career Choice** is Amazon's pre-paid tuition program for fulfillment center associates looking to move into high-demand occupations. Amazon will pay up to 95% of tuition and fees towards a certificate or degree in qualified fields of study, leading to enhanced employment opportunities for in-demand jobs. Since launching Career Choice in 2012, over 40,000 Amazon employees across 14 countries worldwide have received training for high-demand occupations including aircraft mechanics, computer-aided design, commercial trucking, machine tool technologies, medical lab technologies, nursing and more.

**Machine Learning University** (MLU) is an initiative that helps Amazon employees with a background in technology and coding gain skills in machine learning. As machine learning plays an increasingly important role in customer innovation, MLU helps employees learn core skills to propel their career growth—skills that are often learned only in higher education. Divided into six-week modules, the program requires only half to one full day of participation a week. MLU is taught by more than 400 Amazon Machine Learning scientists who are passionate about furthering skills in the field. Originally launched as a small cohort, the program is on course to train thousands of employees.

**Amazon Technical Academy** is a training and job placement program that equips non-technical Amazon employees with the essential skills to transition into, and thrive in, software engineering careers. Combining instructor-led, project-based learning with real-world application, graduates of the program master the most widely used software engineering practices and tools required to thrive in a career at Amazon. This tuition-free program was created by Amazon software engineers for Amazon employees who want to move into the field.

**Amazon Technical Apprenticeship** is a Department of Labor certified program that offers paid intensive classroom training and on-the-job apprenticeships with Amazon. Providing a combination of immersive learning and on-the-job training, the Amazon Apprenticeship program has already created paths to

technical jobs for hundreds of candidates working to break into professions including cloud support associate, data technician and software development engineer.

Mechatronics and Robotics Apprenticeship gives employees the opportunity to learn skills and technical knowledge needed to fulfill a technical maintenance role. The program, which is registered with the U.S. Department of Labor, helps employees increase their wages up to nearly 40% at the end of the first phase. For apprentices who are selected for and complete the second phase, the average wage can increase by up to another 48%.

**Cloud skills.** According to Gartner, worldwide cloud industry spending is expected to grow from $257 billion in 2020 to $364 billion in 2022. As the cloud industry continues to grow, so will the demand for IT talent, presenting significant opportunity for entry-level and experienced IT talent alike. As part of our global commitment to provide free cloud computing training to 29M people by 2025, AWS offers a suite of educational tools and programs to train and build knowledge of cloud computing competencies to expand and diversify the pipeline of cloud skilled talent within the U.S. workforce. These programs, which include **AWS re/Start, AWS Academy, and AWS Educate**, to name a few, are being implemented across the U.S., with existing statewide education engagements in CA, UT, AZ, TX, GA, IN, VA, and more. We support the workforce and economic development efforts of state and local governments via public and private education systems, teaming with institutions across the U.S. to offer cloud skills education as part of credit and non-credit programs (e.g. certificates and degrees) at scale.

AWS Training and Certification offers individuals access to free digital training and exam preparation courses to prepare for AWS Certifications. AWS Certifications enable learners to validate their AWS cloud computing expertise with an industry-recognized credential.

AWS Educate creates pathways to in-demand cloud jobs, from software development and cloud architecture to machine learning and cybersecurity. The program offers self-paced learning content with 12 Cloud Career Pathways featuring between 30 and 50 hours of self-paced content per learning pathway. The program also continues to roll out new ways to reach learners by supporting programs like Northern Virginia Community College's JumpStart program, which offers tuition-free college courses to eligible high school graduates.

AWS re/Start offers a free, full-time, 12-week skills development program that prepares individuals with little or no technology experience to pursue entry-level cloud computing positions and industry recognized AWS Certification. AWS re/Start, which is taught by an AWS Accredited Instructor, also provides learners with resume and interview coaching to prepare for employer meetings and interviews. The program connects over 90% of graduates with interview opportunities.

AWS Fiber Optic Fusion Splicing Certificate program is a two-day training course on fiber optic installation and repair hosted in collaboration with Sumitomo Electric Lightwave. These skills are increasingly needed to build out the world's data and communication networks like 5G as well as data centers. Through lectures and hands-on lessons, students accepted into the program learn real-world deployment techniques using a variety of hand tools to state-of-the-art automated fusion splicing technology. The program also includes a career networking event to connect students and potential employers. This program is offered at no charge for students.

- **Cisco**

Cisco's Networking Academy, which dates from 1997, has grown from a single school to an expanding community of students, educators, employers, NGOs, Cisco employees, and customers.

**Networking Academy** offers courses in high-demand areas of IT such as cloud computing and network administration through either an instructor-led or online, self-paced model. Self-paced classes at NetAcad.com are free, with the cost for instructor-led classes determined by the institution (such as a community college, public school district, or college).

Courses align with industry-recognized certifications that prepare students for positions at every level, while also boosting their earning potential. For example, students can learn to plan and install a home or small business wireless internet network, troubleshoot connectivity problems, and mitigate online security threats.

Networking Academy aligns closely with domestic efforts to reskill the workforce. For example, it has become a critical component of the state of Michigan's efforts to strengthen its workforce through a state-wide digital acceleration program centered around education.

With job creation in mind, Network Academy offers a broad range of resources to aid students in finding the right position, from incorporating business skills into classes to providing discounts on certification exams, offering career preparation webinars, and hosting a job matching engine that pairs hiring employers with qualified students.

Now offered globally, Cisco's program of instruction helped 1.9 million students find jobs between 2005 and 2019.

- **Facebook**

Facebook is partnering with Pathstream to increase access to high quality careers in digital marketing for underserved students. The 6-course **Digital Marketing Certificate**, developed by Facebook and Pathstream, is an online program that teaches the comprehensive skills needed to succeed in entry-level digital marketing roles. Courses can be credited toward bachelor's degrees. As part of this partnership, Facebook and Pathstream support community colleges, located in various urban and rural communities across the country, to build their capacity to deliver these programs to their local communities. To do this, Facebook and Pathstream provide community college partners with the online learning environment and curriculum, implementation and technical support, ongoing instructor training, career services for students including resume reviews, recruiter engagement, and job placement. To date, over 6000 students have enrolled in the courses.

**Career Connections** is a Facebook initiative that creates jobs, trains jobseekers, and empowers local economies. Facebook partners with businesses to create paid digital marketing summer internships for jobseekers across the US, with a particular focus on underrepresented communities. Participants receive exclusive training, $500 in Facebook/Instagram ad credits, and mentorship from a Facebook employee. Facebook's goal is to train, mentor and support jobseekers as they launch their professional careers while helping SMBs become more competitive by strengthening their online presence.

**Facebook Career Programs** provides access to education and connects people to jobs that can unlock greater opportunities for themselves, their families and their communities—regardless of their education, background or experience. Facebook Career programs help job seekers acquire new skills through specialized training and gain career certificates in growing fields. All people who earn a certification will gain access to the Facebook Certification Career Network—an exclusive job board that connects people with top employers who have committed to hiring skilled and certified talent through Facebook Career Programs.

In 2020, COO Sheryl Sandberg announced Facebook's commitment to support and empower Black, Latinx, and Hispanic communities through **Facebook Elevate**. The program's goal is to provide free digital skills training to 1 Million members of the Black community and 1 Million members of the Latinx & Hispanic communities throughout the U.S. by 2023. Facebook Elevate is fueled by the mission to accelerate the economic success of these historically excluded communities of color by serving small businesses, nonprofits, creators, job seekers, and students with education, community, mentorship and empowerment.

Alongside this mission, Facebook has committed to empowering Black learners with $100,000 dollars in scholarships towards digital skills certification through Blueprint - Facebook's online learning platform. These scholarships will allow recipients to take certification exams including the "Facebook Digital Marketing Associate" and "Social Media Marketing Certificate" at no cost. Certification enables learners to gain access to 120+ companies looking to hire skilled talent through the Facebook Certification Career Network.

For more information:

- Facebook Elevate
- Facebook Scholarship to Certification
- Facebook Elevate Community Group

**Blueprint** is a Facebook skills and training program that empowers people and businesses to reach their goals with Facebook, Instagram and Messenger. People around the world who have discovered Blueprint are developing their skills, testing their knowledge, and establishing themselves as experts in digital marketing.

**Facebook Blueprint Spotlight** is a series of live and previously recorded online training webinars led by Facebook experts. These sessions dive deep into specific marketing topics, helping businesses learn the skills they need to run successful digital campaigns. In each live session, you can interact with the instructor in real-time, providing a unique, customizable learning experience. Spotlight is also one of several tools Blueprint offers to help people prepare for a Facebook Certification, the highest level of accreditation recognized by Facebook.

Improving diversity in hiring is a key focus for many companies but unconscious bias still exists. Skills based hiring provides a way for companies and candidates to be matched more efficiently while reducing the likelihood of biases. It opens the door for applicants that have non-traditional work experience, broadening the talent pool, and can lead to a more diverse workforce by not automatically eliminating candidates without a college degree. Facebook is currently piloting a **Skills Based Hiring Tool** to make job seekers more aware of the tangible skills they have in order to provide them with the confidence needed to apply to higher skilled roles. Our product is focused on helping applicants understand what companies are looking for & helps them communicate how they would meet those needs to better serve employers. We are also working with employers to change recruiting and job descriptions to reflect skills requirements to reduce discrimination in hiring practices.

Facebook is now in the 10th year of its partnership with **Year Up**, a nonprofit organization that works to close the opportunity divide by providing young adults with the training and support needed to build successful careers. At the Facebook on-campus program, Year Up has a learning and development center, providing five months of in-class learning and six months of internship experiences. With Year Up's assistance, we build the foundation not only to obtain employment, but also to thrive as an employee. We have hosted 450+ externs across 8 orgs as diverse as Enterprise Engineering, Global

Operations, Global Business Marketing, Recruiting, Infrastructure, Community Partnerships, Creative Shop, and Facilities.

Facebook's **Virtual Workforce Connection Training Program** is a 2-week long career bootcamp to help professionals climb in their careers. This comprehensive training combines best-in class job-search resources with personal career coaching, and small group workshops. The program is being delivered in partnership with Year Up and Grads of Life, national non-profits with 20+ years of expertise helping talent access quality careers.

- **Walmart**

Walmart in July 2021 announced that it will waive nominal fees and begin paying 100% of college tuition and books for associates through its **Live Better U (LBU) education program**. The initiative will allow approximately 1.5 million part-time and full-time Walmart and Sam's Club associates in the U.S. to earn college degrees or learn trade skills without the burden of education debt.

As the largest U.S. private employer, Walmart is committing to invest nearly $1 billion over the next five years in career-driven training and development. Through its LBU program, it provides education programs through 10 academic institutions chosen for their history of success with adult and working learner programs as well as their focus on degree completion.

Walmart is committed to eliminating the burden of education debt. Cost is a leading barrier for earning a degree, with student loan debt in the U.S. topping $1.7 trillion. Since launching LBU in 2018, more than 52,000 associates have participated in Walmart's program to date and 8,000 have already graduated. Nearly 28,000 associates were active in a LBU program in the summer of 201.

In June 2021 Walmart announced an initiative called **Community Academy**, which offers free classes to the U.S. public for personal and career investment. Community Academy virtual courses are available nationwide at no cost with open registration. Class topics include everything from résumé building and interviewing skills to budget and finance, standardized test preparation and navigating college admissions. Each of the courses is grouped into one of five overall themes – community, personal finance, home, career progression and technology – with plans to expand offerings throughout the year.

Community Academy builds off an existing program for store associates known as **Walmart Academy**, which claims a network of more than 200 locations in stores across the country. Walmart Academy teachers have led more than 2 million training sessions on topics ranging from store processes to leadership and soft skills. The learning centers offer foundational, role-specific and ongoing education training that prepares associates both for their current role and the future. During the pandemic, Walmart shifted to offering virtual instructor-led training, providing more than 111,000 remote associate trainings over the past year.

# EXHIBIT 26

# INNOVATION, COMPETITIVENESS, OPPORTUNITY: A Policy Agenda to Build Tomorrow's Workforce

The increasing use of and demand for technology is creating new types of jobs in every sector of the economy that require an evolving set of skills. Tasks associated with jobs across many sectors are not the same today as they were just 20 years ago. Yet, as job requirements change, new technologies are generating job growth and enhancing productivity. These trends will become even more prominent with the growing use of emerging technologies, such as artificial intelligence.

Although changes are taking place, using software to create solutions to enrich every aspect of our lives presents great opportunity. Software innovation is transforming every sector of the American economy. A recent Software.org: the BSA Foundation study shows the software industry contributed more than US$1.1 trillion to the US GDP in 2016 — a $70 billion increase in just the last two years.[1] The study also showed that the software industry is a powerful job creator, supporting more than 10.5 million jobs, with significant effect in each of the 50 US states. And there are many more jobs available than there are people qualified to fill them.

Jobs in software development, computer programming, cybersecurity, and related fields are growing at an incredible rate. The US Bureau of Labor Statistics estimates that one million computer programming jobs in the United States will go unfilled by 2020.[2] Likewise, the National Initiative for Cybersecurity Education projects a global shortfall of at least 1.8 million cybersecurity professionals by 2022.[3]

Enabling the American workforce to transition smoothly into the workforce demands of the new digital economy requires preparing new generations for jobs of the future, assisting current workers as they transition to the emerging opportunities of the digital economy, and expanding opportunities to reach a bigger pool of talented workers. The government and private sector must work together to:

- Improve access to STEM education;
- Create alternative pathways to evolving workforce;
- Expand workforce retraining;
- Broaden access to technology; and
- Promote responsible immigration policy.

Software is also generating new jobs across industry sectors, requiring new skills ranging from advanced manufacturing to new approaches to customer service and retail sales. Employers are encountering challenges in filling vacancies that require use of new technologies, but opportunities for qualified workers abound.

Both the government and the private sector have important roles in implementing policies that will prepare the next generation for the jobs of the future and allow the current workforce to transition successfully into the new job environment.

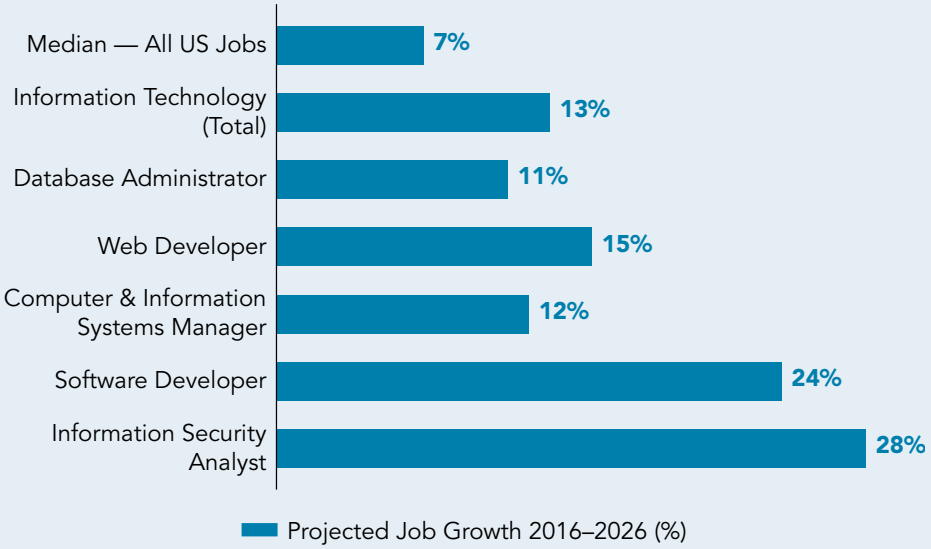
[1] "The Growing $1 Trillion Economic Impact of Software," Software.org (September 2017), available at https://software.org/reports/2017-us-software-impact/.

[2] Tom Kalil and Farnam Jahanian, "Computer Science Is for Everyone!" The White House (December 11, 2013), available at https://obamawhitehouse.archives.gov/blog/2013/12/11/computer-science-everyone.

[3] "Workforce Demand," Fact Sheet, National Initiative for Cybersecurity Education (October 26, 2017), available at https://www.nist.gov/sites/default/files/documents/2017/10/26/nice_workforce_demand_pdf.pdf.

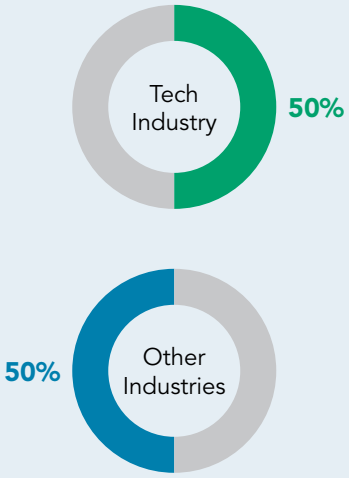
# Meeting the Workforce Demands of the New Economy

## IT Job Growth Will Far Outpace Other Jobs




Source: Bureau of Labor Statistics[4]

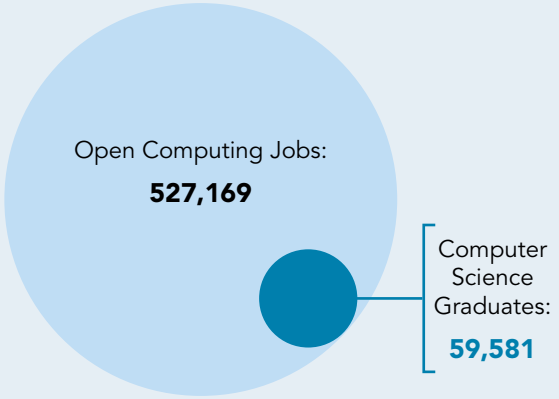
## Half of All Coding Jobs Are Outside the Tech Industry, 2016




Source: Oracle Academy/Burning Glass Technologies[5]

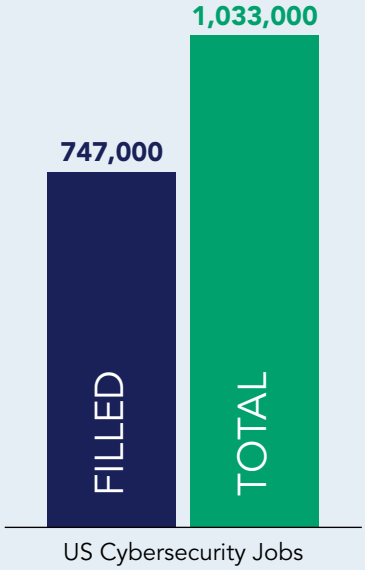
**65%** of children now entering primary school will hold jobs that currently don't exist.[6]

## STEM Education Must Expand to Keep Pace, 2015




Source: Quartz[7]

## Job Demand Far Outstripping Supply in Cybersecurity
**(October 2016–September 2017)**




Source: CyberSeek[8]

[4] Data drawn from Bureau of Labor Statistics, "Occupational Outlook Handbook," available at https://www.bls.gov/ooh/home.htm.

[5] "Beyond Point and Click: The Expanding Demand for Coding Skills," Burning Glass Technologies (June 2016), available at https://www.burningglass.com/wp-content/uploads/Beyond_Point_Click_final.pdf.

[6] *The Future of Jobs: Employment, Skills, and Workforce Strategy for the Fourth Industrial Revolution*, World Economic Forum (January 2016) available at http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.

[7] Sarah Kessler, "You Probably Should Have Majored in Computer Science," *Quartz* (March 10, 2017) available at https://qz.com/929275/you-probably-should-have-majored-in-computer-science/.

[8] Data drawn from "Cybersecurity Supply and Demand Heat Map," CyberSeek, available at http://cyberseek.org/heatmap.html.

# Building Tomorrow's Workforce: Why It Matters

**Investing in tomorrow's workforce:**

Ensures US **Competitiveness** in a Changing Global Economy

Spurs **Innovation** Across Industry Sectors

Expands **Economic Opportunity** Across the United States

Promotes **Economic Security** for Millions of Americans

## Improve Access to STEM Education

STEM education equips students with problem solving, critical thinking, and other abilities that are important for jobs in virtually every industry. Making STEM education inclusive and widely available builds interest in developing in-demand skills and expands the available workforce for technology-related jobs. BSA therefore supports:

**Transforming K-12 STEM Education.** STEM education is essential to building a highly skilled workforce, but too few students currently have access. Enhancing government investments in early STEM interventions, expanding public-private partnerships, re-envisioning vocational education, and training more STEM-qualified K–12 teachers are critical priorities.

**Encouraging Greater Diversity and Inclusivity in STEM Education.** Making STEM education more widely available — and encouraging inclusion of underrepresented groups — through scholarships, loan forgiveness, and other initiatives will help ensure the jobs of the future are available to the entire population.

**Broadening Exposure to STEM in Higher Education.** Although many students in higher education choose non-STEM areas of study, ensuring a baseline exposure to STEM fields among these students can prepare graduates in all fields to embrace technology in whatever career they may choose.

**Aligning STEM Curricula to Real-World Demands.** Greater integration of high-demand practical disciplines, such as software engineering, data science, and cybersecurity, into computer science and other STEM curricula will ensure investments in STEM education translate into a qualified, highly skilled workforce.

## Expand Workforce Retraining

Emerging technologies will create new jobs and change the skills demanded in many existing jobs. In addition to preparing the next generation workforce, we must ensure the current workforce has access to the skills needed as the job market evolves. Policies that promote access to training in 21st century skills for workers seeking to adapt to new professional demands can ensure that the evolving economy leaves no one behind. BSA therefore supports:

**Investing in Mid-Career Training in High-Demand Tech Skills.** Congress should establish mid-career retraining programs to provide American workers with high-demand cybersecurity and IT skills, helping match qualified workers to growing occupational fields. Tax incentives to offset costs to workers for specialized training and certification programs could also pay dividends.

**Preparing Employees for Advanced Manufacturing.** Programs such as the Manufacturing Extension Partnership can allow employees to access training to let them take full advantage of advanced manufacturing technologies.

**Increasing Training and Reskilling to Prepare Veterans for Careers After the Military.** Military personnel develop talents and skills needed for success in the private sector during their service, but training and certification with specific industry technology platforms can facilitate their successful transition. Targeted training and reskilling programs for transitioning military and veterans and their families will expand the high-tech workforce and create new opportunities for veterans.

## Create Alternative Pathways to the Evolving Workforce

As our economy changes, we need to consider whether our education model should change as well. In the new economy, technical schools, apprenticeships, boot camps, and other alternative pathways may be just as effective as traditional classrooms in generating the skills and interests necessary to thrive in 21st century careers. BSA therefore supports:

**Strengthening Apprenticeship Programs.** Apprenticeships can be an important way to gain the skills and experience needed for the evolving job market. Building public-private partnerships, simplifying requirements, and identifying incentives will make apprenticeships more feasible and attractive for the future workforce.

**Expanding Technical School Education.** The Perkins Act CTE program, the federal government's primary career and technical education effort, should be strengthened and expanded to make technical school education more accessible to future workers, and should embrace initiatives to make technical school education more relevant to future workforce needs.

**Mainstreaming Boot Camps, Online Courses, and Other Alternative Education Models.** Boot camps, online courses, community colleges, and alternative educations models like P-TECH can each help reach new student populations, help students tailor their education to their own needs and pace, and impart high-demand skills to workers unable to participate in degree programs or other traditional pathways. The government should increase investments in these and other alternative models to expand the path to the 21st century workforce.

## Broaden Access to Technology

Technology enables the creation of jobs in all industries and in all parts of the country. Ensuring equal opportunity to access technology is fundamental to job creation and economic growth. BSA therefore supports:

**Achieving Universal, Affordable High-Speed Internet Access.** Affordable access to high-speed Internet is increasingly a necessity for many professions; yet, more than a third of Americans still lack access. The government should develop a near-term plan to close this gap through investments in Internet infrastructure in underserved areas and efforts to ensure its affordability.

**Ensuring Equitable Access to Technology in the Classroom.** Exposing students to cutting-edge technologies at an early age can improve educational outcomes and prepare students for technology-related careers; yet access to technology in the classroom varies widely across different communities and income groups. The government should invest in innovative efforts to expand access to technologies in these underserved classrooms.

## Promote Responsible Immigration Policy

As the software industry evolves, the gap between available technology-related jobs and qualified workers continues to grow. Although we work to improve education and training of the US workforce, high-skilled immigration can ensure these jobs — and the innovation they support — remain in the United States. Responsible immigration policy can enable the United States to recruit the best and brightest across industry sectors to fill high-demand jobs and contribute to American innovation. BSA therefore supports:

**Strengthening the H-1B Visa Program.** The H-1B visa program has enabled American industry to recruit top talent from around the world to contribute to American innovation and job creation. Strengthening the program, to include authorization for spouses to work, more support for recent graduates entering the workforce, and an expansion of visa caps, will help the US economy maintain its competitive edge.

**Supporting DREAMers.** Research has repeatedly shown that Deferred Action for Childhood Arrivals (DACA) recipients tend to attain comparatively high levels of education and be employed in high-skilled jobs, creating a new generation of skilled workers. The software industry — and its customers — employ DACA recipients. Protecting their future is important to workplace stability, to expanding US GDP, and, as a result, to creating new jobs for all Americans.

# EXHIBIT 27

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# SUPPLY CHAIN RESILIENCE ISSUE BRIEF

## CYBERSECURITY & CROSS-BORDER ACCESS TO DATA

The ability to locate and transfer data in the most functionally secure manner is a cybersecurity risk management best practice. This is in part because cross-border visibility into cyber-related data allows for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Additionally, companies may choose to store data at geographically diverse locations to obscure the location of data and reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. Conversely, when governments mandate localization or restrict the ability to transfer and analyze data in real-time, they create unintended vulnerabilities, as summarized below:

- **Integrated Cybersecurity Planning.** Data transfer restrictions and localization requirements force organizations to adopt a siloed approach to data, often restricting the locus of certain data, but not others. This differentiation creates unnecessary technical complexity without any corresponding benefit to security. Simply put: artificial requirements to store data within borders strain the people, processes, and technologies an organization needs to manage its cybersecurity risk.

- **Cybersecurity Awareness.** Data transfer restrictions and localization requirements impede visibility of cybersecurity risks, not only at the intra- and inter-organizational levels, but also at national and international levels. If cyber defenders cannot access threat indicators or other cybersecurity data collected in one jurisdiction, it becomes harder to address malicious cyber activity in other jurisdictions.

- **Cybersecurity Collaboration.** Data transfer restrictions and localization requirements can impede cross-border collaboration, information sharing, and other coordinated network defense. When such restrictions and requirements isolate network defenders from each other, they cannot adopt a unified and coordinated defensive posture against malicious actors that do not respect national borders. In short, data transfer restrictions can give malicious actors that do not respect local legal requirements a lasting structural advantage over cyber defenders that do.

- **Third-Party Cybersecurity Services.** Many organizations amplify their own cybersecurity risk management through third-party cybersecurity service providers. Best-in-class services depend on access to cyber data from around the globe. Without this access, these services and their users become more vulnerable to compromise.

- **Cybersecurity Resiliency.** Whether a particular geographic area is at high risk for a natural disaster or in a potential future war zone, having data efficiently distributed is a crucial component of resiliency. The misconception that keeping data only within national boundaries will increase its security can actually create significantly more risk.

- **Protectionism in the Name of Cybersecurity.** Localizing data within a country—or blocking its transfer—has no functional cybersecurity benefit. Security is determined by the technical and operational protections that accompany the data, not the location. Transfer restrictions and localization requirements are often used to advance other objectives. Perhaps the most systemic problem with using cybersecurity laws to require localization, then, is that it diminishes the role of laws and policies that are truly designed to improve security.

# EXHIBIT 28

# Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures

By Peter Swire, DeBrae Kennedy-Mayo, Drew Bagley, Sven Krasser, Avani Modak & Christoph Bausewein[1]

## Table of Contents

**I. Introduction**
**II. The Tension in EU Data Protection Law Between Cybersecurity "State of the Art" and Potential Privacy-based Limits on Processing Personal Data**
- **A. EU Law Supporting Strong Cybersecurity Protections**
- **B. ENISA's Cybersecurity Guidance**
- **C. Potential Privacy-based Limits on Processing Personal Data for Cybersecurity Purposes**

**III. The MITRE ATT&CK Framework and Examples Where Localization Creates Obstacles for Defenders**
- **A. The MITRE ATT&CK Framework and TTPs**
- **B. Two Key Themes for TTPs Affected by Localization**
- **1. Impacts to Cybersecurity: "The Who and the What" of an Attack**
  - **a. Threat Hunting**
  - **b. Privilege Escalation Attacks**
- **2. Impacts to Cybersecurity: Risks from Knowing Less Than the Attacker**
  - **a. Pen Testing and Other Red Teaming**

**IV. Quantifying Anticipated Degradation Effects**
- **A. Reconnaissance and Initial Access**
- **B. Command and Control**

**V. Assessing European Cybersecurity Certification Regimes Requiring Localization**
**VI. Conclusion**

## I. Introduction

This paper continues the research program begun in "The Effects of Data Localization on Cybersecurity – Organizational Effects" ("*Effects*"). (Swire 2022). That paper is now available on SSRN, and is in final phases of revision for a peer-reviewed, inter-disciplinary journal. In this new paper, we continue to examine obstacles to cybersecurity that result from "hard" data localization, where transfer of data is prohibited to other countries. We also continue the focus on defensive cybersecurity – effects on the ability of organizations such as corporations and government agencies to identify, protect, detect, respond, and recover in the face of cyber-attacks.

The importance of data localization has risen rapidly in recent years. This paper focuses on examples from the European Union ("EU"), which has taken significant steps toward *de facto* localization of personal data in the wake of the 2020 *Schrems II* decision of the European Court of Justice (*Schrems II* 2020). Among enforcement actions since that decision, the Portuguese data protection authority ordered a government agency to terminate its use of cybersecurity services from U.S.-based cybersecurity company Cloudflare (CNPD 2021). In the Data Act and other proposed legislation, the EU would also impose localization rules for defined categories of both personal and non-personal data (COM/2022/68 2022, Art. 2(1)(af)). Additional localization could result from the proposed European Cybersecurity Certification Scheme for Cloud Services ("EUCS"), discussed in Part V (ENISA 2020).

This paper thus continues to examine the effects of localization rules for personal data, while recognizing that some localization rules may also block categories of non-personal data. As Nigel Cory and Luke Dascoli have documented, the number of data localization measures roughly doubled from 2018 to 2021, including at least 62 countries with 144 restrictions (Cory and Dascoli 2021).

Using an approach based on organizational form, *Effects* provided a new categorization of the effects of data localization on cybersecurity management. We analyzed effects within an organization, across organizations with payment, and across organizations without payment. First, our analysis showed that despite data localization often being used as a proxy for better data protection, such policy would actually threaten an organization's ability to achieve *integrated management of cybersecurity risk*. We analyzed International Standards Organization ("ISO") 27002, as a way to systematically examine the effect of data localization on a widely-used set of cybersecurity management controls. We found that 13 of the 14 ISO 27002 controls, as well as multiple sub-controls, would be negatively affected by localization of personal data. Second, the analysis explained how data localization pervasively limits *provision of cybersecurity-related services by third parties*, a global market of roughly $200 billion currently, with doubling expected within a few years. Put simply, a great variety of cybersecurity services rely on transfers of personal data across borders. Third, data localization threatens non-fee cooperation on cybersecurity defense. Notably, localization undermines *information sharing for cybersecurity purposes*, which policy leaders have emphasized as vital to effective cybersecurity.

This paper supplements *Effects* by organizing the risks to cybersecurity by the techniques, tactics, and procedures ("TTPs") of threat actors and defenders. To categorize the TTPs, we have relied on two authoritative approaches. First, we analyzed types of attacks in the widely-known MITRE ATT&CK Framework, which details high-level adversary tactic categories and individual techniques that adversaries can use within each of the tactic categories. We also examined the technical and organizational measures supported by the European Union Agency on Cybersecurity ("ENISA") and the German TeleTrust IT Security Organization in Germany in their 2019 guidelines on "The State of the Art" for cybersecurity (ENISA and TeleTust 2021). Using these two approaches, we highlight three important tactics defenders use for cybersecurity purposes – (1) threat hunting/threat intelligence; (2) privilege escalation attack/lateral movement; and (3) red teaming/pen testing. The two categorizations result in similar conclusions -- all three of these categories, considered essential to a mature cybersecurity

program, would routinely require the cybersecurity defenders to access types of personal data that would be restricted by current data localization laws and proposals.

Part II of this paper examines the tension between the EU's regulatory requirements for cybersecurity and data protection. Requirements for effective cybersecurity include Article 32 of the General Data Protection Regulation ("GDPR"), Article 13(1) of the EU CER Directive, Article 21(1) of the NIS2 Directive and Article 5 (1)(g) of the EU Cybersecurity Act (EU Directive 2022/2557, 164-198; EU Directive 2022/2555, 80-152; EU Regulation 2019/881, 15-69). Under these and similar laws, organizations in the EU are expected to deploy effective security safeguards appropriate to the risk taking into account the "state of the art" in cybersecurity as outlined by ENISA's guidance (ENISA and TeleTrust 2021). At the same time, data protection laws prohibit the processing of personal data unless it is lawful (Art. 6 and 9 of the GDPR) and adequately protected when transferred out of the EU (Chapter 5 of the GDPR). As defined within the EU, "personal data" is a broad term that includes numerous categories of data routinely used by cybersecurity defenders. For example, IP addresses are provided to a server as an essential part of web communications (*Breyer* 2020).[2] Despite this functionality and ubiquity, IP addresses are included within the scope of "personal data" that EU enforcement actions have found should not be transferred to the U.S. and other non-EU third countries. In recent EU enforcement actions, simply the possible transfer of IP addresses to the U.S. has been the stated basis for data protection authorities to find that Google Analytics is unlawful on EU websites (ADPA 2021; CNIL 2022).

Part III of this paper examines the MITRE ATT&CK Framework and how it organizes relevant aspects of a cybersecurity defense system. The analysis highlights how data localization requirements undermine the three examples of threat intelligence, privilege escalation, and red teaming.

Part IV supplements the effects in Part III by providing a quantitative model illustrating effects of data localization under plausible assumptions. In the model, halving the number of IP addresses available to a defender would more than double the likely time until a new attack is detected.

Part V extends the analysis to the cybersecurity approaches now being considered under the proposed EUCS. The hard data localization in some proposals appear to conflict with the findings of this paper, that hard data localization would undermine defensive measures such as threat intelligence, privilege escalation, and red teaming.

Part VI offers conclusions. The U.S., Europe, and other nations face incessant and sophisticated cyber-attacks. In the face of these threats, imagine that policymakers were considering a law that would degrade threat intelligence, leave systems open to privilege escalation, and bar effective pen testing and other red teaming. Such a proposed law would deserve great skepticism. As documented in this paper's research, however, data localization laws appear to have such effects. This paper adds to the finding in *Effects*, that "until and unless proponents of localization address these concerns, scholars, policymakers, and practitioners have strong reason to expect significant cybersecurity harms from hard localization requirements."

## II. The Tension in EU Data Protection Law Between Cybersecurity "State of the Art" and Potential Privacy-based Limits on Processing Personal Data

In this Part we set forth the legal requirements in the European Union for cybersecurity "state of the art," and briefly describe ENISA's guidelines for achieving that "state of the art." We then discuss potential privacy-based limits on processing personal data.

### A. The GDPR's Call for State of the Art Cybersecurity

The GDPR, including in its Recital 49, requires that cybersecurity be an integral part of data protection (ENISA and TeleTrust 2021, 9; GDPR Rec. 49). Article 5(1f) of the GDPR sets forth "Principles relating to processing of personal data." Among other requirements, personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures" (GDPR Rec. 39).

Article 32 of the GDPR addresses the "Security of processing" particularly mandating that the "state of the art" of cybersecurity practices be included in the risk analysis for handling data security (GDPR Art. 32; ENISA and TeleTrust 2021, 9, 87).[3] One commentator has described the "state of the art" as consisting of "measures that are based on proven knowledge, of an advanced technical development, practically suitable, ready and available for technical implementation, but have not necessarily become established in practice yet" (Selzer 2021, 123). Notably, cloud services for global threat analysis are already a common component of many security solutions. Furthermore, approaches such as Threat Intelligence Platforms, at their core, aggregate and share data pertinent to threat detection. This threat-relevant data often includes IP addresses and other information considered "personal data" under EU law (Kime, 2023).

Article 32 of the GDPR adopts a risk-based approach to what measures are appropriate. Data controllers should deploy "appropriate technical and organizational measures." The appropriateness of measures depends both on risks to cybersecurity and to "the rights and freedoms of natural persons" (GDPR Rec. 78).

Where a breach of security occurs, Article 33 of the GDPR requires an organization to notify the competent data protection authorities within 72 hours unless it is unlikely to pose a risk to the fundamental rights and liberties of data subjects. Furthermore, Article 34 of the GDPR requires an organization to notify the individuals themselves where there is likely to be a high risk to their rights and freedoms. Complementary guidance from the EDPB makes clear that "high risk" is defined by the circumstances surrounding the nature of the data, risk mitigation measures in place, and the recipient of the breached data (EDPB 2023).

Recital 75 of the GDPR defines "Risks to the Rights and Freedoms of Natural Persons" as personal data processing which could lead to physical, material or non-material damage. The Recital applies to damages that specifically can result from cybersecurity incidents, such as identity theft, fraud, financial loss, damage to reputation, and loss of confidentiality. The Recital

also lists other relevant damages, including where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data.

### B. ENISA Guidelines on "State of the Art" for Cybersecurity

The conundrum is even stronger since the European Union Agency for Cybersecurity ("ENISA") in co-operation with the IT Security Association Germany ("TeleTrust") has issued guidelines on the "state of the art" required for appropriate technical and organizational measures ("Guidelines") in 2019, shortly after GDPR went into effect. These Guidelines provide guidance on "What is 'state of the art' in IT security?" (ENISA 2019). In examining 'state of the art,' the Guidelines adopt the approach that "state of the art depends on whether a measure is technically necessary, suitable and appropriate from the perspective of technical practitioners. It can and should be possible to react to more current threats – and especially to the current technical possibilities for attack." (ENISA and TeleTrust 2021, 11).

We offer two observations about these Guidelines. First, the Guidelines provide an explanation of what technical and organizational measures are expected in order to meet the "state of the art" provided by the very EU agency dedicated to achieving a high common level of cybersecurity across the EU. We explore some of these measures in detail below in Part III, as we discuss key Tactics, Techniques, and Procedures that are affected by data localization.

Second, we note an interesting discussion of risk in the Guidelines. As discussed elsewhere in more detail, the European Data Protection Board ("EDPB") has expressed disapproval of a risk-based approach for assessing when transfer of personal data is lawful (Christakis 2020). ENISA, however, explicitly states that appropriate cybersecurity measures should take into account the level of risk to fundamental rights. ENISA says:

> "Article 32 of the GDPR regulates "security of processing" to ensure that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as *the risk of varying likelihood and severity for the rights and freedoms of natural persons*, appropriate technical and organizational measures are implemented." (emphasis added) (ENISA 2019).

In forthcoming research, Théodore Christakis is examining in detail whether and how a "risk-based approach" is appropriate under EU law and practice.

### C. Potential Privacy-based Limits on Processing Personal Data for Cybersecurity Purposes

Along with the EU expectation for providing state of the art for cybersecurity, there are EU legal authorities that appear to limit achievement of that state of the art. In particular, the GDPR places restrictions on processing of personal data. Both processing and personal data are defined terms in this regulatory scheme.

The GDPR applies broadly to personal data that originates from the EU, as described in Article 3(1) of the GDPR. Under the GDPR, "personal data" means any information relating to an identified or identifiable natural person, pursuant to Article 4 (1) of the GDPR. The European

Commission ("Commission") has explained the broad scope of "personal data" as defined in Article 4 of the GDPR: "Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data" (EC: "What is Personal Data"). As examples, the Commission includes not only obvious identifiers such as name and address, but also more technical identifiers such as: "location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; a cookie ID; [and] the advertising identifier of your phone" (EC: "What is Personal Data"). Other information available to administrators of company or agency computer systems are also often considered personal data, such as MAC addresses where they are linkable to a personal device (Future of Privacy Forum 2014).

"Processing" is also a broad term, meaning any operation performed on personal data. This includes any access, collection, storage, adaptation or alteration, use, transfer, disclosure by transmission, otherwise making available, or even the erasure or destruction of personal data.

The broad scope of "processing" of "personal data" effectively means that ubiquitous unique, and often-times public, identifiers inherent to modern IT and network infrastructure are regulated by GDPR. Examples from the state of the art for cybersecurity include collection of security telemetry from endpoints, cloud workloads, network email, or threat data from previously siloed security tools across an organization's technology stack for easier and faster investigation, threat hunting, and response. One consequence is that certain processing of personal data may be unlawful even when it would seem necessary and proportionate, such as processing for cybersecurity purposes to protect critical infrastructure, national security, economic purposes, and even the security of an individual's data.

EU data localization has become a more prominent legal risk in the wake of the 2020 *Schrems II* decision of the European Court of Justice, which announced limits on transfer of personal data to third countries (*Schrems II* 2020). Subsequently, the EDPB issued guidance about assessing the laws and practices of the destination country and technical and organizational safeguards (termed "supplementary measures") to ensure adequate protection in the transfer of personal data (EDPB 2021). The EDPB expressed reservations about applying a risk-based approach to such transfers.

These legal developments have raised concerns for organizations using cybersecurity services that are not exclusively delivered within the EU, including hosting, support, engineering, and service. Customer service, IT operations, or a security operations center that "follows the sun," to provide 24/7 support, are examples of services that may be difficult or impossible in practice to provide exclusively from within the EU.

The conundrum is how to proceed when data protection laws designed to limit harms to personal data and to protect personal data have the apparent consequence of increasing harms to personal data (by setting data localization limits on applying the state of the art for cybersecurity). We note that guidance interpreting the data breach rules under the GDPR makes clear that notification is not required where a personal data "breach is unlikely to result in a risk to the rights and freedoms of individuals" (EDPB 2023). Risk is focused on "physical, material or non-material damage" to breach victims, such as "discrimination, identity theft or fraud,

financial loss and damage to reputation." In assessing this, "consideration should also be given to other personal data that may already be available about the data subject." This suggests that in most contexts the data elements used in cybersecurity, such as IP address, MAC address, or email address, are low risk – not requiring a breach notice even when they are seized illegally by hackers and transferred to a third country. On the other hand, under some interpretations processing of these same data elements are considered a violation of the data subject's fundamental rights when they are transferred intentionally, even when being used by an organization for GDPR Article 32 and Recital 49 cybersecurity purposes. When reviewing both the legal requirements in the European Union for cybersecurity "state of the art" and the privacy-based limits on processing personal data, the conclusion that emerges is there has not been full and explicit consideration among EU legal authorities about how overall to achieve both cybersecurity state of the art and also limit use and transfer of many data elements that are required to institute the state of the art (Bagley 2022).[4]

## III. Using the MITRE ATT&CK Framework to Develop Themes for Where Localization Creates Obstacles for Defenders

With the current EU data localization approach in mind, we next turn to examination of the effects of hard data localization laws on cybersecurity tactics, techniques, and procedures ("TTP"). NIST defines TTP as

> "The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique" (NIST).

In Part III, we first explain the role of the MITRE ATT&CK Framework as a leading approach for assessing TTPs. We explain the methodology for using the Framework to identify which TTPs are most likely to be affected by data localization rules. We explain two themes for such TTPs: the "who and what" of an attack, and the "risks from knowing less than the attacker."

To explain these themes, we provide more detail on threat hunting and privilege escalation as two examples of the "who and what" of an attack, and then use red teaming and pen testing as an example of the "risks from knowing less than the attacker." For each of these, we provide: (a) the anatomy of the approach; (b) types of personal data; (c) alternatives to use of personal data; and (d) the requirements of the ENISA Guidelines applied to each of threat hunting, privilege escalation, and red teaming.

### A. The MITRE ATT&CK Framework and TTPs

In researching the effects on TTP, we use the widely-known MITRE ATT&CK framework. MITRE's ATT&CK framework focuses on pre-compromise preparations and post-compromise activities of adversaries (MITRE: Enterprise Matrix). It provides a detailed

enumeration of common adversary behaviors after they have gained access to a system within a network (Strom et al. 2017). MITRE researchers explained that the framework serves "as a method for discovering analytic coverage and defense gaps inside a target network" (ibid, 1). For our purposes, the framework can help pinpoint "defense gaps" resulting from limits on transfer of personal data.

The MITRE Framework relies on examination of "tactics" and "techniques." Tactics describe the reasons why the adversary acts or the goals that the adversary hopes to accomplish (ibid, 12). The tactics discussed in the framework are: (1) Reconnaissance; (2) Resource Development; (3) Initial Access; (4) Execution; (5) Persistence; (6) Privilege Escalation; (7) Defense Evasion; (8) Credential Access; (9) Discovery; (10) Lateral Movement; (11) Collection; (12) Command and Control; (13) Exfiltration; and (14) Impact.

Techniques are more detailed than tactics and describe the actions that the adversary takes to accomplish their tactics. The ATT&CK framework analyzes these techniques from both the offensive and defensive points of view (ibid, 12; CrowdStrike: IOA v. IOC).[5] Version 13 of ATT&CK for Enterprise includes the aforementioned 14 tactics and 196 techniques (MITRE 2023). Instead of being a theoretical taxonomy that seeks to categorize every possible category of attack, the techniques have been based empirically on observed intrusions. MITRE sought to "address the need for additional details while remaining grounded in observed and plausible adversary behavior" (Strom et al. 2017, 9). To illustrate the application to current types of attacks, rather than a general taxonomy, some of the techniques are specific to widely-used software, such as "Windows Remote Management" or "DLL side loading" (referring to dynamic link libraries in the Windows operating system) (Cybereason Global SOC Team 2022).

Although the methodology for use of the MITRE ATT&CK framework evolved during the course of research for this article, the combined team (i.e., the current co-authors from Georgia Tech and CrowdStrike) utilized the MITRE ATT&CK framework as a starting point for assessing the TTPs that are most affected by the localization limits.

### B. Two Key Themes for TTPs Affected by Localization

Based on the combined team's assessment, we present two themes. First, localization laws can disrupt the defenders' ability to determine "The Who and the What" of an attack. The basic idea is that details about "who" is attacking often requires access to personal data. Similarly, as an attacker moves through a defender's system, there are often account names or other personal data in tracking "what" the attacker does in the system. Put another way, the telemetry and other data used by defenders may often include personal data (or other protected data), in ways that create obstacles for defenders if that data is not available due to hard localization. As discussed further below, threat hunting and privilege escalation are two important defensive measures that are likely to be especially hard hit by limits on data transfer.

Second, localization laws can result in "Risks From Knowing Less Than the Attacker." An essential part of good cyber defense is for the defenders to test the system through "red teaming," including penetration ("pen") testing. Pen testing involves the defense hiring "white hat" attackers to find as many vulnerabilities and configuration issues as possible, exploit them, and determine risk levels (Talamantes). Red teaming is a more general approach, for the defender to identify physical, hardware, software, and human vulnerabilities. In addition to pen testing, red team skills include social engineering, threat intelligence, and reverse engineering (Coursera 2022).

Data localization laws would appear to present serious obstacles to pen testing and other red teaming. The intuition is that attackers will be willing to break the law, to seek out and transfer personal data across national borders. Defenders, by contrast, must follow the law. If defenders hire pen testers, those testers would not be able to probe for vulnerabilities that would require learning account information and other personal data, notably where the data is stored in a different country. Since a large fraction of cyber-attacks involve crossing national borders, the defenders would systematically be able to test and learn about vulnerabilities in their own systems less well than the attackers.

### 1. Impacts to Cybersecurity: "The Who and the What" of an Attack

Notably, cyber attacks today often do not involve the use of malware, instead leveraging the use of legitimate credentials increasingly obtained from "access brokers" (CrowdStrike 2023b). This means defenders must prioritize detecting the behavior of the adversary in a victim's system. To highlight the complexities of the need to use personal data in "state of the art" cybersecurity, we discuss two examples that go to "the who and the what" of an attack – threat hunting and privilege escalation. The basic idea is that details about who is attacking often requires access to personal data. Similarly, as an attacker moves through a defender's system, there are often account names or other personal data in tracking "what" the attacker does in the system. Put another way, the telemetry and other data used by defenders may often include personal data (or other protected data), in ways that create obstacles for defenders. Data may not be available due to hard localization or encumbered data may be inadvertently obtained in the course of pen testing, exposing the defenders to legal risks.

#### a. Threat Hunting.[6]

Threat hunting is the practice of proactively searching for cyber threats in a company's environment that have bypassed the endpoint security defenses. Threat hunting is critical to addressing advanced persistent threats (APTs). Threat hunting works with the assumption that the attacker is already in an organization's system. Steps include: hypothesis-driven investigation, investigation using tactical threat intelligence to catalog known Indicators of Compromise (IOCs) or Indicators of Attack (IOAs), and advanced analytics and machine learning investigations (Taschler 2023; CrowdStrike 2023a; Baker 2023; CrowdStrike 2022a).

**i. Anatomy of Approach.** The process for threat hunting involves three steps: the trigger, the investigation, and the resolution. The trigger points the defender to a specific system or area of the network for further investigation. The investigation involves using tools to determine

whether the potential compromise of the system is malicious or benign. The resolution involves communicating the intelligence related to the malicious activity to operations and security teams so they can respond to the incident and mitigate the threats (Taschler 2023).

**ii. Types of personal data.** An attacker generally creates digital footprints that may include personal data. These may exist in logs generated in the operating system or telemetry data captured by cybersecurity technologies such as the EDR (ENISA and TeleTrust 2021, Sec. 3.3.22). Examples of personal data may include usernames, file names, and IP addresses.

For hypothesis-driven investigations, a large pool of crowdsourced attack data gives insight into attackers' latest tactic, techniques, and procedures (Taschler 2023). This crowdsourcing often includes personal data.

A large and increasing fraction of attacks do not use malware, so defenders doing threat hunting routinely rely on examining details of Indicators of Compromise (IOCs) or Indicators of Attack (IOAs), which may include personal data, as shown for instance in documentation of detection of attacks by an APT (CrowdStrike: IOA v. IOC).

For advanced analytics and machine learning, defenders look for irregularities across an array of telemetry. These defenses use queries and automation to extract leads and then have a skilled human defender identify the signs of attacker activity (Taschler 2023).

**iii. Alternatives to Use of Personal Data.** The effectiveness of threat hunting would likely be decreased due to the limited IOCs and IOAs from countries with data localization. Data localization would imply that protected data could likely not leave these countries but would not necessarily prohibit data from non-data localization countries from entering. It is certainly possible that these non-data localization countries may be unwilling to share information with countries that have data localization in place. Countries or regions with larger populations, such as the EU and India, may be less affected than countries with smaller populations, but the extent of such difference deserves additional empirical investigation.

The non-sharing of information could lead to a situation where an attack could be successful region to region, instead of cybersecurity specialists being able to defend against the attack worldwide once it had appeared in one region. In addition, the smaller regional datasets complicate building a proper baseline of normal behavior for an organization. That impedes human threat hunters, but it especially hinders the creation of machine learning-based threat detectors, which require large and diverse datasets to be trained properly. This in turn raises the costs of operating security infrastructure at scale and increases the costs of security incidents where time is of the essence.

**iv. Threat hunting and the ENISA Guidelines.** The ENISA Guidelines on "state of the art" contemplate extensive efforts to conduct threat hunting, and threat intelligence more broadly. Notably, the guidelines include "Technical Measure - 3.2.27 Threat intelligence," which provides:

> Tactical Cyber Threat Intelligence includes malware analysis and the import of individual, static, and behavioral threat indicators into defensive IT security solutions. Operational Cyber Threat Intelligence is used to improve knowledge about an attacker, his skills, infrastructure and attack tactics to implement more targeted cybersecurity measures such as proactive threat hunting. Strategic Threat Intelligence enables a better understanding of the current threat situation (threat assessment) (ENISA and TeleTrust 2021).

Other relevant parts of the ENISA Guidelines are "Technical Measure - 3.2.22 - Endpoint Detection and Response" and "Technical Measure - 3.2.24 – Attack Detection and Analysis" (ibid).

### b. Privilege Escalation Attacks

The next example focuses on a privilege escalation attack using spear phishing (Falcon OverWatch Team 2021; CrowdStrike 2022b; CrowdStrike 2023b). Spear phishing often is part of a "privilege escalation" attack – an attack designed to gain more access than authorized by the system. Gaining privilege enables "lateral movement" by the attacker, so that the attacker can move from the account originally compromised by phishing to other parts of the system of interest to the attacker (CrowdStrike 2023b).

Defending against spear phishing implicates "the who and the what" of an attacker's activities, such as identifying accounts and tracing an attack through a system, including by use of individuals' credentials. The concern would be if the adversary can move unobstructed while the defender is legally prohibited from seeing unique identifiers within an organization that are stored on networked endpoints in multiple countries.

**i. Anatomy of Approach.** Phishing is a term for emails or other communications that are designed to trick a user into believing they should provide a password, account number, or other information. The user then typically provides that information to a website controlled by the attacker. Spear phishing is a phishing attack that is tailored to the individual user, for example, when an email appears to be from the user's boss instructing the user to provide information.

In the White Paper entitled "Finding Cyber Threats with ATT&CK-Based Analytics," MITRE describes a hypothetical campaign involving spear phishing that we incorporate here to emphasize the impact of personal data in the scenario (Strom et al. 2017, 2).

In our example, consider an employee in the EU, working for a company that also operates in the U.S., who falls victim to a spear phishing attack. The employee downloads an executable, which downloads a second stage Remote Access Tool (RAT) payload, giving a remote operator access to the victim computer as well as an initial access point into the network. The adversary then uses tools already available on the compromised computer to learn more about the victim's system and the surrounding network (ibid, 2-4).

**ii. Types of Personal Data.** In defending against the privilege escalation attack, numerous steps of the attack could have personal data at issue. First, the attacker uses spear phishing to gain access, compromising one person's account (CrowdStrike 2022b). Next, the attacker exploits the credentials of the victim's account to explore the network and achieve lateral movement (CrowdStrike 2023b). The attacker's goal may be to extract particular high-value documents or to remain in the system as an advanced persistent threat (APT) (CrowdStrike 2023a).[7] For example, to achieve persistence, the attacker might create a fake account under an assumed identity, which will contain types of personal data from the defender's vantage point (MITRE: Create Account).

More generally, the attacker regularly creates digital footprints that may include personal data. Such footprints may be left, for instance, in: (i) operating system generated logs or; (ii) telemetry data captured by cybersecurity technologies such as ENISA-endorsed endpoint detection and response (EDR) (ENISA and TeleTrust 2021, Sec. 3.3.22). Such data may contain usernames, file names, IP addresses, and other sorts of personal data or non-personal but protected data.

For the defender, the MITRE framework examines both detection and defense. Approaches to detection of spear phishing include reviewing application log content, network traffic flow, and network traffic content (MITRE: Internal Spearphishing). Network traffic content has numerous possible approaches such as monitoring and analyzing traffic patterns. These patterns may include gratuitous or anomalous traffic patterns, anomalous syntax, anomalies in use of files that do not normally initiate connections for respective protocols); and monitoring network traffic for requests and/or downloads of container images (MITRE: Network Traffic).

Because successful spear phishing results in the attacker having access to a valid account, defenders may still be attempting to detect the attack after the attacker has entered the system (MITRE: APT28). The defender monitors logon sessions looking for suspicious activity. Such activity may include: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; and accounts logged in at odd times or outside of normal business hours (MITRE: Valid Accounts). With regard to the types of data monitored, these monitoring activities would review data such as device ID, time of day, day of week, and geolocation. The patterns from the new logins would then be compared to the historical information to determine if deviation exists (ibid; MITRE: CAR-2013-10-001). This routine defender monitoring would apparently be degraded if the defender could no longer log and review parts of the system that happen to be in a different country. In addition, as discussed in *Effects*, cybersecurity services may be provided remotely, such as when a company operating in the EU staffs its cybersecurity team outside of the EU, hires a vendor who does so, or manages or relies upon global infrastructure.

**iii. Alternatives to Use of Personal Data.** When attempting to detect or defend against spear phishing, the user account suspected to be compromised is generally one of a person affiliated with the targeted organization, often at a high level. Much of the data reviewed during an investigation into such a cyber incident would be personal information, if actually associated

with the person rather than a system account, such as email address, IP address, and geolocation information. Certainly, looking at the historical data of the victim of the attack and building a profile of the victim's habits (and location) over time would be reviewing personal data. In a company that is international, data localization may be particularly impactful. If the person spear phished works in the EU, and the company is based in the U.S., the EU division of the IT department likely could not send information concerning the spear phishing attack to the main IT department in the U.S.

In some instances, it may be possible to create defenses against phishkits consistent with hard data localization. If detection of phishing operated, for instance, on hashed or encrypted versions of personal data, some defensive operations may still operate successfully. Such approaches, however, have not been widely deployed to date and may well be technically infeasible.

**iv. Privilege Escalation and the ENISA Guidelines.** Among other possibly relevant measures, the ENISA Guidelines on "state of the art" include two technical measures directly relevant to defending against privilege escalation.

First is Technical Measure - 3.2.22 - Endpoint Detection and Response: "Ideally, detections are correlated and the technique and tactics (including tools used such as malware, trojans, PowerShell scripting) and the attacker's target are displayed (exfiltration of data, setting up a backdoor, lateral movement within the organization, rights escalation, etc.) are displayed" (ENISA and TeleTrust 2021).

Second is Technical Measure - 3.2.29 Monitoring of Directory Services and Identity-Based Segmentation: "Which IT security threat(s) is the measure used against? Misuse of privileged accounts and escalation of authorization" (ENISA and TeleTrust 2021).

### 2. Impacts to Cybersecurity: Risks from Knowing Less Than the Attacker[8]

An essential part of good cyber defense is for the defenders to test the system through "red teaming," including penetration ("pen") testing. Pen testing may be more familiar to readers. It involves the defense hiring "white hat" attackers to find as many vulnerabilities and configuration issues as possible, exploit them, and determine risk levels (Talamantes). Red teaming is a more general approach, for the defender to identify physical, hardware, software, and human vulnerabilities. In addition to pen testing, red team skills include social engineering, threat intelligence, and reverse engineering (Coursera 2022).

#### a. Pen Testing and Other Red Teaming

Data localization laws would appear to present serious obstacles to pen testing and other red teaming. The intuition is that attackers will be willing to break the law, to seek out and transfer personal data across national borders. By contrast, defenders are obliged to comply with the law. If defenders hire pen testers, those testers would not be able to probe for vulnerabilities that would require learning account information and other personal data, notably where the data is stored in a different country. Since a large fraction of cyber-attacks involve crossing national

borders, the defenders would systematically be able to test and learn about vulnerabilities in their own systems less well than the attackers.

**i. Anatomy of Approach.** Red teaming identifies the risk and susceptibility of attack against key business information assets. The red team effectively simulates the techniques, tactics, and procedures of genuine threat actors, in a controlled manner, and with authorization from the defending organization. The red team assesses the organization's ability to detect, respond, and prevent sophisticated and targeted threats. The red team engages closely with the internal cybersecurity team, including the incident response team, to provide meaningful mitigation and comprehensive post-assessment debriefing (bsi).

Pen testing views the organization through the eyes of a bad actor, seeking to discover cybersecurity vulnerabilities. An effective penetration tester may identify where a hacker might target, how they would attack, how the defenses would fare, and the possible magnitude of a breach. At the conclusion of testing, pen testers generate detailed reports, including examples of successful attacks, screenshots, methodology, and remediation recommendations (Coursera 2022).

ii. **Types of Personal Data.** In order to understand the extent to which pen testing and other red team activities might be affected due to hard data localization, we carried out an academic exercise where we identified what personal data might be needed by defenders to emulate an APT or to detect if any adversarial techniques are currently being employed within an organization. In order to do a systematic and exhaustive study, we used the MITRE ATT&CK framework to help us walk through the techniques employed in each of the 14 tactics and see how many of those would be impacted if personal data were to be removed. Here, we analyzed the techniques for each tactic to deduce what personal data would be needed to detect and defend against them. Based on the nature of information, we identified that the personal data leveraged here would comprise of one or many of the following: IP addresses, email addresses, domains, social media profiles, digital certificates, access tokens, etc.

Our analysis led us to the conclusion that 13 out of the 14 techniques (all tactics except 'Execution') would be negatively impacted by removal of personal data. By impacted, we mean that it would hinder information sharing for cyber defense purposes.

**iii. Alternatives to Use of Personal Data.** Thus far, we have not identified effective alternative strategies for conducting pen testing and red teaming, in the absence of the ability to see specific identifying information concerning individual accounts, file names, IP addresses, log entries, and other information that a pen test would routinely access. In essence, cybersecurity is naturally reliant upon the very protocols and identifiers inherent to modern computing.

**iv. Red Teaming, Pen Testing, and the ENISA Guidelines.** Numerous legal regimes have recommended or mandated penetration testing as an essential component of an organization's overall cybersecurity program. Article 32 of GDPR states that companies must regularly test, assess, and evaluate the effectiveness of technical and organizational measures that

ensure the security of data. ISO 27001 provides that information about technical vulnerabilities "shall be obtained in a timely fashion" and remediated to address the associated risk (isms.online; ibid, Standard A.12.6.1). Requirement 11 of PCI DSS specifically mandates the performance of regular penetration testing for service providers and large merchants (ERMProtect). SOC 2, in CC4.1 and CC7.1, has specific requirements that mention penetration testing and vulnerability management for auditors to review (AICPA) (Fowler). There are specific provisions concerning pen testing in financial services regimes, including under FINRA, SWIFT, and the New York state law governing financial institutions (FINRA; NYAG; SWIFT).

More specifically, ENISA has also noted the effectiveness of penetration testing and related techniques. The ENISA Guidelines include Technical Measure – 3.3.2.12 Technical System Audits: Technical system audits (inspections at the network, system and application level). Such audits "must be performed regularly by or on behalf of the organisation. These are typically carried out as penetration tests or web checks." It adds: "For a comprehensive IS penetration test, in addition to the technical audit, vulnerabilities in the IT systems tested are rooted out through technical investigations using special security tools, among other things. In doing so, the testers access the IT systems to be inspected on site under supervision by the administrators" (ENISA and TeleTrust 2021, 77).

The ENISA Guidelines also include Operational Measure – 3.36 Management of Information Security Risk. It states: "Hardly less difficult is the estimation of probabilities of occurrence. It is advisable to use as many external and internal sources of information as possible. The former includes CVE[22] lists, vendor information, CERT services (e.g., from the BSI), and the latter include the evaluation of information security incidents, penetration tests, audits or awareness measures" (ibid, 89).

## IV. Modeling Quantitative Effects of Data Localization

We next present a model for estimating, in one setting, the quantitative effects of data localization. We first explain reasons why data localization would likely increase the time needed for defenders to spot a new attack. We then provide a quantitative model that indicates that the time for detection will more than double if the Internet is partitioned in half due to localization rules.

### A. Data Localization and the Speed of Detection Matters

As described earlier in the paper, data localization would result in a reduction in observable telemetry. Telemetry in this setting is "data collected from a network environment that can be analyzed to monitor the health and performance, availability, and security of the network and its components, allowing network administrators to respond quickly and resolve network issues in real-time" (BlackBerry). Examples, among many others, include data from Intrusion Detection and Intrusion Prevention systems, and netflows into and out of a system (Lebovitz 2021). Telemetry also includes data about execution, file transfers, configurations, and other observable activity on an endpoint (Karantzas 2021).

Prior research has shown a strong relationship between reducing observable telemetry and the speed of detecting and responding to attacks. Network Telescopes have been previously used to detect Distributed Denial of Service (DDoS) attacks and Internet worm propagation patterns (Moore et al. 2001; Moore et al. 2002). The size of the Network Telescope, i.e. the number of IP addresses used for observation, has a significant impact on the telescope's efficacy (Moore et al. 2004). Similar network effects leveraging global insights and observations have also been used to stop Unsolicited Bulk Email (UBE, "spam") and Business Email Compromise (BEC) (Tang et al. 2008). Beyond network detection, endpoint detection and response (EDR) provides a core set of cybersecurity telemetry used by defenders to is detect adversary activity on devices, including computers, virtual machines, and cloud containers (Karantzas 2021).

Reducing the scope of monitoring can reduce the efficacy of cybersecurity in various ways. First, the activities of an adversary can occur outside of the monitored footprint, slowing detection. Second, the fidelity of monitored quantities can decline. The prevalence of a measured quantity contributes to multivariate analysis using approaches such as machine learning (ML); therefore, reducing quantity reduces the accuracy of inferences about cybersecurity risks. Third, a smaller monitored footprint results in a smaller dataset that can be used for ML training. A smaller dataset especially hobbles modern deep learning-based approaches that require large amounts of data to establish baselines.

Far from achieving state of the art cybersecurity, the reduction in observable telemetry from data localization would likely cause delays in detecting and responding to attacks. Speed is vital to detecting and containing the adversary. Industry data shows the "breakout time," the time until an adversary moves laterally after initial access, averages about one and a half hours (CrowdStrike 2022c). Once the adversary moves laterally, the attack is harder to contain. In light of the high costs from a data breach, moving quickly is vital to limiting damage (IBM 2022). Recognizing the importance of speed in mitigating cybersecurity risks, the U.S. Cyberspace Solarium Commission noted that:

> A company's ability to rapidly, detect, investigate, and remediate network intrusions is a useful indicator of the maturity of its security operations, in its ability both to defend against cyberattacks and to mitigate the types of cybersecurity risks that could harm its business operations and financial conditions (Cyberspace Solarium Commission 2020).

The need for speed is also derived from regulatory requirements such as GDPR's 72-hour breach notification requirement. Consequently, how quickly a defender is ability to collect, analyze, and leverage security-related telemetry data is a key component of modern cybersecurity.

B. A Model for Reconnaissance and Initial Access

To provide a quantitative assessment of the impact of localization requirements on the detection of Advanced Persistent Threats (APTs), we present a high-level model of adversary scanning behavior during reconnaissance.

We assume an adversary is scanning a list of 100 million IP addresses ($N$) for a zero-day vulnerability. We further assume that we need to observe the adversary communicate with a

vulnerable system to distinguish it from a common scan. Furthermore, a cloud-based protection platform is protecting $K$=100,000 of these systems. These systems may be endpoints that run a sensor software, which communicates and coordinates defenses using a global centralized cloud platform. We successfully detect the campaign when the first protected system is contacted by the adversary. From that point forward, mitigations across the population of vulnerable systems can be taken. Hence, the faster we can react, the better.

Localization requirements may force the operator of the centralized cloud to segment the monitored footprint into several isolated domains. As a result, each segmented cloud would have fewer sensor-protected systems available to detect the campaign. For the sake of this analysis, we assume that we segment the cloud into two domains of equal size with $K/2$ systems each.

We assume the adversary scans at a rate $r$ of 60 probes per hour (i.e., one per minute). This rate is based on the adversary's strategy of evading volume-based detection – detection would become easier if the adversary used a higher rate of probes.

To model the problem, we use a hypergeometric distribution, i.e. drawing from a total population $N$ with $K$ instances allowing for detection. The probability that after $n=rt$ probes we achieved $k$ detections is given by:

$$\Pr(X = k) = \frac{\binom{n}{k}\binom{N-n}{K-k}}{\binom{N}{K}}$$

The probability that at time $t$ we achieved more than zero detects is given by:

$$\Pr(X > 0) = 1 - \Pr(X = 0) = 1 - \frac{\binom{n}{0}\binom{N-n}{K}}{\binom{N}{K}} = 1 - \frac{\binom{N-rt}{K}}{\binom{N}{K}}$$

Figure 1 graphs the results of our model. The solid line shows the probability of detecting the attack where the defense can use the full set of sensors. In this scenario, achieving a minimum 80% probability of protection requires 27 hours of observation. The dashed line shows the probability of detecting the attack where localization enables the defense to see only half ($K/2$) of the sensors. To achieve the same 80% probability, it would now take 55 hours.
In summary, using the sort of plausible, simple model seen previously in the literature, reducing the number of sensors in half would result in average detection time for an attack taking more than twice as long.

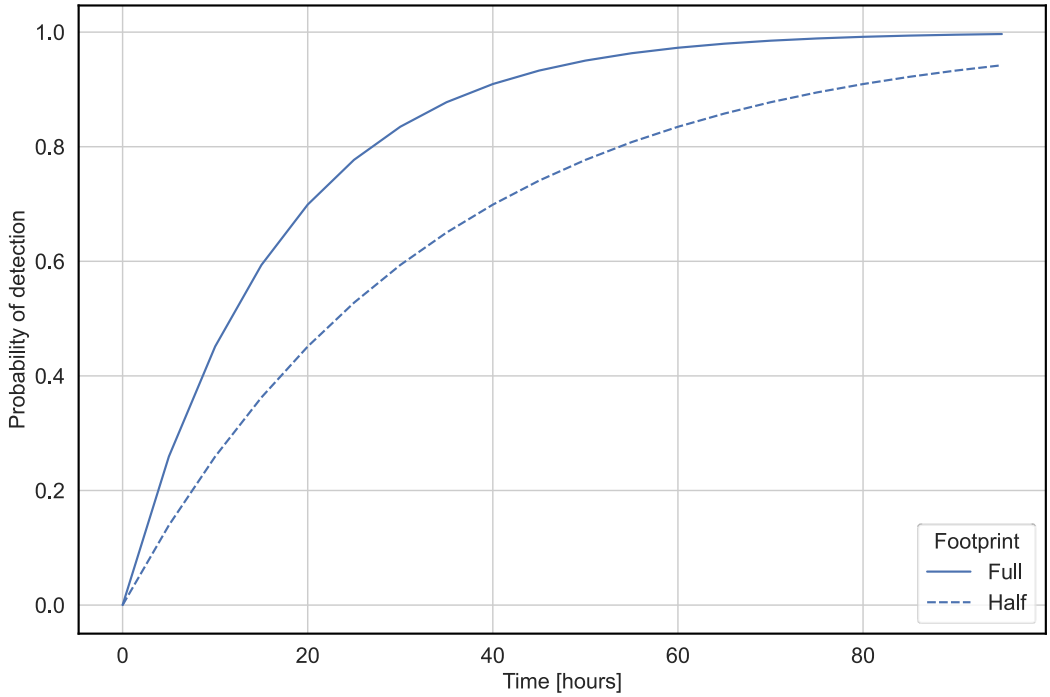



*Figure 1: probability of a sensor monitoring a target chosen by the adversary vs time in hours*

## V. Assessing European Cybersecurity Certification Regimes Requiring Localization

We next turn to recent measures and proposals in the EU to require data localization, justified in the name of improving cybersecurity. We discuss the certification known as SecNumCloud adopted in France, as well as proposals by ENISA and Italian authorities. In light of the multiple and significant risks to cybersecurity from localization, discussed in *Effects* and this paper, it is logical that such measures and proposals should at a minimum consider the risks to cybersecurity from localization, along with consideration of claimed benefits.

ENISA is currently considering the European Union Cybersecurity Certification Scheme on Cloud Services (EUCS). The EU Cybersecurity Act of 2019 called on ENISA to assist with the preparation of 'candidate cybersecurity certification schemes.' ENISA launched a public consultation in 2020 and proposed its first draft of the EUCS in 2021 (ENISA: Certification). The task for the EUCS is to provide a voluntary, EU-wide framework for the certification of the cybersecurity of cloud services. The certification is supposed to counter fragmentation between the EU member states, while facilitating trade and understanding of security features by harmonizing the security of cloud services with EU regulations, international standards, best industrial practices, and existing certifications in EU Member States. Although the certification would be generally voluntary, the high assurance level is expected to become mandatory for the

essential services listed under the EU Network and Information Security 2 (NIS2) Directive (EU Directive 2022/2555, 80-152).

ENISA has considered basing the EUCS on the cybersecurity certification known as SecNumCloud, developed by France's national cybersecurity agency, ANSSI, in 2016 (ANSSI). As updated in 2022, SecNumCloud has two related localization requirements (Prime Minister of France 2021a). First, it requires defined cloud services and other organizations to prohibit data and system access from organizations located outside the EU. This requirement requires data to be stored locally and use only local support and technical staff (Cory 2021). Second, it requires cloud providers to be "immune to any extra-EU regulation," with strict limits on foreign ownership and representation on a company's board of directors (Propp 2022; Prime Minister of France 2021b; Cory 2021).

Several member states have opposed this approach, which would prohibit Software as a Service and cloud services generally that store data outside of the EU (Bertuzzi 2021). The U.S. government has raised concerns about possible violation of international trade agreements (Propp 2022). Other EUCS' critics have described "limited transparency and lack of stakeholder engagement" in ENISA's drafting process, and say ENISA should focus instead on "the actual technicalities of cybersecurity" rather than base cloud service provision on national origin (Digital Europe 2022; Cory 2023).

Going beyond certifications, Italy considered but later rejected a draft presidential decree with strict localization rules for cybersecurity services. As originally drafted, Italy would have implemented the 2017 European Network and Information Security Directive (NIS I) to set requirements on functions and services covered by its National Cybersecurity Perimeter legislation (EU Directive 2022/2555, 80-152). The original requirement would have effectively meant that organizations deemed part of Italy's cybersecurity perimeter could only adopt the cybersecurity technologies and practices endorsed by ENISA if the requisite infrastructure and workforce was solely in Italy. According to FAQs issued by the Italian National Cybersecurity Agency (Agenzia per la Cybersicurezza Nazionale), the proposed localization constraints were aimed at facilitating interactions with the supervisory authority in case of incidents having an impact on national security. The stated goals, among others, were to verify the implementation of security measures through physical on-site inspections, as well as verification and assessment of possible causes of incidents.

As discussed in this paper, such localization proposals run counter to the cybersecurity "state of the art," as set forth by ENISA and other government agencies. Moving forward, our research suggests that ENISA should, at a minimum, consider the risks to cybersecurity from localization before adopting localization measures (Digital Europe 2022). In addition, transfers of data for cybersecurity purposes can be fostered within the ongoing political dialogue supporting Data Free Flow with Trust (DFFT), the approach proposed by former Japanese Prime Minister Abe at the World Economic Forum (Davos Conference) in January 2019 (WEF 2020; Arasasingham and Goodman 2013). The DFFT concept promotes the international free flow of

data useful for addressing business and social issues while ensuring trust in privacy, security and intellectual property rights. Consistent with the DFFT approach, the Organisation for Economic Co-operation and Development (OECD) in 2022 published its Declaration on Government Access to Personal Data Held by Private Sector Entities. This Declaration announced common principles for government access to data held by the private sector, to safeguard privacy when accessing personal data for national security and law enforcement reasons.

## VI. Conclusion

In our first paper, *Effects*, we provided a framework for understanding the effects of data localization on cybersecurity, based on effects within an organization, across organizations for payment, and across organizations without payment. This paper complements that analysis, with greater focus on technical measures, for the techniques, tactics, and procedures of threat actors and defenders. We have used the ENISA Guidelines and the MITRE ATT&CK Framework as authoritative approaches for cataloguing relevant TTPs. In this paper, we have focused on the example of data localization in the European Union, but similar analysis would apply to any countries contemplating such a localization regime that restricts data transfers.

We have used examples to highlight two themes for when data localization laws appear to pose particularly severe obstacles to cybersecurity. The first theme concerns "the who and the what" of attackers. Threat hunting and threat intelligence are core activities for defenders, but they involve analysis of identifying information, including account names, IP addresses, and many other types of potentially personal data. Our other example concerns privilege escalation, where attackers seek to move laterally in an organization to reach their objectives. As the spear phishing example illustrates, organizations analyze telemetry and information of many sorts, to detect initial intrusions and follow clues across the organization to detect and then respond to APTs and other intruders (OECD 2022).[9]

The second theme concerns pen testing and other forms of red teaming. Put simply, there are risks where defenders know less than attackers. Yet data localization laws block pen testing and other forms of red teaming whenever the probe moves from part of the organization (in one country) to another part of the organization (in another country). The same analysis applies if the red teaming applies to the increasingly important portion of cybersecurity focused on supply chain. Organizations today often purchase services and infrastructure from other organizations, in ways that implicate the purchaser's cybersecurity if there are vulnerabilities in the supply chain. Effective red teaming today includes a comprehensive approach to an organization's risks, including from vendors. Thus, even where a company operates only in one jurisdiction, there are often dependencies on other jurisdictions. Even though pen testing is expected or required for many organizations, data localization laws thus put at risk the effectiveness of such pen testing.

As we continue this research, we welcome comments and suggestions about other ways that data localization laws may affect risks to defenders' TTPs. For now, we close with three implications of the research.

First and most generally, we recommend that cybersecurity experts and government agencies examine the risks detailed in this paper. For instance, before ENISA takes any action to localize cybersecurity services, we believe it important for ENISA to consider how any proposal would impact the state of the art mandated by ENISA, for activities such as threat hunting, preventing escalation of privileges, and red teaming/pen testing. Our research to date has not discovered any such analysis by ENISA. Relatedly, we have not thus far seen discussion by ENISA of how Article 32 of GDPR and ENISA's state-of-the-art requirements can be achieved consistent with the strict sort of localization that data protection regulators have supported in recent enforcement cases.

Second, where policymakers decide in favor of data localization, we urge consideration of creating cybersecurity exceptions. Such exceptions might be relatively general, such as use of personal data for cybersecurity purposes. Alternatively, exceptions could be more targeted, such as permitting use of personal data for pen testing, incident response, and other specific purposes.

Third, the risks to cybersecurity from localization – including effects on individuals, corporations, and national security – should be analyzed together with any claimed benefits. The claimed benefits of localization may include less lawful access by governments and other actors who seek data held outside of the country. Empirically, it is far from clear whether risk systematically increases with data transfer, or that most types of data shared for cybersecurity purposes would actually be of any interest to other governments. Whatever the actual risks from transferring data, it seems irrational to use data localization as a proxy, or even pillar, for data protection and to focus only on possible benefits from restricting data flows while ignoring known, likely, and apparently substantial risks to cybersecurity. This has the unintended effect of disincentivizing the adoption of practical, EU-endorsed cybersecurity best practices. In sum, until and unless proponents of localization address these concerns, scholars, policymakers, and practitioners have strong reason to expect significant cybersecurity harms from hard localization requirements.

---

## Notes

[1] The statements in this document are solely by the authors and should not be attributed to the Cross-Border Data Forum, CrowdStrike, or any client. For research support on this project, the authors thank the Center for International Business and Education at Georgia Tech, the Cross-Border Data Forum, the Georgia Tech Scheller College of Business, the Georgia Tech School of Cybersecurity and Privacy, and Microsoft. The authors thank Nathan Lemay for his substantial initial research contributions to this paper.

[2] After (*Breyer*, 2020), static IP addresses could fall in the scope of personal data within the meaning of Directive 95/46/EC, as far as they provide sufficient information on the history of a user and make it possible to identify him.

[3] GDPR is based on "a risk-based approach in terms of its protection objectives."

[4] See (Bagley, 2022). "Four Takeaways as the European Union's General Data Protection Regulation (GDPR) Turns 4." *Security Senses*, May 26. https://securitysenses.com/posts/four-takeaways-european-unions-general-data-protection-regulation-gdpr-turns-4. By design, the state of the art is not a static requirement, as cybersecurity risks evolve rapidly.

[5] Indicators of Compromise (IOCs) include file hashes, IP addresses, and domain names. An important distinction between a technique in ATT&CK and an IOC is that many of the ATT&CK techniques are legitimate system functions that can be used for malicious purposes, whereas an IOC deployed as an intrusion detection mechanism is typically an indication of an action known to be caused by or under the influence of an adversary.

[6] The authors thank Nathan Lemay for his early suggestion to focus on the threat hunting/threat intelligence example.

[7] Commenters have asked us whether personal information about the attacker would also be covered by data localization laws. To date, we are not aware of any data localization law that would ban transfers generally but allow transfers to detect criminal cyber-attacks. We note, however, the analogy to the "hacker trespasser" provision in Section 217 of the USA-PATRIOT Act. https://www.justice.gov/archive/ll/subs/add_myths.htm#s217. Under that provision, the owner of the computer system may request law enforcement assistance to monitor trespassers in the system, without violating otherwise-applicable wiretap laws that would prohibit providing the information to law enforcement. In both settings, it would seem perverse to protect the hacker/trespasser's personal data from the system owner and law enforcement seeking to counter the criminal intrusion.

[8] The co-author Avani Modak played the leading role on researching red teaming and pen testing.

[9] Another unintended consequence of data localization is that attackers and their wrongful activity may be protected by the data protection regimes, making it harder to detect their activity. Attackers thus may seek to locate their activity hubs (either actual or appear to be located) within countries or regions with strict data localization mandates.

## Notes On Contributors

***Peter Swire*** is J.Z. Liang Chair, Georgia Tech School of Cybersecurity and Privacy, and Professor of Law & Ethics, Georgia Tech Scheller College of Business. He is Research Director of the Cross-Border Data Forum and senior counsel with Alston & Bird LLP.

***DeBrae Kennedy-Mayo*** is a faculty member in the Georgia Tech Scheller College of Business and a Senior Fellow, the Cross-Border Data Forum.

***Drew Bagley*** is Vice President & Counsel, Privacy and Cyber-Policy, CrowdStrike and an adjunct faculty member, American University School of Public Affairs.

***Sven Krasser*** is Senior Vice President & Chief Scientist, CrowdStrike.

***Avani Modak*** is a Masters in Cybersecurity graduate of the Georgia Tech School of Cybersecurity and Privacy.

***Christoph Bausewein*** is Assistant General Counsel, Data Protection & Policy, CrowdStrike.

## References

AICPA. 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, (March 2020)

https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria-2020.pdf

ANNSI. "European Secure Cloud – A New Label for Cloud Service Providers." https://www.ssi.gouv.fr/en/actualite/european-secure-cloud-a-new-label-for-cloud-service-providers/.

Arasasingham, Aidan and Goodman, Matthew. 2013. "Operationalizing Data Free Flow with Trust (DFFT)." *Center for Strategic and International Studies*, April 13. https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft.

Austrian Data Protection Authority (ADPA) decision, as issued on 22 December 2021. https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf (original German), https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf (unofficial English translation)

Bagley, Drew. 2022. "Four Takeaways as the European Union's General Data Protection Regulation (GDPR) Turns 4." *Security Senses*, May 26. https://securitysenses.com/posts/four-takeaways-european-unions-general-data-protection-regulation-gdpr-turns-4.

Baker, Kurt. 2023. "What is Cyber Threat Intelligence?" *CrowdStrike*, March 23. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence.

Bertuzzi, Luca. 2021. "Germany calls for political discussion on EU's cloud certification scheme." *Euractiv*, September 21. https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/.

BlackBerry. "Telemetry for Cybersecurity." https://www.blackberry.com/us/en/solutions/endpoint-security/extended-detection-and-response/telemetry.

bsi. "What is red teaming and what are the benefits to my business?" https://www.bsigroup.com/en-IE/Blog/digital-trust--blog/what-is-red-teaming-and-the-benefits-to-organizations/#:~:text=A%20red%20team%20assessment%20is,the%20business%20into%20the%20future.

Christakis, Théodore. 2020. "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy." December 7. doi: 10.2139.

Cory, Nigel and Dascoli, Luke. 2021. "How Barriers to Cross-Border Data Flows are Spreading Globally, What They Cost, and How to Address Them." *Information Technology & Innovation Foundation*, July 19. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

Cory, Nigel. 2021. "'Sovereignty Requirements' in French—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners." *Information Technology & Innovation Foundation*, December 10. https://itif.org/publications/2021/12/10/sovereignty-requirements-france-and-potentially-eu-cybersecurity/.

Cory, Nigel. 2023. "Europe's Cloud Security Regime Should Focus on Technology, Not Nationality." *Information Technology & Innovation Foundation*, March 27. https://itif.org/publications/2023/03/27/europes-cloud-security-regime-should-focus-on-technology-not-nationality/.

Coursera. 2022 "Red Team vs. Blue Team in Cybersecurity." November 1. https://www.coursera.org/articles/red-team-vs-blue-team.

CrowdStrike, "Indicators of Attack (IOA) v. Indicators of Compromise (IOC)." https://www.crowdstrike.com/resources/white-papers/indicators-attack-vs-indicators-compromise/.

CrowdStrike. 2022c. "Global Threat Report 2022." https://www.crowdstrike.com/global-threat-report/.

CrowdStrike. 2022s. “IOA VS IOC.” October 5. https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/.

CrowdStrike. 2022b. “What is Privilege Escalation.” June 3. https://www.crowdstrike.com/cybersecurity-101/privilegeescalation/#:~:text=A%20privilege%20escalation%20attack%20is,operating%20systems%20or%20web%20applications.

CrowdStrike. 2023a. “Advanced Persistent Threat (APT).” February 28. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.

CrowdStrike. 2023b. “Lateral Movement.” April 17. https://www.crowdstrike.com/cybersecurity-101/lateral-movement/.

CrowdStrike. 2023c. “Global Threat Report 2023.” https://www.crowdstrike.com/global-threat-report/.

Cybereason Global SOC Team. 2022. “Threat Analysis Report: DLL Side-Loading Widely (Ab)Used,” *cybereason*, October 26. https://www.cybereason.com/blog/threat-analysis-report-dll-side-loading-widely-abused.

Cyberspace Solarium Commission, Cyberspace Solarium Commission Report, March 2020, p. 83, https://www.solarium.gov/report

Declaration on Government Access to Personal Data Held by Private Sector Entities. 2022. *Organisation for Economic Cooperation and Development (OECD)*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

Digital Europe. 2022. “Joint Letter on ‘sovereignty requirements’ in candidate European Cybersecurity Certification Scheme for Cloud Services.” June 16. https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/06/DIGITALEUROPE_Joint-letter-on-%E2%80%98sovereignty-requirements-in-candidate-EUCS.pdf.

Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) , OJ L 333, 27.12.2022, p. 80-152.

Directive 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022, p. 164-198.

Discreto del Presidente del Consiglio dei Ministri 14 Aprile 2021. https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg, n. 81.

EDPB. 2021. “Recommendations 01/2020 on measures that supplement transfer tools.” June 18. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

ENISA. 2019. “What is ‘State of the Art” in Cybersecurity?” February 7. https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security.

ENISA and TeleTrust. 2021. “IT Security Act (Germany) and EU General Data Protection Regulation: Guideline ‘State of the Art’ Technical and Organisational Measures.” https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf.

ENISA. “The European Union through ENISA is developing EU cybersecurity certification which provides evidence of compliance to a given level of trust.” https://www.enisa.europa.eu/topics/certification.

ERMProtect Staff. “Penetration Testing for Compliance.” *ERMProtect*. https://ermprotect.com/blog/penetration-testing-for-compliance/.

European Commission. 2022. “Proposal for a Regulation of the European Parliament and of the Council of 23 February 2022 on harmonised rules on fair access to and use of data (Data Act).” Brussels, COM (2022) 68 final.

European Commission. “What is Personal Data.” https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

European Data Protection Board (EDPB). 2023. “Guidelines 9/2022 on personal data breach notification under GDPR version 2.0.” March 28. https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

European Union Agency for Cybersecurity (ENISA). 2020. “Cloud Certification Scheme: Building Trusted Cloud Services Across Europe.” December 22. https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme.

Falcon OverWatch Team. 2021. “Nowhere to Hide: 2021 Threat Hunting Report.” *CrowdStrike*. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021ThreatHunting.pdf, p. 33.

Financial Industry Regulatory Authority (FINRA). 2018. “Report on Selected Cybersecurity Practices – 2018.” December. https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf.

Fowler, Adam. “SOC 2 CC4: Common Criteria related to Monitoring Activities.” *Design Compliance and Security*. https://www.designcs.net/soc-2-assessments-common-criteria-related-to-monitoring-activities/.

French Commission nationale de l'informatique et des libertés (CNIL) decision, as issued on 10 February 2022. https://www.cnil.fr/sites/default/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf

Future of Privacy Forum. 2014. “MAC Addresses and De-Identification.” March 27. https://fpf.org/blog/mac-addresses-and-de-identification/.

Government of France: Office of the Prime Minister. 2021a. “Circular No. 6282-SC of July 5, 2021 relating to the doctrine for the use of cloud computing by the State.” July 5. https://www.legifrance.gouv.fr/circulaire/id/45205?page=1&pageSize=10&query=*&searchField=ALL&searchType=ALL&sortValue=PUBLI_DATE_DESC&tab_selection=circ&typePagination=DEFAULT.

Government of France: Office of the Prime Minister. 2021b. “SecNumCloud.” https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a.pdf.

IBM. 2022. “Cost of a Breach Report 2022.” https://www.ibm.com/resources/cost-data-breach-report-2022.

In Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (16 July 2020), Court of Justice of the European Union.

In Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland (19 October 2020), Court of Justice of the European Union.

isms.online. “ISO 27001 Annex A.12.1.” https://www.isms.online/iso-27001/annex-a-12-operations-security/.

Karantzas G, Patsakis C. An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. *Journal of Cybersecurity and Privacy*. 2021; 1(3):387-421. https://doi.org/10.3390/jcp1030021

Kime, Chad. 2023. “Top 7 Threat Intelligence Platforms.” *eSecurity Planet*, February 10. https://www.esecurityplanet.com/products/threat-intelligence-platforms/.

Lebovitz, Gregory. 2021. “Network security threat detection – Comparison of analytics methods.” *Google Cloud*, September 16. https://cloud.google.com/blog/products/networking/when-to-use-5-telemetry-types-in-security-threat-monitoring.

MITRE. “APT28.” https://attack.mitre.org/groups/G0007/.

MITRE. “Create Account.” https://attack.mitre.org/techniques/T1136/.

MITRE. “Enterprise Matrix.” https://attack.mitre.org/matrices/enterprise/.

MITRE. “Internal Spearphishing.” https://attack.mitre.org/techniques/T1534/.

MITRE. “Network Traffic.” https://attack.mitre.org/datasources/DS0029/#Network%20Traffic%20Content.

MITRE. “Updates April 2023.” https://attack.mitre.org/resources/updates/updates-april-2023.

MITRE. “Valid Accounts.” https://attack.mitre.org/techniques/T1078/.

Moore, David, Colleen, Shannon, and Brown, Jeffery. 2002. "Code-Red: a case study on the spread and victims of an Internet worm." *Internet Measurement Workshop (IMW)*. https://catalog.caida.org/paper/2002_codered.

Moore, David et al. 2004. "Network Telescopes: Technical Report." *Cooperative Association for Internet Data Analysis (CAIDA)*. https://catalog.caida.org/paper/2004_tr_2004_04.

Moore, David, Voelker, Gregory and Stefan Savage. 2001. "Inferring Internet Denial-of-Service Activity." *USENIX Security Symposium*. https://catalog.caida.org/paper/2001_backscatter.

Moulinos, Konstantinos and Pauna, Adrian. 2013. “Good practice framework for an EU ICS testing coordination capability.” *ENISA*, December. https://icscsi.org/library/Documents/Best_Practices/ENISA%20-%20Good%20Practices%20for%20an%20EU%20ICS%20Testing%20Coordination%20Capability.pdf.

National Institute of Standards and Technology (NIST). “tactics, techniques, and procedures.” https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures.

New York State Attorney General (NYAG). “Report a Data Breach.” https://ag.ny.gov/internet/data-breach.

Portugal National Data Protection Commission. 2021. “CNPD Suspends Flows to the US.” April 27. https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/.

Propp, Kenneth. 2022. “Cybersecurity Regulation Takes a Sovereign Turn.” *European Law Blog*, September 12. https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.

Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 199, Rec. 49.

Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15-69 .

Selzer, Annika. 2021. “The Appropriateness of Technical and Organisational Measures under Article 32 GDPR.” *European Data Protection Law Review*, 2021(1): 120-128. doi:10.21552/edpl/2021/1/16.

Strom, Blake et al. 2017. “Finding Cyber Threats with ATT&CK-Based Analytics.” *MITRE*, June 22. https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics.

Swire, Peter & Kennedy-Mayo, DeBrae. 2022. “The Effects of Data Localization on Cybersecurity – Organizational Effects. SSRN, June 22. https://ssrn.com/abstract=4030905.

Talamantes, Jeremiah. “Penetration Testing vs. Red Teaming: What’s the Difference?” *Red Team Secure*. https://www.redteamsecure.com/blog/penetration-testing-vs-red-teaming.

Tang, Yuchun et al. 2008. “Support Vector Machines and Random Forests Modeling for Spam Senders Behavior Analysis.” *Proceedings of the IEEE Global Communications Conference*. doi: 10.1109.

Taschler, Scott. 2023. “What is Cyber Threat Hunting?” CrowdStrike, April 17. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/.

World Economic Forum (WEF). 2020. “Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows.” June 10. https://www.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows.

# EXHIBIT 29

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# ISSUE BRIEF

## COMPETITION & CROSS-BORDER ACCESS TO DATA

US supply chain resilience depends on competitive market conditions, characterized by open competition and low barriers to entry. As the DoJ Antitrust Division states in its submission in this same review, USTR should advance "trade policy [that] promotes competitive, diversified, resilient, and innovative supply chains."[i] Such diversified and competitive supply chains depend, first and foremost, on cross-border access to knowledge, information, and data by enterprises and workers in the United States and abroad. The converse is also true: when foreign governments improperly block or impede data transfers and access to information, they distort the marketplace in ways that negatively affect virtually all enterprises and workers across the supply chain.

**First**, cross-border data restrictions and data localization mandates are particularly harmful to competition because they disproportionately impact smaller firms, which lack the resources to develop in-country data centers. Allowing trading partners to arbitrarily mandate data localization and restrict data transfers raises new barriers to entry and increases the power of incumbents and "foreign monopolies and firms that are state-owned [or] state sponsored" – contrary to the President's Executive Order on Competition. For example, USTR inaction on data localization mandates imposed by Asia-Pacific trading partners will likely ultimately augment the market power of large regional cloud service providers (e.g., such as Alibaba or Huawei Cloud), effectively increasing the reliance of both local, US, and other foreign enterprises on these entities.[ii] This outcome does not promote US supply chain resilience.

**Second**, allowing foreign governments to impose undue restrictions on US cross-border access to data from abroad will only amplify the market power of those that have already amassed massive data sets. Ironically, USTR's refusal to negotiate with allies on cross-border data policy, which the USTR has premised on a stated desire to disfavor a "very small number of extremely powerful and dominant companies," could foreseeably have the opposite effect. Permitting foreign governments to impede access to cross-border data sources for all Americans (including students, consumers, workers, small business, and all other types of companies) threatens their interests more than it disfavors the largest US data aggregators already in possession of massive data sets. By refusing to challenge foreign governments when they block or impede US access to new sources of overseas data, USTR's actions artificially inflate the value of data sets that are already held by a very small group of data aggregators. USTR may, in effect, be creating a sheltered market that confers artificially augmented market and pricing power on such entities – at the expense of other US businesses and persons. As AI's importance grows, preserving marketplace competition requires safeguarding cross-border access to information for everyone, so that economic benefits don't simply flow to a select few.

**Third**, there is no conflict between antitrust and cross-border data norms at issue here. Nothing in these US trade rules on cross-border data (which are based in US law) would impede new antitrust legislation or enforcement in the United States. Rather, by refusing to take actions that would benefit the entire economy, the USTR created unnecessary controversy that distracted from efforts to legislate solutions to new competition challenges relating to gatekeeper platforms and the app economy. Instead of supporting the specific legislative efforts of Senators and Representatives who had long sought to address these gatekeeper platform and app economy issues, USTR effectively created a huge distraction that undermined those legislative efforts. USTR's surprise reversal of longstanding US policy on cross-border data galvanized a large and diverse coalition in opposition to the USTR's inexplicable policy stance. The coalition comprises industry groups in every sector, individual enterprises, small business groups, public interest groups, academics, and over 100 lawmakers. While many of these groups might otherwise have supported – or have been neutral on – the abovementioned legislative efforts, USTR's missteps made further progress on those issues much more difficult.

For all of the foregoing reasons, protecting competition in the manner described by the DoJ Antitrust Division requires agreeing with allies to refrain from cross-border data policies that distort markets, including policies in the form of arbitrary, disguised, discriminatory, or unnecessary cross-border data barriers, data localization mandates, digital customs duties, or other digital trade barriers.

[i] https://www.regulations.gov/comment/USTR-2024-0002-0152

[ii] *See e.g.,* Global Data Alliance, *Comments on Thailand Cloud Security Policy* (2024), at: https://globaldataalliance.org/wp-content/uploads/2024/05/en05142024gdacloudsec.pdf This policy requires localization of data in Thailand and localization of backup data in either Southeast Asia or parts of China.

# EXHIBIT 30

# Why Financial Services are Vital to US International Economic Strategy

Type: Podcasts

Date: September 14, 2021

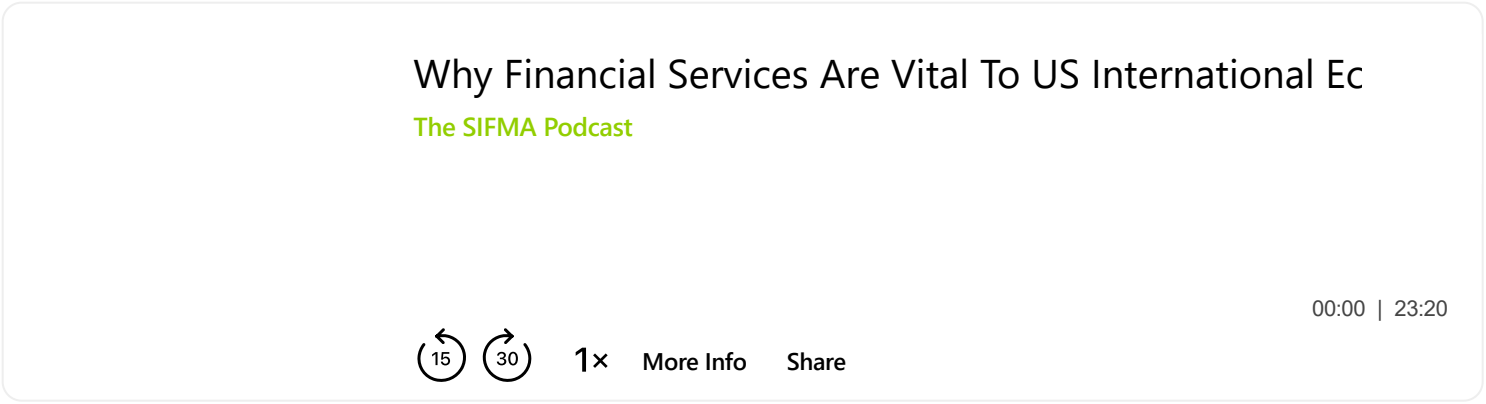
By: Peter Matheson, Douglas Bell and Kimberley Claman

Issue: International Trade and Investment

## *A Conversation with Citi and EY*

International trade and investment in financial services is crucial to U.S. economic growth and job creation.

In this podcast, SIFMA managing director Peter Matheson sits down with Kimberley Claman, Director of International Government Affairs at Citi and Chair of SIFMA's International Policy Committee, and Douglas Bell, Global Trade Policy Leader at EY and previously a senior trade policy advisor for the U.S. Department of the Treasury, U.S. Trade Representative (USTR) and the White House, to discuss why cross-border financial services are so important. Their conversation builds on SIFMA's whitepaper, Financial Services and Main Street Supporting American Economic Growth and U.S. Competitiveness. This white paper demonstrates the fundamental role the U.S. financial services industry plays in the U.S. economy and highlights that, in an increasingly competitive global economy, it is vital that financial services are integrated into the U.S. international economic strategy.




# Transcript

*Edited for clarity*

**Peter Matheson:** Thanks for joining us for this episode in SIFMA's podcast series. I'm Peter Matheson and I'm Managing Director of International Policy and Advocacy at SIFMA. We are here today to answer the question as to why international trade and investment in financial services is crucial to see economic growth and job creation. In SIFMA's new white paper, Financial Services and Main Street Supporting American Economic Growth and U.S. Competitiveness, is a primer on this issue and was published in June.

We developed this white paper to demonstrate the fundamental role the U.S. financial services industry plays in the U.S. economy and to highlight that in an increasingly competitive global economy it is vital that financial services are integrated into the United States's international economic strategy.

To discuss why cross-border financial services are so important to the whole U.S. economy and the other issues set forth in the white paper I'm pleased to be joined today by Kimberley Claman, Director of Global Government Affairs at Citi and also currently Chair of SIFMA's International Policy Committee, and by Douglas Bell, Global Trade Policy Leader at EY and previously a Senior Trade Policy Official in Treasury, USTR, and the White House.

Kimberley and Doug, welcome. Let's get started with our first question. There's a huge focus right now in the U.S. economy on the goods position part of it, including the manufacturing sector and its associated supply chain and a strong desire to see those sectors rejuvenated and to grow. How do financial services get into that picture? Let's start with you, Doug.

**Douglas Bell:** Well, thanks, Peter, and it's great to be here, and that's a great question to start us off with. I think it's, you know before we kind of get going on that I think it's worth just reflecting on why is it such a major focus right now. And I think we look, you know if we're all experiencing the supply chain

aspect of it when you go to the store and you have the clerk telling you that your favorite mayonnaise isn't there because of supply chain issues, it's really on everyone's mind.

And then that's a function of a couple of things, right? I mean we have the pandemic and everything that has been going on with that, and the bottlenecks that it has introduced. It has also highlighted vulnerabilities in the supply chain, the concentration in manufacturing in certain jurisdictions.

You layer on that sort of the political and economic security concerns that are out there and you sort of have this perfect storm of, you know a real focus and the perceived need to really maybe make some adjustments, you know where goods are manufactured, building in greater resiliency into supply chains.

But what's really interesting, and this is the first point I really want to make, is that in that conversation what you don't hear is the bottlenecks in the financial system, or how the financial system, whether it's trade finance or other areas, are really contributing to sort of that challenging environment that we're talking about. And that's really worth commenting on because that has not always been the case in the past.

With the financial crisis in 2008, 2009, that trade finance, for example, was a real problem. So that is a testimony to sort of how well functioning the financial system, you know the valuable regulation that has taken place and then just how well the system is serving. So if financial services are not part of the problem is the financial system part of the solution, and I think the answer there is a definite yes. And I think that that solution takes a couple of different forms.

First and foremost is well-functioning capital markets and financial intermediation to really address the needs that, you know the focus on manufacturing and supply chain. These things aren't going to happen by themselves. They're not necessarily self-funding so firms are really going to need to sort of, you know if building back better means accessing funds through capital markets or banking and they're really is a real important role to play.

And it's also, and I think Kimberley will comment on this too, is directly through payment systems and other schemes that have been used by companies to transfer funds the financial system has been an incredibly important part of it. So I think when you just take a step back, look at the big picture, it's pretty clear that the financial system has a really important and positive role to play in the transition that we're envisioning in both manufacturing and supply chains.

**Peter Matheson:** Thank you, Doug. Kimberley?

**Kimberley Claman:** Thank you, Peter, and great to be here with you and Doug today. I like what Doug said about let's take a step back for a second and think about the fact that financial institutions provide

capital to every sector of the U.S. economy and that it's crucial to allowing firms and industries to invest and innovate, grow and create jobs.

It's important to recognize the dynamism that this capital unleashes and through investments in agriculture, manufacturing, and other service industries the positive impact of finance multiplies and helps generate much more in terms of growth and jobs than the financial sector accounts for directly. And manufacturing is a powerful example of the importance of financial services in the supply chain and as a foundation of the whole economy.

I want to just give three examples of how the financial services industry is fundamental to U.S. manufacturing, to its operations and helping to employ 12 million people throughout the economy. First, the spectrum of financial services provided to manufacturers is wide-ranging, including financing for research, construction of plants, production, and the supply chain to get manufactured goods to customers in the U.S. and overseas markets.

I want to pick up on one point that Doug alluded to in his remarks which is on trade finance. Trade finance is a crucial way in which financial services firms support U.S. manufacturers. And just to give a little detail trade finance represents the financial instruments and products that are used by companies to facilitate international trade making it easier for importers and exporters to transact business.

It's used to protect against international trade's unique inherent risks such as currency fluctuations, political instability, issues of nonpayment, or the creditworthiness of one of the parties involved. Estimates suggest it is worth around $75 billion per annum. It really demonstrates the point of how important finance is to manufacturing. Finally, the presence of an international financial services industry is also qualitatively important to the global success of our manufacturing base.

For U.S. manufacturing to succeed internationally it is crucial that it has access to global finance and the expertise that goes with it.

**Peter**: Thank you, Kimberley. We're hopefully now emerging from the COVID crisis, which has been with us now in the United States for around 16 or 17 months. It has affected all of us, it has affected the business community and the economy and people's everyday lives. How is the financial services industry engaged with countries and communities wrestling with the huge challenges posed by COVID? Let's direct this question to Kimberley.

**Kimberley**: Thanks, Peter. This has certainly been a challenging year, year and a half for everyone. I'm really hopeful that everyone is doing well and being safe and in good health. The U.S. financial services industry is fundamental to our economy and that matters every day of the year. But the past year and a half has demonstrated particularly vividly how central to our livelihoods financial services are. Financial

firms have been integral in helping our communities mitigate many of the economic effects of the COVID-19 pandemic.

This proactive support to communities across the country has taken multiple forms and has ranged from help to individuals, to small businesses, and governments. I'll highlight just a few examples. Financial firms have led the huge increase in social bond issuance to help respond to the crisis. These bonds have raised funds for health care provision, nursing homes, and various forms of support to low-income and unemployed groups.

Early in the crisis banks eliminated fees on a wide range of products and took steps to expand access to digital banking tools such as the acceleration of the availability of contactless payment via credit cards. In fact, according to a study by a global management consulting firm between March 2019 and April 2020 overall contactless card usage in the U.S. grew by 150 percent.

Financial services firms also administered the paycheck protection program loan applications for small business owners and have been critical to intermediating a wide variety of government support measures to support individuals, firms, and the wider economy. And because capital markets and financial institutions are fundamental to saving, investment, and job creation it will also be essential to the recovery for the COVID-19 crisis in every sector of the U.S. economy.

**Peter**: Thank you, Kimberley. We've already discussed the focus on the composition of the recovery in terms of growth of manufacturing, growth of services, and the linkages between those sectors, how services, financial services in particular, contribute to the rest of the economy and help those then grow. But as we see economies recover from the COVID crisis there's also a strong focus on the quality of economic growth, not just its quantity.

And by that one particularly important dimension will be the sustainability of the recovery from an environmental perspective. What part can financial services play in helping realize that? Let's direct that one to Doug.

**Douglas**: Right, well, thanks, Peter. You know I think I would answer, there's kind of a two-part answer to that. The first is a little bit of what, well, not a little bit, a lot of what Kimberley has been describing in terms of sort of the role of the financial system and in terms of developing economic growth, allocating capital, and when we think of the scope of what is going to be required to put the global economy less carbon-intensive basis, it's profound.

And we talked about the rather large scale involved in recovering from COVID and these supply chain shocks to start us off, but this dwarfs that. If you just think of an industry just like steel and the critical role that it plays, you know what does it mean to have clean steel and sort of the capital investment required

to do that, you're talking trillions of dollars. And so the ability to mobilize that capital, to direct that capital, the financial system plays that role.

And so if that's to happen the financial system is going to have to be able to do that effectively. And I think we do have that system in place, but it's going to really require all elements, whether it's capital markets, banking, venture capital, all the different cylinders of the financial system having to operate at full capacity. That's one aspect. The other piece which I think is just starting to emerge and which is going to be incredibly important is sort of the whole what I would call pricing of climate risk.

And you know we started to see that, of course, in the financial markets where you now have big investors saying that we need to look at climate risk, that's an important part of valuation. And that is a way, you know those types of tools and those mechanisms are really how you start to incentivize behavior and in a way that goes beyond the role that governments can play for example because the scope and the scale of this transition that I'm describing will have to, it will require a huge private sector component to it.

In fact, in many regards it'll have to be, if we're to be successful it will have to be driven by the private sector. So putting in place that ability to sort of capture that risk, price for that risk, and use that to allocate capital will be incredibly important over time and I think will be one of the secrets. And so we see it in other aspects as well in terms of like corporate reporting, again, starting to be driven by, you know out of the securities markets.

But all those things are going to play an incredibly important role. So it's not just kind of the standard things that we look to our financial system to do, which is to allocate capital, but how it's allocated and on what basis and capturing risk and really ensuring that that allocation is done in a way that's going to be the most socially beneficial across the globe, so developing world, developed economies, across economies.

**Peter**: Thanks, Doug. We've talked a lot up until this point about the relationship between the financial services industry and the rest of the economy and the interlinkages there. I think it's very important to recognize that the U.S. financial services industry is itself a source of huge competitive advantage to the U.S. economy. That's reflected in a number of indicators. Those include the fact that New York is commonly regarded as the world's leader and financial center.

But other major cities in the U.S. are also regarded as key financial centers. And if you look at reports that measure countries' competitiveness the financial system is always identified as a key strength of the U.S. economy. My question here is does that competitive advantage in financial services translate into broader benefits for the rest of the U.S. economy. Let's start on this one with Kimberley.

**Kimberley**: Thanks, Peter. First, I think it's important to put the economic scale of the U.S. financial system in context. U.S. capital markets are the world's largest accounting for 41 percent of global equity and 40 percent of global fixed income markets. Domestically they fund 72 percent of U.S. economic activity. As a result of this competitive strength, the United States has consistently run a trade surplus in financial services. Exports have risen steadily through the 21st century, and the financial services surplus is worth $95 billion annually.

The U.S. has surpluses on financial services trade with every other G20 economy. I think that's a really important data point that crystallizes just how strong and competitive the U.S. financial services sector really is. As the SIFMA paper points out, more U.S. jobs are dependent on exports of financial services than are dependent on exports of motor vehicles or computers.

And because we are the most competitive country in the world in financial services over 670,000 U.S. jobs are dependent on exports of financial services. But that's only the direct employment, that is people employed by financial institutions. And beyond that, it is estimated that 3.6 jobs are created in the rest of the U.S. economy for every one job in financial services.

I should also note that the international nature of financial services also benefits the U.S. through the $760 billion invested in the United States by foreign banks, brokers, and other institutions which collectively employ almost 400,000 workers in the United States. The benefits of the U.S. financial sector's presence overseas are far broader than these direct impacts that I've just described, and I think they're worth noting as well.

U.S. financial institutions operating abroad introduce greater competition in those markets increasing their efficiency and improving the quality of global investment. U.S. firms operating overseas raise the standards of financial services contributing positively to financial stability and the local economy. U.S. financial services firms are crucial in conveying U.S. values and business practices across the globe.

Also, it's important to note that these overseas footprints contribute to global efforts against anti-money laundering and terrorist financing. And finally, importantly overseas investment strengthens activities and investment at home and benefits small and medium enterprises, the next generation of small business. And we can look positively to the future. All of this, all of this described, means that the strength of the U.S. financial services industry will continue to play a pivotal role in ensuring the future growth of our economy.

**Peter**: Thank you, Kimberley. Doug, what's your perspective?

**Kimberley**: Well, Kimberley gave a pretty good primer, so she didn't leave a lot on the table there, so. But I think it's worth, a couple of additional points worth with just quickly making. I think the first is, is that

the breadth, the scope of the U.S. financial system really makes credit available to a really wide swath of the U.S. economy, and it does it cheaply, competitively, and in a transparent manner for the most part. So that has just ripple effects across the economy.

And let me give a specific example because it's one that's studied and lots of other countries have tried to duplicate, and that's Silicon Valley. And if you look at the role that it has played in innovation in the U.S. economy, how it has been able to do that, and there's lots of things that go into it, of course, I mean, there's good universities and a culture of entrepreneurship, and all those things are important.

But inevitably when countries have tried to duplicate that environment one of the things that they have the hardest time sort of duplicating is in fact the U.S. financial services industry and its ability to fund that kind of innovation. And whether it's sort of bringing the capital to bear, whether it's the specific institutional structures that finance that innovation, it's really hard to duplicate that.

And so while I wouldn't call the financial system a sufficient condition for that kind of innovation, it's a necessary condition. And so I think it's just really worth noting that when other countries are trying to sort of step up their economic growth, you know if it's developing countries think of the emphasis that's put on microfinancing. Policymakers recognize the role that the financial system plays.

A well-functioning, well-regulated market really makes a huge difference in terms of economic growth, whether it's the allocation of capital, whether it's ensuring that contracts are held to, that people earn a fair return. All of these kinds of features that we sort of tend to take for granted in the United States, but really the financial system is a distinctive feature in our economy and really contributes to growth.

And as we've been discussing some of the big challenges that we face going forward, whether it's supply chain, resiliency, or dealing with climate change, again, the financial system will be a really important and critical part of the solution to those challenges.

**Peter**: Thank you, Doug. In concluding I think I'd just like to draw on a couple of observations that Kimberley and Doug made. Kimberley was talking there about the trade surplus that the U.S. has in financial services, and that's definitely one measure of the competitiveness of the U.S. financial services industry and how well it performs out there in the global economy.

She also talks about the dependence of future growth on the health of the financial services industry and the contribution that it makes there. And Doug earlier on used the word "solution" thinking about financial services and how it can solve the problems and challenges that we are confronting in our economy today. And I think those are all really important lessons and concepts.

# EXHIBIT 31A

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# SUPPLY CHAIN RESILIENCE ISSUE BRIEF

## REGULATORY COMPLIANCE & CROSS-BORDER ACCESS TO DATA

**Cross-border access to information and data transfers support supply chain resilience by promoting efforts to comply with various regulatory requirements relating to financial transparency, securities regulation, and prohibition on illicit finance (among other areas).**

- **Data Transfers & Preventing Illicit & Criminal Activity:** US supply chain resilience is directly threatened by a range of illegal activity – often associated with transnational criminal enterprises, private- or nation state-sponsored cyber-attackers, rogue states, and terrorist groups – that increase both economic and national security risks to the United States. This activity includes bribes, kickbacks, and various corrupt payments, which can lead to breaches of public integrity; overpayment for contracts; and the delivery of dangerous, adulterated, or counterfeit goods and services. This activity also includes criminal money laundering of the proceeds of illegally traded goods or human trafficking, and even terrorist financing activities.

- **Data Transfers & Financial Regulatory Compliance:** Data transfers and cross-border access to data for forensic or investigatory purposes are critical to combatting such criminal activity across the supply chain. Data transfers and information access support compliance with governmental rules designed to prevent consumer fraud, securities and financial crimes (e.g., insider trading), money laundering, and corrupt practices. For example, fraud detection models are typically built on global transaction data or transaction data collected from multiple countries because fraud patterns are not limited by national boundaries. Fraud trends that appear in one region or country may apply in others as cardholders travel to different countries, cardholders transact online with merchants in different countries, and the perpetrators of fraud do not respect any national boundary lines. Thus, to build effective fraud models and to gain the necessary insights into fraudulent activity in order to help prevent it, these models must be built off of global or multi-country data sets, based both on the location of the merchant and the location of the cardholder.

- **Data Transfers & Financial Transparency:** Data transfers and cross-border access to data are also essential to ensuring financial accountability, stability, and transparency that are critical to US supply chain and economic resilience. The ability to anticipate, manage, and respond to financial and economic shocks depends upon maintaining access to accurate and reliable sources of firm- and microeconomic-level data, as well as sources of sectoral-, market- and economy-wide data. In at least one jurisdiction, government officials have severely limited the research and outbound transfer of such data, even going so far as to criminalize such activity.[1] Being denied cross-border access to such economic data is highly destabilizing to supply chains, securities exchanges, and other financial markets. As the United States has the world's largest financial markets, it is particularly important to our own economic stability to maintain ready and immediate access to such market and financial data from around the world.

- **Data Transfers & Government Investigations.** Some claim that data localization and data transfer restrictions are necessary to ensure that authorities will have access to data relevant to conduct investigations. The location of the data, however, is not the determining factor. Indeed, financial service regulators and enforcement authorities from countries including Australia, Canada, Japan, Mexico, Singapore, the UK, and the US have agreed that financial services data should not be subject to localization requirements in one country, provided that financial regulatory authorities have ready access for regulatory and supervisory purposes to information stored in any other territory. This is in part due to the recognition, as explained by some of these authorities, that "data localization requirements can increase…operational risks, hinder risk management and compliance, and inhibit financial regulatory and supervisory access to information." [1]

- **Data Transfers & Multi-Jurisdictional Law Enforcement Access.** Responsible private sector service providers work to respond to lawful requests for data consistent with their obligations to their customers and to protect consumer privacy. As reflected in the Organisation for Economic Co-operation and Development's (OECD) Declaration on Government Access to Data Held by the Private Sector, like-minded governments are working to define their core principles and common values when accessing personal data for national security and law enforcement purposes. The principles help increase trust in cross-border data transfers. Generally speaking, if the service provider has a conflicting legal obligation not to disclose data, law enforcement has several options. International agreements—including Mutual Legal Assistance Treaties (MLATs) or Agreements (MLAAs), multilateral treaties, and other agreements, such as those authorized by the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act—can establish foundations for mutual legal assistance and reciprocal transfers of law enforcement data. Courts may also issue requests to authorities abroad for the transfer of data through letters rogatory.

[1] Starting in 2023, China intensified its scrutiny of foreign consulting and accounting firms via a range of cross-border data-related investigations of these enterprises. These investigations were sometimes premised upon purported theft of state secrets or purported espionage. China also made increasing use of travel exit bans in conjunction with these efforts. Please see here for media coverage: Asahi, Bloomberg, WSJ (Data access restrictions), WSJ (anti-espionage act), WSJ (Micron, Astellas, Bain, Mintz, investigations), NYTimes.

# EXHIBIT 31B

ANTI-CORRUPTION HELPDESK

PROVIDING ON-DEMAND RESEARCH TO HELP FIGHT CORRUPTION

# SUPPLY-CHAIN CORRUPTION, CUSTOMS TRANSPARENCY AND CONSUMER PROTECTION

## QUERY

What are the links between corruption, lack of transparency and customs? What are the best practices for customs transparency and consumer information? What steps can be taken to improve access to the information in question?

## PURPOSE

We are working with other NGOs to prevent corruption-tainted products from passing through customs in order to protect consumers.

## CONTENT


1. Connections between corruption risks and customs transparency
2. Best practices in customs transparency
3. Steps to improve consumer information
4. References



Author(s)
David Jackson

Reviewer(s)
Marie Chêne, Transparency International,
tihelpdesk@transparency.org



Date: 3 June 2016


## SUMMARY


Supply chains are susceptible to many different forms of corrupt practices and illicit behaviour, all of which inflict costs and harm to the wider society. Different strategies exist to address these risks, such as legislation, enhancing management procedures and pursuing due diligence. Yet all of these rely on transparency.

Customs is a possible link in the supply chains where transparency can be increased. This brief discusses the connections between customs transparency, corruption in supply chains and consumer protection before identifying best practices to increase the transparency of products passing through customs and best practices for how consumers can access more information. The final section focuses on next steps that the governments, businesses and civil society can make to increase the transparency of products passing through customs.



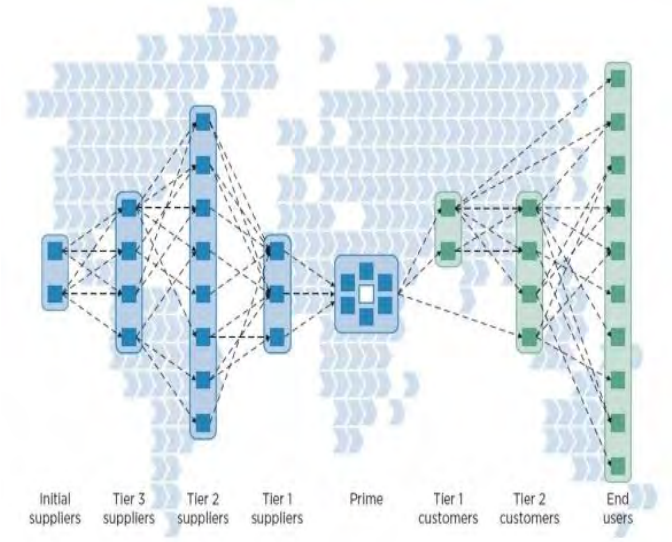


*This Anti-Corruption Helpdesk is operated by Transparency International and funded by the European Union.*

# 1 THE CONNECTIONS BETWEEN CORRUPTION, LACK OF TRANSPARENCY AND CUSTOMS

## Corruption challenges in supply chains

Global business transactions work through intricate supply chains: "the persons, entities and infrastructure that transform materials and human capital into intermediate and finished products and services for customers and consumers" (Global Compact 2010, p. 7). Supply chains can often be vast networks, involving a multitude of actors –suppliers, assemblers, producers, distributors, retailers and, finally, consumers – operating across different jurisdictions (see diagram below).




Source: (IfM 2014)

Supply chains are susceptible to many different forms of corrupt practices and illicit behaviour, all of which inflict costs and harm to the wider society. These corruption risks include:

### *Human rights abuses and environmental damage*

- Modern slavery can persist when businesses are not aware of certain practices within their supply chain (UK Government 2015). Estimates made by the Walk Free Foundation (2014) suggest that there are 35.8 million men, women and children trapped in modern slavery.
- The OECD also reports that corruption in supply chain facilitates human trafficking (OECD 2015).
- More general labour exploitation and mistreatment occurs in global supply chains, where workers have few rights and dire working conditions. Misconduct in the supply chains of some of the world's major brands, such as the Rana Plaza factory collapse, has been well documented (CCC 2016).
- Opaque supply chains make it difficult to deal with the environmental risks of illicit activities. The United Nations Office on Drugs and Crime (UNODC), for example, suggests that the environmental costs from the production of counterfeit goods are understated (UNODC).

### *Organised crime and illicit trade*

- Organised crime and illicit trade benefit from the vulnerabilities of global supply chains (OECD 2016). For example, the US government report that trade-based money laundering – the process of disguising criminal proceeds through trade to legitimise their illicit origins – is a particular vulnerability for global supply chains (ICE).
- It is estimated that annual trade-based money laundering exceeds billions of dollars and is growing each year (ICE).

### *Corruption*

- Generally, billions of dollars are lost in supply chains due to different kinds of fraud, including physical and information theft, bribery, money laundering, kickbacks, fraudulent billing and various purchasing schemes (Global Compact 2010).
- Most companies suffer from corruption in supply chains. The Kroll Global Fraud report, based on a survey of 768 executives, found that 75 per cent of companies had fallen victim to an incident of fraud in the past year, a rise of 14 per cent in just three years, and that 69 per cent of companies had suffered a financial loss as a result of fraud during 2015 (Kroll 2015).
- PricewaterhouseCoopers' analysis of 600 companies that had experienced supply chain disruptions shows that the companies' average shareholder value plummeted when compared to

their peers, their stock prices experienced greater volatility, and they suffered sharp declines in return on sales and return on assets (PwC 2008, p. 5).

## What is the potential impact on consumers of these risks?

### *Health risks*

In 2007, for example, the government of Panama unknowingly used diethylene glycol falsely labelled as glycerine to make 260,000 bottle of cough syrup. The origin of the counterfeit chemicals was traced from Panama through trading companies in Spain to a source near the Yangtze Delta in China. As the poisonous substance travelled from China, a certificate attesting to the purity of the shipment was repeatedly altered. One hundred people died in Panama from ingesting the tampered cough syrup (Picard & Alvarenga 2012, p. 58).

### *Misleading product information*

In 2013, DNA tests revealed that some meat products labelled as beef from a well-known supplier contained a considerable proportion of undeclared horsemeat or pork. Blind spots in the supply chain were at fault as, unknown to the end-producers, the meat was suddenly being supplied by different providers than previously. Investigations revealed that the horsemeat sometimes took a complicated route through sub-suppliers across several countries (Zurich Risk Nexus 2015, p. 5).

### *Lack of information to make choices*

Risks to consumers are posed because the level of information that businesses have about their supply chain is not sufficient; often businesses are unable to work out what is going on beyond first-tier suppliers (Picard & Alvarenga 2012, p. 57). Indeed, the majority of companies that do business globally suffer from a lack of supply chain visibility:

- The 2014 edition of the Business Continuity Institute's annual survey of 525 companies based in 71 countries found that roughly 75 per cent of companies lacked full supply chain transparency and only about a quarter coordinated and reported supply chain disruptions across the enterprise (Zurich Risk Nexus 2015).
- A study conduct by Stanford's Graduate School of Business revealed that while most respondent companies have social and environmental systems in place for internal operations, less than a third have similar structures to monitor the practices of their immediate and extended supplier network (Linich 2014).

## How does a lack of transparency in customs contribute to these risks?

Different strategies exist to address these risks, such as new legislation, enhancing management procedures, and pursuing due diligence. Yet *all of these rely on transparency*. Increasing transparency is about bringing to light information that can document the behaviour of different actors within each tier of a supply chain in order to allocate responsibility and agency at all levels (CCC 2016, p. 2). Transparency, therefore, provides the foundation for strategic action against corruption and human rights violations

Customs is a possible link in the supply chains where transparency can be increased. In particular, customs can be an important location where critical information can come to light to enable:

- public authorities to protect against misconduct and illicit behaviour
- consumers to know where, who and under what conditions the product was made that they want to buy
- consumer and human rights organisations to verify due diligence of companies and identify malpractice

Transparency in the customs sector can refer to two aspects of a customs regime. Generally, transparency relates to the extent to which information about customs' operations and procedures is available. The WTO Glossary defines transparency in customs as "the degree to which trade policies and practices, and the process by which they are established, are open

and predictable" (WCO 2016). It includes a number of interrelated actions, such as[1]:

- Customs laws, regulations, procedures and administrative guidelines should be made public, be easily accessible and applied in a uniform and consistent manner.
- The basis upon which discretionary powers can be exercised should be clearly defined.
- Appeal and administrative review mechanisms should be established to provide a mechanism for clients to challenge or seek review of customs decisions.

Using a similar definition, the World Economic Forum has developed a Customs Transparency Index for which transparency encapsulates the overall transparency of the procedures and regulations related to customs clearance.[2] Transparency refers, therefore, among other things, to: the extent to which the laws and regulations are published in an official journal; changes to regulations can be commented on prior to implementation; and that there is a public and regularly updated website available with a full description of all customs procedures (WEF 2014).

Corrupt actors benefit from a lack of this kind of transparency. Hence, the link between this kind of transparency and corruption is quite clear: the less transparent that customs are, the higher the corruption risks. Accordingly, the World Customs Organization's (WCO) Arusha Declaration on Integrity in Customs (revised 2003) aims at enhancing the efficiency of its member states' administrations to help eliminate the risks and opportunities for corruption.

Less commonly, transparency in customs can also refer to the availability of information about products passing through customs; in other words, the extent of information about products (for example, identity and origin of product) is available via a publicly accessible database. A review of the literature suggests that this kind of transparency is less commonly discussed as a source of corruption. In fact, it is difficult to find an evidenced-based link between this kind of transparency and the risk of corruption. There seems to be little research on the effects of databases and customs and its possible consequence for addressing corruption. There are no legal standards about this kind of transparency and it is not an integrated element of trade agreements or international conventions.

## 2 BEST PRACTICES IN CUSTOMS TRANSPARENCY

Even though few policy documents discuss transparent databases at customs as a mechanism to reduce corruption in supply chains, some civil society groups advocate for customs databases as part of a general model of transparency for supply chains (see CCC 2016). There are also best practices which do try to increase the transparency of products passing through customs and best practices for how consumers can access more information. This section identifies some of these best practices.

### Best customs practices to generate transparency of product information

#### *United States*

The US government can be said to lead the way in providing some kind of transparency of products passing customs through setting up the Interactive Tariff and Trade DataWeb, which provides US international trade statistics and US tariff data to the public full-time and free of charge. The available data relates to the customs value, first unit of quantity, second unit of quantity, landed duty-paid value, dutiable value, calculated duties and import charges for all kinds of commodity imports.[3] This data has been made available as part of a broader initiative of transparent government instigated by the president. The information available is limited, however. It is unlikely the data allows for the identification of the

[1] Best practices in terms of the integrity of procedures and operations can be found in the World Custom Organization's Compendium of Best Practices (WCO 2007).

[2] This indicator is based on seven survey questions taken from the GEA Customs Capabilities Reports, evaluating World Economic Forum's calculations based on data from the Global Express Association. http://www3.weforum.org/docs/WEF_GlobalEnablingTrade_Report_2014.pdf

[3] https://dataweb.usitc.gov/scripts/user_set.asp

manufacturer of certain products; rather it is mostly designed to assess trade patterns.

The US government has also developed a specialized computer system called the Data Analysis & Research for Trade Transparency System (DARTTS) that is managed by the Trade Transparency Unit (TTU) within the US Immigration and Customs Enforcement (ICE).[4] Established in 2004, this initiative is "designed to protect the integrity and security of the US economy by targeting and eliminating systemic vulnerabilities in commercial trade and the financial and transportation sectors susceptible to exploitation by criminal and terrorist organizations" (ICE).

The database is based on the idea that the best way to analyse and investigate suspect trade-based activity is to have systems in place that can monitor specific imports and exports to and from given countries. Using automated analysis tools, the TTU examines the voluminous data to seek out anomalous patterns in international trade that could reveal financial irregularities indicative of trade-based money laundering, customs fraud, contraband smuggling and even tax evasion. The raw data, sourced from both US and foreign sources, contain information on the product ID, the vendor and receiver. However, data from the DARTTS is not publicly available (ICE).

### *European Union*

There is a trend to make customs information electronic across the EU, but this is more about customs harmonisation and facilitation rather than transparency and anti-corruption. The Union Customs Code (UCC) is a 2016 update to customs legislation across the EU, and will introduce a number of revisions to existing requirements.

The UCC was enacted to modernise and simplify trade into and within the EU. It also aims for a harmonisation of customs procedures across the member states. In particular, the UCC will make changes to customs procedures and authorisations, modifications to existing electronic procedures and introduce a new digital processes, including the Proof of Union Status.

The key principle of the UCC is that all customs declarations should be electronic. However, there is no mention of public databases within the new code.

## Examples of how technology could be used to generate more information for consumers

Technological innovation is providing unprecedented visibility into supply chains. Companies and civil society groups must harness this technology, and fortunately there are some examples of best practice which lead the way.

These practices could be adapted to help customs authorities generate data to increase transparency. For example, on a general level, product-tracking technology means that processes in a supply chain are digitally recorded so that any licit or illicit activity will leave digital footprints that can be made nearly impossible to tamper with or erase (Picard & Alvarenga 2012, p. 60).

Examples include:

- Product labelling has been transformed by microscopic electronic devices, genetic markers for agricultural products and a new generation of bar codes that can be read with standard mobile phones. Radio-frequency identification tags, well established for inventory management and other purposes, are becoming smaller, cheaper and more flexible. A new generation of tags – such as Hitachi's sand-grain-size mu-chip – can be used, for instance, to label jewellery inconspicuously (New 2010).
- Retail giants, such as Tesco and Walmart have used an innovative service from UK supply chain services firm Historic Futures. The system enables textile suppliers to collect and submit information about cotton products, with a focus on ensuring that products are not manufactured from Uzbek cotton that was harvested with child labour. These data are used internally, allowing the retailers to be more confident in making ethical claims about their products (New 2010).

[4] https://www.ice.gov/trade-transparency

- Swiss textile company, Switcher, labels each of its products with a code that consumers can enter at the website Respect-code.org to retrieve information about the firms and factories along the supply chain, as well as from ISO 14000 environmental-performance certificates (New 2010).
- The integrity of the product could be provided not by the supply chain but by the product itself. For example, Coats Textiles in the United Kingdom has developed a "digital thread" with a security code embedded in the thread (Picard & Alvarenga 2012, p. 60).
- New technology means that if a company does not make transparent information available to their customers, others will provide it. GoodGuide provides a mobile phone application to get information on a product's health, environmental and social impacts. If it transpires, for example, a washing powder has a low environmental score, GoodGuide will propose an environmentally friendly alternative (Picard & Alvarenga 2012, p. 60).

## 3 STEPS TO IMPROVE CONSUMER INFORMATION

This section focuses on the broader public policy angle of the issue and on the best practices of governments, businesses and civil society in generating more information that can be used in the public domain about products passing through customs. To this end it provides best practices in three areas: regulation, civil society advocacy and technology.

### Regulation

Regulations on supply chains differ across jurisdictions and vary in the kind of due diligence and reporting obligations they demand from companies. Two acts lead the way in explicitly demanding action against human rights violations:

- The California Transparency in Supply Chains Act means that since 2012 companies in California with business operations worth more than US$100 million annually disclose their efforts, if any, to ensure that their supply chains are free from slavery and human trafficking (CorA 2015).
- In the UK, the government has introduced a provision in the Modern Slavery Act 2015 which requires certain businesses to produce a statement setting out the steps they have taken to ensure there is no modern slavery in their own business and their supply chains. If an organisation has taken no steps to do this, their statement should say so. One key purpose of this measure is to prevent modern slavery in organisations and their supply chains. A means to achieve this is to increase transparency by ensuring the public, consumers, employees and investors know what steps an organisation is taking to tackle modern slavery (UK Government 2015).

Other regulation can be sector-based:

- The Dodd Frank Act (paragraph 1502) in the USA means that since January 2013 all companies listed on a US stock exchange must prove and make publicly accessible the origin of certain conflict minerals, such as tin, tantalum (from coltan ore), tungsten and gold. The corresponding draft of an EU Regulation does not, however, contain any binding regulations concerning due diligence. Furthermore, the proposed regulation is intended to be limited to those companies which market conflict minerals directly (CorA 2015).
- The EU Timber Regulation, which came into force on 3 March 2013, requires all companies importing timber or wood products to the EU for the first time to adhere to particular due diligence obligations and to document that the wood and the traded products originate from legal logging sources. Timber merchants from within the EU must also be able to verify the merchant from whom they bought the timber or wood products, and to whom they have sold these on to, along the entire supply chain. This information must be conserved for five years (CorA 2015).
- In September 2014, the Council of the European Union adopted the directive on disclosure of non-financial and diversity information by certain large companies. This means by 2017, environmental, social and employee-related reporting will be mandatory for all companies based in the EU with more than 500 employees. While detailed regulations will be the responsibility of member states it is clear it will be the organisations'

responsibility to identify risks and deficiencies in their supply chain and to prevent potential violations against the companies own sustainability goals. The EU directive encourages organisations to report against well-established and recognised frameworks such as the Global Reporting Initiative, the UN Global Compact, or ILO Tripartite Declaration.

Increasing transparency in global supply chains is in line with international principles for fair and ethical business practices.

- The UN Global Compact, the UN's corporate sustainability initiative, has enshrined the principles of the UN Convention against Corruption (2005) into an anti-corruption instrument for corporations: the 10th Principle. This principle serves as an inspiration for companies adopting or reviewing internal anti-corruption policies, strategies and measures. The 10th Principle commits UN Global Compact Participants in particular not only to avoid corruption but to develop policies against it and to join government bodies, UN agencies and civil society to realise a more transparent global economy (Global Compact 2010).
- UN Guiding Principles on Business and Human Rights (2011) are a set of guidelines for states and companies to prevent, address and remedy human rights abuses committed in business operations. According to UN Guiding Principles, governments where brands and retailers are registered should encourage and, where appropriate, require business enterprises to communicate how they are addressing their effects on human rights. Governments where clothing is produced have a duty to make sure systems are in place to protect human rights.

## Civil society advocacy

Many civil society organisations (CSOs) advocate for greater supply-chain transparency. One of the leading organisations is the Clean Clothes Campaign (CCC), which is dedicated to improving working conditions and supporting the empowerment of workers in the global garment and sportswear industries. CCC's position paper on transparency provides a transparency model for the production of clothes and garments and could be used by other CSOs in their pursuit of transparency in other sectors and industries. To generate greater transparency in supply chains, the CCC calls for (CCC 2016):

governments in consumer countries to:

- require companies to report, on an annual basis, on the effectiveness of their responses to address the adverse effects of their activities on human rights, including in their supply chain
- require companies disclose the names, addresses and contact details of their supplier facilities, subcontracted suppliers (tiers 2 and 3) and labour agents managing home-working facilities, at least on an annual basis
- require products sold within the jurisdiction to be labelled to include a product code linked to a website that will provide information including supply chain traceability, employment statistics at the facility, economic information of the facility, pricing information and product information
- operate a standardised shipping database at an EU level which stores records for all exports and imports of cargo entering European ports, noting the class of cargo, the trading names of the companies involved, the point of origin, the value as an FOB price and quantity, and the ultimate destination and recipient, and make this available by access request

garment brands and retailers to:

- report annually on the effects of their activities throughout the supply chain on human rights, including explicit reporting on due diligence processes, policies, and on the effectiveness of their responses to address the adverse effects of their activities, using measurable indicators
- disclose the names, addresses and contact details of supplier facilities, subcontracted suppliers and labour agents managing home-working facilities, on an annual basis or more frequently
- publish social audit reports
- work alongside key stakeholders to report regularly on the effects to human rights and work towards protection and remedy where appropriate

suppliers and manufacturers to:

- disclose a buyer list, on an annual basis or more frequently
- disclose the names, addresses and contact details of subcontractor facilities and labour agents managing home-working contracts, on an annual basis or more frequently
- publish social audit reports in the public domain, including information on: number of workers in each department and grade, number of migrant and juvenile workers, percentage turnover of workers, number of grievances filed by workers, number of accidents causing injuries in the recent period
- appoint an individual at top level management responsible for social performance and publish the contact information for this individual

governments in producing countries to:

- require suppliers report on an annual basis on effectiveness of their responses to address the adverse effects of their activities on human rights, supply chain traceability, employment statistics, economic information and social audit reports
- publish a database of findings of labour inspectorates showing compliance with labour rights as per local law, naming suppliers that have repeatedly failed to meet standards over periods of six months or more

### Businesses

The damage to a company's reputation in particular can dramatically affect the value of the brand, relationships with business partners and share prices (Global Compact 2010). Shareholders, consumers, civil society and government have growing expectations that company executives be knowledgeable and accountable for what is happening in their extended supply chains (Picard & Alvarenga 2012, p. 57).

Evidence suggests supply chain integrity is increasingly at the forefront of supply chain managers' priorities. A 2008 PwC study surveyed 59 global consumer and retail companies and found that large brand-owners were particularly sensitive to both the reputational and operational risk of supply chains (Picard & Alvarenga 2012, p. 58).

Part of the burden for greater transparency in supply chains is carried by companies. There are many practical guides available to help businesses generate more information on their supply chains through implementing certain internal management procedures, such as inventory management, procurement procedures, recordkeeping, reporting practices, inspection and testing protocols. These guides include:

- UN Global Compact's Fighting Corruption in the Supply Chain: A Guide for Customers and Suppliers (2010)
- OECD Guidelines for Multinational Enterprises (2011)
- Deloitte University's The Path to Supply Chain Transparency (Linich 2014)
- Zurich Risk Nexus's Supply Chain Integrity (Zurich Risk Nexus 2015)

## 4 REFERENCES

CCC. 2016. Position Paper on Transparency. Clean Clothes Campaign. Amsterdam. http://www.cleanclothes.org/resources/publications/2016-04-ccc-position-paper-with-demands-on.pdf/view

CorA. 2015. Statement on Supply Chains. http://www.cora-netz.de/cora/wp-content/uploads/2015/05/G7-Statement-Supply-Chains-CorA-ForumHR_2014-05.pdf.

Global Compact. 2010. Fighting Corruption in the Supply Chain. A Guide for Customers and Suppliers. United Nations. New York. https://www.globalcompact.de/wAssets/docs/Korruptionspraevention/Publikationen/stand_together_against_corruption.pdf

ICE: Website. 2014. Trade Transparency Unit. https://www.ice.gov/trade-transparency

Capturing Value from Global Networks: Strategic Approaches to Configuring International Productions, Supply and Service Operations. University of Cambridge. http://www.ifm.eng.cam.ac.uk/uploads/Events/Briefing_Day_2014/Capturing_Value_from_Global_Networks.pdf

Kroll. 2015. Global Fraud Report. Vulnerabilities on the Rise. http://www.kroll.com/global-fraud-report

Linich, D. 2014. The Path to Supply Chain Transparency: A Practical Guide. DUPress. http://dupress.com/articles/supply-chain-transparency/

New, Steve. 2010. The Transparent Supply Chain. In *Harvard Business Review* (October). https://hbr.org/2010/10/the-transparent-supply-chain

OECD. 2015. Developing a Framework for Combatting Corruption Related to Trafficking in Persons. Paris (Background papers).
http://www.oecd.org/gov/Background-Paper-Developing-a-framework-for-combatting-corruption-related-to-trafficking-in-persons.pdf

OECD. 2016. Fighting the Hidden Tariff. Global Trade Without Corruption.
Contribution to OECD Integrity Forum. OECD. Paris.
http://www.oecd.org/cleangovbiz/2016-Integrity-Forum-Background-Report.pdf

Picard, J. and Alvarenga, C. 2012. Illicit Trade, Supply Chain Integrity and Technology. In Global Enabling Trade Report. WEForum.
http://www3.weforum.org/docs/GETR/2012/GlobalEnablingTrade_Report.pdf

PwC. 2008. From Vulnerable to Valuable. How Integrity Can Transform a Supply Chain (Achieving operational excellence series).
http://www.pwc.com/us/en/supply-chain-management/publications/supply-chain-report-download.html

UK Government. 2015. Transparency in Supply Chains. A practical guide.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/471996/Transparency_in_Supply_Chains_etc__A_practical_guide__final_.pdf

UNODC: The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime. Focus on Series.
https://www.unodc.org/documents/counterfeit/FocusSheet/Counterfeit_focussheet_EN_HIRES.pdf

Walk Free Foundation. 2014. The Global Slavery Index.
http://www.globalslaveryindex.org/findings/

WCO. 2007. Compendium of Integrity Best Practices. World Customs Organisation.
http://www.wcoomd.org/en/topics/integrity/~/media/F8980A7CB73A4F2E80A137967AF75CA8.ashx

WCO. 2016. Integrity Development Guide. World Customs Organisation.
http://www.wcoomd.org/en/topics/integrity/~/media/B89997B68D6A4E34AE9571979EADA39F.ashx

WEF. 2014. Global Enabling Report. WEForum.
http://www3.weforum.org/docs/GETR/2012/GlobalEnablingTrade_Report.pdf

Zurich Risk Nexus. 2015. Supply Chain Integrity. Protecting Companies' Blind Spots. With assistance of SICPA.
https://www.sicpa.com/sites/default/files/news/files/risk-nexus-supply-chain-integrity-november-2015.pdf

*"Anti-Corruption Helpdesk Answers provide practitioners around the world with rapid on-demand briefings on corruption. Drawing on publicly available information, the briefings present an overview of a particular issue and do not necessarily reflect Transparency International's official position."*

# EXHIBIT 32

February 26, 2024

The Honorable Antony J. Blinken
U.S. Department of State
2201 C Street N.W.
Washington, D.C. 20520

The Honorable Gina M. Raimondo
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

The Honorable Katherine Tai
Office of the United States Trade Representative
600 17th Street NW
Washington, DC 20508

Dear Secretaries Blinken and Raimondo and Ambassador Tai:

The below-signed civil rights, civil liberties, and open Internet advocates have championed a free and open internet while fighting against the harms that emerging technologies may pose for liberty, privacy, and equity. These goals can – and must – be achieved together. While we appreciate President Biden's steps to address the actual and emerging harms of artificial intelligence,[1] we are concerned that the withdrawal of key commitments at the World Trade Organization and in international trade negotiations will signal that the United States no longer stands by a free and open internet. We ask that you reiterate the United States' twin commitments to preserving the internet as a truly global medium and to retaining its ability to make specific adjustments to allow for critical public policy objectives such as the regulation of algorithmic systems to support privacy and equity.

Late last year, the U.S. Trade Representative withdrew support for a number of commitments at the World Trade Organization that underpin a global, open internet,[2] including opposing forced data localization, supporting the free flow of information, combatting mandatory transfers of intellectual property, and championing non-discrimination for information products.[3] Advocates and governmental bodies have long championed these commitments as key for fostering human rights and ensuring access to information globally.[4] As former Federal Communications

---

[1] *E.g.*, Comments of the American Civil Liberties Union, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, Docket No. OMB-2023-0020 (Dec. 5, 2023), here; Comments of the Center for Democracy & Technology (Dec. 5, 2023), here; ReNika Moore & Cody Venzke, *ACLU Statement on President Biden's Executive Order on Artificial Intelligence*, ACLU (Oct. 30, 2023), here.

[2] Gavin Bade, *NSC, USTR at Odds Over Digital Trade Decision at WTO*, Politico Pro (Nov. 9, 2023), here.

[3] Letter from Sens. Ron Wyden, Mike Crapo et al. to President Joseph R. Biden (Nov. 30, 2023), here (hereinafter Congressional Letter).

[4] Adrian Shahbaz, Allie Funk & Andrea Hackl, *User Privacy or Cyber Sovereignty? The Human Rights Implications of Data Localization,* Freedom House (July 2020); *Policy Brief: Human Rights*, Internet Society (Oct. 30, 2015),

Commissioner Michael Copps observed in early net neutrality debates over two decades ago, these commitments reflect the recognition that "Internet openness and freedom are threatened whenever someone holds a choke-point that they have a legal right to squeeze. That choke-point can be too much power over the infrastructure needed to access the Internet. And it can also be the power to discriminate over what web sites people visit or what technologies they use."[5] Those concerns apply whether the discriminatory power is exercised by private power or public authorities.

The United States' withdrawal of its commitments may be read to signal an abandonment of those principles of openness, freedom, and non-discrimination:

- **Data localization.** Data localization requirements may be abused to disfavor foreign companies and speakers and undermine the functioning of a global, interoperable internet by upending the ways in which data can flow across borders.[6] Data localization places personal data "firmly within reach of governments,"[7] creating unique risks for people's privacy, free expression, access to information, and other fundamental freedoms.[8] Data localization efforts can also exacerbate cybersecurity concerns by requiring duplication of the servers and data localized in each jurisdiction.[9] Those cybersecurity vulnerabilities may make data *more* vulnerable to foreign surveillance and privacy breaches, while failing to address sophisticated attacks that do not rely on the foreign transfer of data.[10]
- **Restrictions on cross-border flows of information.** International flows of information are essential for people in the United States and around the world to participate in global discourse and commerce, and broad limitations on those data flows would restrict their ability to access content from across the globe.
- **Forced disclosure of source code.** The forced disclosure of products' source code may undermine intellectual property rights, privacy, and security. An entity that is required to disclose source code "may fear theft of its IP" and its transfer to a competing entity.[11] Mandated disclosure of source code may likewise allow adversaries to identify and exploit security and privacy vulnerabilities. Although the United States should commit to protecting against forced transfers and exploitation of source code, those commitments

---

here; Sen. Ron Wyden, *The Free Internet Is a Global Priority*, Wired (Apr. 22, 2015), here; *The Impact of Forced Data Localization on Fundamental Human Rights*, Access Now (June 4, 2014), here.

[5] Michael J. Copps, Commissioner, Federal Communications Commission, Remarks at New America Foundation at 9 (Oct. 9, 2003), here.

[6] Shayerah I. Akhtar & Michael D. Sutherland, Congressional Research Service, Digital Trade and U.S. Trade Policy 15-16 (2021), here (hereinafter CRS Report).

[7] Erol Yayboke et al., *The Real National Security Concerns over Data Localization*, CSIS (July 23, 2021), here.

[8] Allie Funk & Jennifer Brody, *Reversal of US Trade Policy Threatens the Free and Open Internet*¸ Tech Policy Press (Nov. 14, 2023), here.

[9] H Jacqueline Brehmer, Data Localization: The Unintended Consequences of Privacy Litigation, 67 Am. U. L. Rev. 927, 962-63 (2018), here.

[10] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 714-21 (2015), here.

[11] CRS Report at 17-19.

should still permit sufficient transparency around algorithmic systems to guard against discrimination and other harms, as discussed below.

- **Discrimination against foreign digital products.** Nondiscrimination has long been a keystone in U.S. digital policy, ensuring that individuals, not governments or infrastructure providers, ultimately choose what information is created and accessed.[12] This principle enables individuals to choose the best products and platforms for their needs – including those that have better content moderation or privacy policies.

Abandoning those commitments can result in concrete harms. For example, data localization mandates might impact a global service like Wikipedia (the free online encyclopedia created and maintained by volunteers around the world) and its users worldwide. Over the past decade, the Wikimedia Foundation (the nonprofit that hosts Wikipedia) has received an increasing number of requests to provide user data to governments and wealthy individuals, who wish to censor accurate public information or to identify and take retaliatory action against the volunteers editing Wikipedia.[13] These mandates would worsen this trend by subjecting the data of vulnerable individuals to direct seizure by authorities that do not respect human rights.

Besides threats to privacy, free expression, and even the safety of Wikipedia volunteer editors, the financial costs of establishing data collection and storage facilities in countries around the world would threaten the economic viability of nonprofit, small businesses, and larger commercial entities alike.

Growing requirements for data localization are happening alongside a global crackdown on free expression. And people's personal data – which can reveal who they voted for, who they worship, and who they love – can help facilitate this. Rwanda's data protection law, for instance, mandates that companies store data locally unless the country's non-independent cybersecurity regulator approves otherwise. This requirement leaves personal data easily accessible in an environment in which authorities have embedded agents in telecommunications companies and used data from private messages to prosecute dissidents.[14] Similarly, in Uzbekistan, authorities temporarily blocked Skype, TikTok, Twitter, VKontakte, WeChat, and other popular platforms due to their noncompliance with a data localization law, severely limiting people's ability to communicate and access information.[15] Rwanda and Uzbekistan are not outliers. 78 percent of the world's internet users live in countries where simply expressing political, social, and

---

[12] *E.g.*, 50 U.S.C. § 1702(b)(3) (restricting Presidential authority to regulate importation of "any information or informational materials"); *In re Amendment of Section 64.702 of the Commission's Rules and Regulations*, 77 F.C.C.2d 384, 429, para. 116 (1980) (Second Computer Inquiry) (ensuring "nondiscriminatory access to common carrier telecommunications facilities" by providers of information services).
[13] *Transparency Reports*, Wikimedia Foundation, here (last visited Feb. 13, 2024).
[14] *Rwanda*, Freedom House (2023), here.
[15] Catherine Putz, *Uzbekistan Unblocks Twitter, TikTok Still Restricted*, The Diplomat (Aug. 4, 2022), here.

religious viewpoints leads to legal repercussions.[16] The United States should maintain its longstanding opposition to these requirements.

While there are a range of reasons companies have resisted data localization requirements, some are at least in part doing so over concerns they will be complicit in government repression. When data is not stored locally, the respective government often must go through a legitimate – albeit far from perfect[17] – legal process for accessing the information from U.S. companies. But when data is stored on local servers, the ability for companies to resist problematic state demands is hampered. This challenge is further compounded by the emergence of so-called hostage-taking laws, in which international companies are required to have a local presence in a particular country, curbing their willingness to push back against user data requests over concerns for employee safety.

Nonetheless, firm commitment to a free and open internet does not mean surrender to an *unregulated* internet. For example, U.S. civil rights statutes apply to foreign entities that discriminate against individuals in the United States,[18] and neither housing data abroad nor engaging in international data flows will undermine domestic regulation of discriminatory algorithmic decision-making. Regulations of data and AI such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act became law years ago, and there has been no credible challenge under international trade law to either, despite pro-business commentary insisting as much.

Moreover, well-scoped exceptions in treaty language can help protect regulatory goals in regulation of data and AI. International digital trade agreements have long sought to accommodate legitimate public policy objectives. For example, the USMCA recognized an exception to its prohibition on restricting cross-border data flows to "achieve a legitimate public policy objective."[19] Well-scoped exceptions in negotiations at the WTO and elsewhere may similarly allow for flexibility for domestic regulation to address emerging harms; indeed, some of the signatories of this letter have recognized the need to ensure that international agreements do not "thwart" algorithmic impact assessments and audits.[20]

---

[16] Allie Funk et al., Freedom on the Net 2023 (2023), here.
[17] Access Now, ACLU, CDT, et al., Coalition letter on CLOUD Act (Mar. 12, 2018), here.
[18] Equal Employment Opportunity Commission, Enforcement Guidance on Application of Title VII and the Americans with Disabilities Act to Conduct Overseas and to Foreign Employers Discriminating in the United States (1993), here ("By employing individuals within the United States, a foreign employer invokes the benefits and protections of U.S. law. As a result, the employer should reasonably anticipate being subjected to the Title VII enforcement . . . . ").
[19] Agreement Between the United States of America, the United Mexican States, and Canada, July 1, 2020, art. 19.11, here.
[20] Letter form Lawyers' Committee for Civil Rights, ACLU, CDT et al. to President Joseph R. Biden at 2 (May 23, 2023), here.

Similarly, Congressional leaders have recognized that source code protections should "ensure that countries [cannot] force businesses to surrender their source code or share it with domestic competitors as a condition of doing business, while preserving the ability of governments to access source code to achieve legitimate public policy objectives, such as conducting investigations and examinations and promoting consumer health and safety."[21] Long-standing U.S. policy supporting an open internet is fully consistent with exceptions to achieve these legitimate public policy objectives.

But these exceptions should be concrete and appropriately scoped. The United States should lead *both* in establishing thoughtful regulations to support equity and privacy *and* in protecting an open and free internet. The United States should clarify immediately that both sets of goals remain at the heart of U.S. policy.

We thank you for your consideration. Please do not hesitate to contact us at cvenzke@aclu.org.

Sincerely,

American Civil Liberties Union
Center for Democracy & Technology
Freedom House
Information Technology and Innovation Foundation
Internet Society
PEN America
Wikimedia Foundation

Signatories in their individual capacities:
Susan Aaronson, Ph.D., Director, Digital Trade and Data Governance Hub, George Washington University and co-PI NIST-NSF Trustworthy AI Institute at George Washington University
Fiona Alexander, Senior Fellow, Digital Innovation Initiative, Center for European Policy Analysis (CEPA)
Dr. Konstantinos Komaitis, Internet Governance expert
Professor Peter Swire, J.Z. Liang Chair, School of Cybersecurity & Privacy, Professor of Law and Ethics, Scheller College of Business at Georgia Institute of Technology
Gary Winslett, Ph.D. Professor of Political Science and International Politics and Economics, Middlebury College

cc: Neema Singh Guliani

[21] Congressional Letter at 2-3.

Shannon Coe
Brian Daigle
Valerie Santos
Robert Tanner
Jillian DeLuna
Tarun Chhabra
Christina Segal-Knowles

# EXHIBIT 33

**Strengthening the Internet** 17 November 2023

# The United States Takes a Dangerous Step Back from Core Internet Principles

The United States Trade Representative has taken a dangerous step back from fundamental principles that ensure the growth of an open, secure, trustworthy, and globally connected Internet. By abandoning these principles that protect the free flow of information online, the United States is contributing to the global erosion of the Internet.

The United States has a long history of leading global initiatives to ensure the Internet remains an open platform for all. In a recent World Trade Organization meeting, however, the United States dropped several principles critical to the development, growth, and success of the Internet, including:

- **Support for cross-border data flows:** At the Internet Society, we know the Internet relies on data flows to connect people, schools, hospitals, governments, and critical infrastructure across the world. The flow of the data is determined by the networks involved, and not any authority. It is a core part of what makes the Internet so valuable to people worldwide.

- **Opposition of mandated data localization rules:** Modern data and networking systems that we work with at the Internet Society shuffle and scramble data across the globe to protect and deliver it as efficiently as possible via the Internet. Beyond harming efficiency and access speed, forcing data to be housed in one place is a security risk that makes our personal data more vulnerable to intruders. Such mandates also reduce the overall resilience of the Internet in the face of local or regional disruptions arising from natural or human-caused disaster.

- **Opposition of discriminatory data policies:** In our work at the Internet Society, we recognize that rules that determine which data is permitted or prohibited on national networks can hinder communication and cross-border Internet services, making it difficult for people to connect with each other. It also forces networks to have to inspect traffic—something only the largest businesses will be able to do—and puts both national security and citizens at risk of harm from surveillance and censorship.

- **Opposition of national demands to see the source code of foreign companies:** At the Internet Society, we see demanding access to source code as akin to requiring companies to

These principles are crucial for a unified and decentralized global Internet. Undermining them creates significant barriers to global communication. It deprives the world of some of the most important benefits that the Internet offers—the ability to access information from around the world, communicate around the world, and share the same online experience with family and friends around the world.

This foundational principle of the Internet—that if you can connect to the Internet, you can reach the world—is its unique value proposition. Without it, both education and medical care would suffer because people around the world would not be able to access the full body of knowledge on the Internet. Human rights would suffer because nations could restrict the ability of their citizens to access information that challenges the views of the government. Economic opportunity—especially for smaller companies—would be limited because it would be too expensive to comply with data regulations in numerous different countries. At the most basic level, people would be less able to keep in touch with loved ones, a basic yet critical feature of the Internet that helped much of the world through the recent pandemic. Data localization rules could make services like shared chat platforms impossible, meaning a grandparent might not be able to read a news story from another country about a grandchild's athletic event.

The United States has been a global leader in promoting open communications around the world. Its dramatic shift in digital trade policy threatens to undermine and undo over two decades of support for a global Internet. It will encourage countries worldwide to follow suit and erect new walls along country borders to restrict the flow of information in the name of digital sovereignty. The result of such policies is not "national internets" or "regional internets", but the loss of *the* Internet.

We call on the US government to reverse course and clarify its position to re-assert its support for an open, globally connected, secure, and trustworthy Internet.

Strengthening the Internet, Statements, North America

‹ Back

# EXHIBIT 34

# Reversal of US Trade Policy Threatens the Free and Open Internet

ALLIE FUNK, JENNIFER BRODY / NOV 14, 2023

*Jennifer Brody is Deputy Director of Policy and Advocacy for Technology and Democracy at Freedom House. Allie Funk is Research Director for Technology and Democracy.*

US Trade Representative Katherine Tai at an event in Riga, Latvia, June 2023. Shutterstock

A surprising reversal of long-standing US policy is slipping under the radar. The US government has long advocated for cross-border data flows, which are foundational for the global internet to function and help facilitate the protection of human rights. However, in late October, the US Trade

Representative (USTR), Katherine Tai, dropped support for these provisions, taking by surprise many people in government, civil society, and the private sector.

The abrupt policy pivot took place at the World Trade Organization (WTO) amid negotiations for the Joint Statement Initiative on E-Commerce. The need to create policy space for Congress and other bodies to regulate major tech firms is one explanation justifying the decision. But limiting cross-border data flows will likely do little to achieve this aim. It instead risks further fragmenting the global internet, emboldening authoritarian governments and their aspiring counterparts, and violating rights around the world. Particularly for people living in countries that already have data localization requirements, the impact on human rights is grave.

The US should instead wield its influence at the WTO to preserve cross-border data flows and demonstrate the myriad of alternative ways to regulate the private sector while protecting the free and open internet.

## Ceding to the authoritarian model of cyber sovereignty

This sudden reversal of US policy can be seen, as Senator Ron Wyden (D-OR) aptly noted, a "win for China's Great Firewall." At multilateral forums, the Chinese government has been working alongside like-minded governments to divide the global internet into state-run enclaves that can be more easily monitored, censored, and controlled. The former secretary general of the International Telecommunications Union (ITU), China's Houlin Zhao, encouraged shifting control over the setting of technical standards toward the ITU, where states hold the power, and away from civil society and other non-governmental experts. Similarly, the United Nations is currently negotiating a cybercrime treaty, originally proposed by Russian officials and co-sponsored by other authoritarian states including China, that could serve as a new vector for governments to criminalize online speech and access people's personal data if strong human rights safeguards are not incorporated.

Unsurprisingly, Chinese officials view the WTO as yet another forum to assert their approach. In negotiations over electronic commerce rules, the Chinese delegation has advocated for the need to consider "internet sovereignty" as a legitimate public policy objective.

The US has long taken an alternative approach to internet governance. Under President Joe Biden's leadership, the US and more than 60 countries signed the Declaration for the Future of the Internet, the cornerstone of US cyber and digital policy and a clear commitment to defend an interoperable, free, and global internet. The US also assumed the chair of the Freedom Online Coalition, a multilateral body of 38 governments, and a US official was elected over a Russian diplomat to lead the ITU. The administration's clear commitment to a global, open, and interoperable internet through these and other relevant initiatives makes the USTR's decision all the more puzzling.

The USTR argues that its position at the WTO aligns with its approach at the Indo-Pacific Economic Framework, another trade deal the administration is negotiating that has also since been halted for similar reasons. But disagreement within the government about the decision at the WTO is mounting. For instance, the National Security Council is reportedly frustrated and has pointed to the need for a "robust" inter-agency process to determine how best to move forward.

## The human rights implications of a more fragmented internet

Restrictions on cross-border data flows can undermine how the global internet operates. The transfer of data across jurisdictions improves internet speeds, enables companies to provide critical services worldwide, and allows data to be stored in the most secure data centers. There are also real human rights risks. On a fragmented internet, people have limited access to information from foreign sources, may struggle to connect with loved ones abroad, and may face barriers to organizing online with communities around the world.

Data localization laws are far from novel—and have long existed in countries such as China, Vietnam, and Russia—but the trend is clearly accelerating. From June 2021 to May 2022, Freedom House identified at least 23 countries that proposed or passed new requirements for local data storage. And over the past year, this number has only grown. By weakening support for cross-border data flows, the USTR may incentivize more governments to adopt these requirements.

Governments often point to concerns over privacy, cybersecurity, monopolistic practices, and online harms to justify the need for data localization. However, these requirements do little in addressing such genuine challenges. Instead, they enhance a government's ability to conduct digital repression by placing massive datasets of people's most intimate information more easily within reach. Particularly in countries with poor rule of law contexts, unconstrained and centralized access to people's data can lead to serious harms to privacy, free expression, freedom of belief, due process, and even physical security.

Growing requirements for data localization are happening alongside a record-breaking crackdown on free expression. And people's personal data – which can reveal who they voted for, who they worship, and who they love – help facilitate this. Rwanda's data protection law, for instance, mandates that companies store data locally unless the country's non-independent cybersecurity regulator approves otherwise. This requirement leaves personal data easily accessible in an environment in which authorities have embedded agents in telecommunications companies and used data from private messages to prosecute dissidents. Rwanda is not an outlier. 78 percent of the world's internet users live in countries where simply expressing political, social, and religious viewpoints leads to legal repercussions.

In Uzbekistan, authorities temporarily blocked Skype, TikTok, Twitter, VKontakte, WeChat, and other popular platforms due to their noncompliance with a data localization law, severely limiting people's ability to communicate and access information. While there are a range of reasons companies have resisted data localization requirements, some are at least in part doing so over concerns they will be complicit in government repression. When data is not stored locally, the respective government often must go through a legitimate–albeit far from perfect–legal process for accessing the information from US companies. But when data is stored on local servers, the ability for companies to resist problematic state demands is hampered. This challenge is further compounded by the emergence of so-called hostage-taking laws, in which international companies are required to have a local presence in a particular country, curbing their willingness to push back against user data requests over concerns for employee safety.

## Regulating Big Tech while protecting a global internet

Regulatory action against the private sector does not require limiting cross-border data flows. Instead, the US can demonstrate how to address poor data security and privacy, a lack of competitiveness in the tech sector, and ineffective oversight mechanisms while still safeguarding the global internet and advocating against data localization elsewhere.

For example, as called for in the Biden Administration's new AI executive order, Congress should pass a federal privacy law that sets strong rules for what data companies can collect, how they can store it, and with whom it can be shared. New laws should also require transparency of companies' AI and data collection systems, human rights due diligence reporting, and sharing platform data with vetted researchers. These safeguards could help people not only in the US but in countries around the world.

Regulatory bodies can also leverage their existing authority to act. The Federal Trade Commission (FTC) and Consumer Financial Protection Bureau are tackling challenges related to commercial surveillance, data security, and the data broker industry. Antitrust lawsuits from the FTC, state attorneys general, and Department of Justice could lay the groundwork for a more diverse and competitive tech sector, leading to better outcomes for people suffering the consequences of corporate malfeasance.

Protecting human rights online, strengthening platform responsibility, and safeguarding a global and interoperable internet are all mutually reinforcing. The US should be transparent about why this decision was made and develop a whole-of-government approach on the topic moving forward. Ultimately, USTR should return to the WTO negotiating table with a renewed commitment in support of cross-border data flows and galvanize allies to reach consensus on this issue. The internet's future – and the rights of the people who use it – depend on it.

# EXHIBIT 35

# The Human Rights Costs of Data Localization Around the World

ALLIE FUNK, JENNIFER BRODY / MAR 26, 2024

*Four civil society experts weigh in on why data localization is becoming an increasingly common policy and what this means for people's rights.*

Network switches. Shutterstock

Data localization, in which companies are mandated to store personal data on local servers, is a growing policy area. But particularly in contexts with poor rule of law, such requirements can allow authorities to access people's data more easily, creating a fertile ground for human rights abuses. Restricting the free flow of data also accelerates the fragmentation of the global internet.

Last October, debate on this topic was again thrown on the international stage when the United States Trade Representative withdrew its support for cross-border data flows at the World Trade Organization. In doing so, the USTR risks exacerbating the growing prevalence of data localization and encouraging other governments to follow suit.

In the discussion below, Freedom House's Allie Funk and Jennifer Brody interview four experts analyzing data localization across Africa, Asia, and Eastern Europe:

- **Alena Epifanova**, Research Fellow at the German Council on Foreign Relations (DGAP)
- **Lillian Nalwoga**, Programme Manager at the Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
- **Shmyla Khan**, Digital Rights Researcher and Campaigner
- **Sabhanaz Rashid Diya**, Founder and Executive Director of the Tech Global Institute

The discussion sheds light on the myriad ways in which data localization is incorporated into law, the complex drivers behind it and associated human rights implications, and how democratic leaders can support global civil society's work to protect human rights online. Note: this record of the conversation has been lightly edited for clarity and concision.

**Allie Funk and Jennifer Brody:**

Data localization comes in many different forms depending on a country's political and legal context. How has this issue emerged in the country or region you focus on?

**Alena Epifanova:**

The data localization law was adopted in Russia in July 2014 against the backdrop of escalating tensions with the West following Edward Snowden's revelations about US government surveillance, as well as Russia's annexation of Crimea. The Kremlin's perception that digital technologies and data could be weaponized against Russia from foreign actors has significantly grown and triggered a shift to strengthening sovereignty. During the same time, Putin's regime faced the largest protests in Russia since the 1990s and aimed to assert the upper hand in controlling all levels of Russian political life and society.

**Lillian Nalwoga:**

Data localization is becoming a growing trend in Africa with a number of countries enacting data protection laws that require data to be stored locally and forbid cross-border transfers of personal data unless authorized by the data protection authorities or designated entities. Governments are using cybersecurity, financial services, and telecommunication regulations to do this.

**Sabhanaz Rashid Diya:**

Data localization has been a growing trend in Asia with many governments enacting legislation that mandate varying degrees of restrictions on cross-border transfers. In Bangladesh, financial services regulations have been used to impose sector-specific local data storage requirements for resident companies. Since 2020, various drafts of the Data Protection Act have imposed forms of mandatory restrictions on international data transfers for both resident and non-resident entities. The country's most recent draft imposes a de facto restriction on cross-border transfer of personal data by making it contingent on having bilateral, regional, or multilateral agreements with transferee countries, while requiring mandatory storage of "classified data," a term undefined in the statute.

**Shmyla Khan**:

Data localization in Pakistan has cropped up in two pieces of proposed legislation: the draft Personal Data Protection Bill and the Rules for Removal and Blocking of Unlawful Online Content (Procedure, Oversight, and Safeguards) Rules, 2020 which focus on "securing" "sensitive personal data" within the boundaries of the country. These laws also require social media companies to register inside the country and establish local offices.

**Allie Funk and Jennifer Brody:**

Freedom House has developed a three-tiered approach to assess the extent to which data localization policies impact privacy, free expression, due process, and other fundamental freedoms. What are you concerned about from a human rights perspective? How have you seen these concerns play out?

**Lillian Nalwoga:**

Unfettered access to personal data undermines data privacy as it gives states the ability to surveil users as and when needed. In Africa, countries with data localization policies are also spending billions of US dollars to buy surveillance technologies and implement data collection programs. Many countries lack the necessary measures to protect personal data, such as adequate privacy laws, and where these laws are present, their implementation is wanting.

**Alena Epifanova:**

When coupled with additional legislation, data localization laws and user data protection measures can be exploited for mass surveillance purposes. In 2016, Russia enacted two federal bills collectively referred to as the "Yarovaya Law." This legislation mandates Internet Service Providers and online platforms to retain user data, including messages, phone calls, images, and other information, for a duration of up to six months. Moreover, it grants the Federal Security Service of Russia (FSB) access to this data upon request, even in the absence of a court order; for instance, the FSB got access to databases of taxi companies in 2023.

**Shmyla Khan:**

Within the Pakistani context, the state, particularly the military establishment, already has access to vast amounts of information and is largely unaccountable. The prospect of having personal data stored on local servers further allows the state to prosecute people for offenses relating to their online speech, such as religious expression or for alleged sedition. It also reduces companies' ability to refuse data requests.

**Sabhanaz Rashid Diya:**

States are increasingly leaning towards legalization of access to vast amounts of personal data without procedural guardrails, expanding their ability to surveil and suppress people. For example, the Bangladesh Telecommunication Regulatory Act, 2018, has provisions requiring telecommunication operators to hand over personal data about their users to law enforcement agencies, else risk losing their licenses. Similar provisions were introduced in both the Cyber Security Act, 2023 and the draft Data Protection Act, 2023. Similarly, India's Digital Personal Data Protection Act, 2023, provides broad exemptions to government entities from procedural guardrails and allows access to personal data on vague grounds of national security and public order. If storage in domestic servers becomes mandatory, then it becomes easier for state entities to coerce access to sensitive data that exacerbates surveillance and self-censorship.

**Allie Funk and Jennifer Brody:**

Any other concerns you want to bring up about the impact of these laws?

**Alena Epifanova:**

Data localization contributes to the fragmentation of the global internet. More and more countries are seeking to assert their sovereignty, build their own internet infrastructure, and introduce their own regulations on data flow. The splintering of the global internet is already impacting how people access information, express themselves online, and communicate with each other.

**Shmyla Khan**:

Countries like Pakistan lack the necessary technical and energy capacity (the country experiences frequent electricity "load shedding") to host such servers. It also creates security issues for the data collected as the country lacks good digital security protocols.

**Sabhanaz Rashid Diya**:

Many Global Majority countries lack the institutional safeguards and infrastructure capacities to keep personal data secure within their national borders. This risks more frequent data breach and privacy violations with little to no meaningful recourse available to the general public.

**Allie Funk and Jennifer Brody:**

Policymakers often pursue data localization in an attempt to tackle legitimate concerns that deserve thoughtful policy responses– such as cybersecurity, better protections for data, bolstering local tech sectors, or countering tech companies' monopolistic practices. Do you have ideas for more rights respecting solutions to these problems?

**Sabhanaz Rashid Diya**:

There is substantive evidence that data localization *alone* cannot bolster local tech sectors or strengthen cybersecurity. Many governments are still pursuing the idea that if *only* they had access to *more* data, then many overarching national security challenges would be resolved.

However, in the absence of investigation capabilities, investments in local tech sectors, developing talent pipelines, robust competition laws, and mainstreaming media literacy, data localization can do little to respond to any of the aforementioned gaps. The "money" in data lies with its processing, not storage, therefore, countries will generally benefit more from creating incentives to boost their local tech sectors and ecosystems.

**Lillian Nalwoga:**

Governments need to draw a balance between data localization, data privacy, and digital transformation agendas. In the case of Africa, different countries are at different levels of digital development and adoption. Restrictions on cross-border data transfers may not only impede efforts to meet the localization demands mandated by certain laws but also limit progress toward adopting their digital transformation agendas.

**Shmyla Khan:**

The government has often used the rubric of tackling cybercrimes and national security concerns to justify these laws. However, history shows that many laws made on this basis of national security are used to silence dissent online.

**Allie Funk and Jennifer Brody:**

How can democratic governments engage and support civil society's efforts to counter data localization?

**Alena Epifanova:**

Democratic policymakers should foster a discussion on the concept of digital sovereignty, which revolves around individual's self-determination and democratic values in the digital realm. Conducting human rights assessments of proposed data localization policies should be imperative. Enhancing international cooperation within organizations such as the World Trade Organization, G20, and the

Organization for Economic Co-operation and Development is crucial to ensure the unrestricted flow of data.

**Lillian Nalwoga:**

I agree with Alena. Democratic governments can provide aid to strengthen infrastructure and invest in innovation and human capital skilling.

**Sabhanaz Rashid Diya:**

Civil society is doing the hard work to navigate a myriad of legislation and to create better regulatory frameworks, but they need the short- and long-term support to do this work. This includes both financial resources and capacity building opportunities. Democratic policymakers should also support civil society's efforts to explore alternative governance models and regulatory innovation. There is not a one-size-fits-all approach to regulating digital ecosystems. What works in one country may not work in another. Instead, laws should be reflective of local needs and communities' realities, while ensuring legislation abides by international human rights law and democratic standards of transparency and inclusivity.

**Shmyla Khan:**

Most countries in the Global South feel left out of the gains from the tech industry, and thus feel compelled to adopt nativist strategies such as data localization to gain more control over data. Democratic actors can help ensure that the benefits from digital technology are equitably distributed and that governments have the resources and capacity to deal with a changing world. They can also strengthen support for local civil society, who are best placed to have these nuanced conversations that can balance the need for regulation of big tech while resisting efforts by undemocratic governments to assert control over personal data.

---

## AUTHORS


### ALLIE FUNK

Allie Funk leads Freedom House's technology and democracy initiative, including Freedom on the Net and Election Watch for the Digital Age. She also represents Freedom House on the Freedom Online Coalition's Advisory Network and at the Global Network Initiative. In addition to Tech Policy Pres, her w...

# EXHIBIT 36

# THE NEW BIG BROTHER

## China and Digital Authoritarianism

A Democratic Staff Report
Prepared for the use of the
Committee on Foreign Relations
United States Senate
July 21, 2020

## TABLE OF CONTENTS


Letter of Transmittal ..... 1

Preface on the Coronavirus ..... 3

Executive Summary ..... 5

**Chapter 1: Building the Model for Digital Authoritarianism Inside China** ..... 9

The Surveillance State: How China Tracks its Citizens ..... 9

The Censorship Apparatus: Exploiting and Blocking Digital Content ..... 16

The Legal System: China's Implementation of Authoritarian Cyber Laws ..... 20

China's Investment in Technologies Predicated on Authoritarian Principles ..... 22

**Chapter 2: Exporting Digital Authoritarianism – China on the Global Cyber Stage** ..... 26

Exporting Technologies and Expanding Digital Authoritarianism ..... 27

Case Study: Venezuela ..... 31

Case Study: Central Asia ..... 33

Case Study: Ecuador ..... 33

Case Study: Zimbabwe ..... 34

A Global Challenge ..... 35

**Chapter 3: Institutionalizing Digital Authoritarianism – China at International Fora** ..... 37

The United Nations ..... 38

World Trade Organization ..... 40

World Internet Conference ..... 41

International Standards-Setting Bodies ..... 42

**Chapter 4: Conclusions and Recommendations** ..... 45

Recommendations ..... 46

**Annex 1: Understanding the Trump Cyberspace Policy** ..... 49

National Security Policy Documents ..... 49

Administration Efforts ..... 51

**Annex 2: The United States and 5G** ..... 55

# Letter of Transmittal

United States Senate,
Committee on Foreign Relations,
*July 21, 2020*

**Dear Colleagues:** The growth and development of the digital domain worldwide has fundamentally changed how individuals, companies, and nations interact, work, and communicate – and with it the structure of global governance. Digitally-enabled technologies ranging from the Internet to mobile communications to emerging technologies, such as artificial intelligence, are accelerating the transmittal and receiving of information, enabling greater trade interactions and economic development, securing communications for our military and our allies, and aiding in the development of even newer, more capable technologies, amongst many other benefits. The United States has not only played a primary role in developing these new technologies, but it has worked to ensure the digital domain operates with openness, stability, reliability, interoperability, security, and respect for human rights.

These principles are under threat from authoritarian regimes, however, which see the advent of new technologies in a far more sinister light: as a means of surveilling and controlling populations, stifling the free flow of information, ensuring the survival of their governments, and as tools for malign influence campaigns worldwide. While multiple authoritarian governments have begun to utilize the digital domain in this manner, the People's Republic of China is at the forefront of developing and expanding a new, different, and deeply troubling governance model for the digital domain: digital authoritarianism.

The rise of this new and worrying model of digital authoritarianism holds the potential to fundamentally alter the character of the digital domain. The People's Republic of China is pressing forward—at times with astounding speed and focus—to build and expand digital authoritarianism through economic, political, diplomatic, and coercive means at home and abroad. The Chinese Communist Party is fostering digital authoritarianism within China's borders by developing an intrusive, omnipresent surveillance state that uses emerging technologies to track individuals with greater efficiency and bolstering its censorship apparatus to ensure information considered detrimental to the regime does not reach its citizens.

The government is shaping a legal system to strengthen the Party's manipulation of the tools of digital authoritarianism and expending vast sums of money to prop up Chinese companies that develop products that enable its authoritarian governance model. On the international level, China is exporting digitally enabled products and the training and expertise to other countries in an attempt to sway other nations to adopt this alternative, authoritarian model for the digital domain. As we have seem time and time again, with examples ranging from Marriott's pull-down menu to the NBA to Zoom's suspension of U.S. host accounts, China is seeking to utilize its newfound clout to reshape the rules of the road in cyberspace away from a free, unfettered, and secure environment to one that facilitates the growth of authoritarianism.

The United States, as the leader of the free world, must stand up for the principles and values that animate the international community and push back against the expansion of digital authoritarianism, using our economic prowess, unmatched innovative and scientific spirit, and ability to bring like-minded countries together. If the United States fails to lead the international community in assuring that governance of the digital domain is consistent with principles and values

that benefit all, then it will be China, not the international community at large, which will shape the future of the digital domain.

Given the critical importance of this issue for the future of global governance—and the clear need for the United States to reassert leadership within this space—I directed Senate Foreign Relations Committee staffers Michael Schiffer and Daniel Ricchetti to conduct a comprehensive study of China's effort to build and expand its model for digital authoritarianism and lay out recommendations for the U.S. government to consider. The report uses primary document research, news and subject-matter analysis, and interviews from both former government officials and nongovernmental experts. I want to thank Doug Levinson, Laura Truitt, Nina Russell, Nadhika Ramachandran, Elizabeth Shneider, and the SFRC Democratic Staff for their work on this report. I would also like to thank Julie Smith, Amy Studdart, and Tommy Ross for reviewing this report and the Congressional Research Service for their contributions.[1]

The report's comprehensive analysis of China's digital authoritarianism describes how the People's Republic of China is successfully developing and implementing its malign governance model internally and, increasingly, making inroads with other countries to also embrace its new digital doctrine. It further illustrates how the expansion of digital authoritarianism in China and abroad has drastic consequences for U.S. and allied security interests, the promotion of human rights, and the future stability of cyberspace. Consequently, the report calls for a series of both Congressional and Executive actions designed to counter China's efforts to expand its model of digital authoritarianism; to strengthen U.S. technological innovation; and, to reinvigorate our diplomatic endeavors around the globe on digital issues. I believe these recommendations are readily available for adoption and implementation by both Democrats and Republicans. Without bipartisan support and the full backing of the United States government, the American people will be far less secure in the digital domain in the years ahead, see a further breakdown of fundamental human rights, and witness the erosion of a free, stable, reliable, and secure digital domain while China's digital authoritarianism is allowed to flourish. American leadership on these issues has been sorely lacking the past three years. It is my sincere hope that this report will serve as a useful bipartisan rallying point for my colleagues in Congress so that we can work together to arrest the erosion of our position and to reassert American leadership and values on the world stage.

Sincerely,

Robert Menendez
Ranking Member

[1] The conclusions of the report do not necessarily reflect the views of the Congressional Research Service.

## Preface on the Coronavirus

When the Senate Foreign Relations Committee Democratic Staff was first tasked with drafting this report, a consensus was emerging that the January 2018 National Defense Strategy's depiction of the "reemergence of long-term strategic competition" against such great power rivals as Russia and China would indeed be the "central challenge" to U.S. interests and security for the balance of the twenty-first century.[2] The Trump administration's characterization of the United States and China entering a "new era of strategic competition" received broad bipartisan support in the Senate as a largely accurate characterization – even if significant differences remained about how to structure U.S. national security policy accordingly.

Moreover, the suites of new and emergent digital technologies that are remaking the face of the U.S. and the global economies—including 5G infrastructure, social media, block-chain, digital surveillance, and genomics and biotechnology—are all widely acknowledged as being on the cutting edge of this new competition and fundamental for U.S. national security in the twenty-first century. Concerns regarding these emergent technologies are embedded in questions about the different, and competing, governance models for their use and control. These differing governance models are shaped by the form and nature of democratic and authoritarian states, which are continually developing, innovating, and operating in the digital space. Areas of competition between democratic and authoritarian states therefore encompass concerns about secure supply chains, privacy, human rights, standards, and the rules of the road for how these technologies would be used by the international community, including sharp power practices for technologies that shape and negotiate culture, education, and the media and are situated at the intersection of diplomacy, influence, and technology.

This report primarily examines how China's repressive government is creating a model of digital authoritarianism for the digital space and what it is doing to both strengthen the model in its own country and expand it internationally. However, the onset of the COVID-19 pandemic in December 2019 has raised a new set of questions about the state and nature of security challenges facing the United States in the twenty-first century, great power competition, and the diffusion and distribution of power in the international system. Moreover, the COVID-19 pandemic has stimulated additional questions about the governance of new and emergent digital technologies and the ways in which democratic and authoritarian states will seek to use them, for good or ill. Due to the fact that research, outside interviews, and the vast majority of the drafting of this report occurred before the outbreak of COVID-19, this report does not delve into how the novel coronavirus is shaping or may shape the future of the digital space as it pertains to digital authoritarianism. However, the connection between COVID-19 and digital authoritarianism is an important subject to examine in the future. This preface is intended to signal the significance of this topic and provide a brief roadmap for what issues may arise moving forward.

One key issue regarding COVID-19 and the digital space is that several democratic states, including South Korea and Taiwan, have adopted privacy practices to combat COVID-19 that previously were regarded as overbearing, all in the service of public health and responsive governance.[3] Meanwhile,

---

[2]Secretary of Defense James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, U.S. Department of Defense, Jan. 2018, at 2.

[3] Anthony Kuhn, "South Korea's Tracking Of COVID-19 Patients Raises Privacy Concerns," *NPR*, May 2, 2020; Milo Hsieh, "Coronavirus: Under surveillance and confined at home in Taiwan," BBC, Mar. 24, 2020.

China's extensive use of surveillance technologies, both to manage its own COVID-19 outbreak and to continue suppressing internal dissent and exerting control in Xinjiang and Tibet, has only served to exemplify the malign use of these tools in the hands of a government that is not answerable to its people. In many cases, the underlying technology and platforms used by different governments are the same or largely similar; it is governance models, political culture, transparency, norms of behavior, and the rule of law that separate the public good from political oppression. Questions regarding the use of these technologies have become only more serious, and the implications more clear, in the face of the pandemic.

Furthermore, these questions are not confined to matters of domestic policy. As the COVID-19 pandemic has progressed, an intense competition for global influence has emerged, with China and Russia seeking to use their digital toolkits to exploit the debates over the public health challenges the pandemic has created in the United States, Europe, and elsewhere. The purpose of controlling such a narrative is to make democracy look less attractive than a "capable" authoritarian model and to use the pandemic to attack the fabric of the democratic system itself.

As the COVID-19 pandemic has all too well illustrated, the brave new world of digital technological use and misuse is already upon us, and policymakers now need to move quickly to determine what sort of people—and what sort of governance—we will have in it.

## Executive Summary

In an era in which rising authoritarianism is working to undermine the fabric of democratic institutions globally, the Internet and connected technologies represent a continually evolving domain that will fundamentally shape the future of politics, economics, warfare, and culture. Cyberspace remains relatively undefined and open to new rulemaking, standardization, and development. The United States has been and remains the premier digital innovator on the globe, and as such the primary entity capable of shaping the future of the digital environment. However, China's rapid rise in key fields, investment in new digital technologies, efforts abroad, and attempts at dominating international rule-making bodies are positioning it to erode the United States' leadership on technological issues and reconfigure the standards of the domain away from free, democratic values.

China has the largest number of Internet users on the planet, with more than 800 million Chinese citizens connected to some form of Internet.[4] Chinese technology companies such as Huawei and ZTE are at the forefront of developing and implementing fifth-generation (5G) telecommunications infrastructure. Chinese patent publications have surged in emerging technology fields such as artificial intelligence (AI), machine learning, and deep learning.[5] China's Belt and Road Initiative (BRI) contains an effort "to create a 'digital Silk Road' that will allow it to shape the future of the global Internet—and reinforce the Chinese Communist Party's leadership at home for decades to come."[6] These endeavors underline that China understands the importance of the digital domain to its domestic political stability and economic, political, and military rise, and wants to lead the globe in shaping the future of the digital world. It further demonstrates that China is executing a long-term plan to dominate the digital space.

While China's rise in the digital space is concerning to the United States in and of itself, an additional pressing issue facing not only the United States but the free world at large is how China is influencing and reshaping the Internet in its own political image. China's government structure can be defined as a repressive, authoritarian regime. In its 2020 Freedom of the World ratings, Freedom House labeled China as "not free" and described the regime as "increasingly repressive in recent years."[7] Despite China's authoritarian style of governing, the country's rise as a major economic and political player in the international sphere is providing the communist regime with increased status among other nations. As journalist Richard McGregor notes, China is pushing "the idea that

---

[4] François Godement et al., "The China Dream Goes Digital: Technology in the Age of Xi," *European Council of Foreign Relations*, Oct. 25, 2018; "China has 854 mln internet users: report," *Xinhua*, Aug. 30, 2019.

[5] World Intellectual Property Organization, *WIPO Technology Trends 2019: Artificial* Intelligence (Geneva: World Intellectual Property Organization, 2019), at 32; Louise Lucas & Richard Waters, "China and US Compete to Dominate Big Data," *Financial Times*, May 1, 2018.

[6] Stewart M. Patrick & Ashley Feng, "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road," *The Internationalist* (blog), *Council of Foreign Relations*, July 2, 2018, https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road; "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," *National Development and Reform Commission, Ministry of Foreign and Affairs and Ministry of Commerce of the People's Republic of China, with State Council Authorization*, March 2015, https://reconasia-production.s3.amazonaws.com/media/filer_public/e0/22/e0228017-7463-46fc-9094-0465a6f1ca23/vision_and_actions_on_jointly_building_silk_road_economic_belt_and_21st-century_maritime_silk_road.pdf.

[7] "Freedom of the World 2020: China," *Freedom House,* https://freedomhouse.org/country/china/freedom-world/2020 (last visited May 20, 2020).

authoritarian political systems are not only legitimate but can outperform Western democracies."[8] China's growing influence on the digital sphere is no different, as it enables China to promote an alternative model for the digital domain based on state control.

This model stands in stark contrast to what the United States and its allies espouse: a free and open Internet that encourages the free flow of information and commerce in ways that advance innovation and market-driven economic growth. Increasingly, other foreign nations, including Ecuador, Serbia, Zimbabwe, Uzbekistan, Kyrgyzstan, and Pakistan have or are looking to acquire Chinese information and communications technologies (ICT) and integrate them into their national infrastructures, opening up potential opportunities for abuse.[9] **China's efforts to advance and proliferate its ICT hardware and systems, both in China and overseas, represent not only a desire to continually expand its economy, but also a push to establish, expand, internationalize, and institutionalize a model for digital governance that this report describes as "digital authoritarianism."**[10]

*Definition - Digital Authoritarianism*
*The use of ICT products and services to surveil, repress, and manipulate domestic and foreign populations.*[11]

China's rise as a key player in the digital domain that uses its influence to promote digital authoritarianism presents fundamental security, privacy, and human rights concerns for the United States and the international community at large. Most troubling, China is working to undermine our democratic institutions and values. Due to the fundamental risks associated with the rise of China's digital authoritarianism, the Senate Foreign Relations Committee (SFRC) Democratic Staff examined the subject for the past year in an effort to provide a holistic study of the threats posed to the United States, our allies, and the international community. As part of its analysis, SFRC Democratic Staff reviewed primary source materials including reports, studies, and official Chinese government releases, as well as news sources, and conducted interviews with former U.S. government officials and non-governmental experts who work in the fields of human rights, technology, cybersecurity or China policy.

The examination conducted by SFRC Democratic Staff offers concerning insights about how China is leveraging new technologies to assert increased control over its population and strengthening its ties with other nations around the globe. This report underscores, for example, how China's government employs facial recognition technology and big data analysis tools to identify, discriminate, incarcerate, and "re-educate" Uyghurs living in Xinjiang, essentially creating a police state that flouts basic human rights and civil liberties. China is not just using these tools at home; it is also working to export its high-tech tools and authoritarian principles throughout the globe. While

[8] Richard McGregor, "Xi Jinping's Ideological Ambitions," *The Wall Street Journal,* Mar. 2, 2018.
[9] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019; Abdi Latif Dahir, "China is exporting its digital surveillance methods to African countries," *Quartz Africa*, Nov. 1, 2018; Yau Tsz Yan, "China taking Big Brother to Central Asia," *Eurasianet*, Sept. 6, 2019, https://eurasianet.org/china-taking-big-brother-to-central-asia; "Chinese facial recognition tech installed in nations vulnerable to abuse," *CBS News*, Oct. 16, 2019; Justin Sherman, "U.S. Diplomacy Is a Necessary Part of Countering China's Digital Authoritarianism," *Lawfare*, Mar. 17, 2020, https://www.lawfareblog.com/us-diplomacy-necessary-part-countering-chinas-digital-authoritarianism.
[10] Alina Polyakova & Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *The Brookings Institution*, Aug. 2019.
[11] *See, e.g.,* Alina Polyakova & Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *The Brookings Institution*, Aug. 2019.

these examples are emblematic of the rise of China's digital authoritarianism, the fundamental takeaway of this report is that **if left unchecked, China, not the U.S. and our allies, will write the rules of the digital domain, opening the doors for digital authoritarianism to govern the Internet and associated technologies.**

This report provides an incisive examination of the key aspects of China's digital authoritarianism, the insidious nature of its proliferation inside China, the damage it is causing around the globe, and proposed legislative solutions and other measures the United States could adopt. In **Chapter 1**, the report describes China's internal model for digital authoritarianism and how China implements digital authoritarianism domestically. The chapter is divided into four subsections, with each subsection highlighting a specific aspect of China's digital authoritarianism model. The first subsection deals with China's "surveillance state," including how China utilizes artificial intelligence, facial recognition technologies, biometrics, surveillance cameras, and big data analytics to profile and categorize individuals quickly, track movements, predict activities, and preemptively take action against those considered a threat in both the real world and online. The second subsection looks into China's digital censorship apparatus and the tools that the Chinese government uses to control flows of data, such as the use of the "Great Firewall" to oversee information and block foreign technology platforms in China. The third subsection delves into China's legal system and how the government is implementing new laws that further strengthen the government apparatus that allows China's digital authoritarianism to flourish. Lastly, subsection four studies China's massive investments in companies that develop new technologies that are both predicated on and aid China's authoritarian principles.

**Chapter 2** examines how China is exporting its digital technologies around the globe as a means of increasing its influence in other nations and, more dangerously, expanding the technologies and methods used for digital authoritarianism. This chapter looks at (1) China's export of underlying digital infrastructure technologies and (2) China's global proliferation of systems and technologies that run on those digital infrastructure technologies, thus advancing China's model for social control. Additionally, the chapter provides case studies of countries around the globe to demonstrate how China is integrating its technologies into these countries and how said integration impacts each nation.

**Chapter 3** details China's efforts at strengthening its involvement and influence in intergovernmental fora. The chapter looks into how China is increasingly using fora such as the United Nations (UN), World Trade Organization (WTO), and other standards-setting bodies to push a Chinese-centric digital domain. China's involvement in these bodies is directly impacting the future rules of the road for cyberspace, and at a time when the United States seems to be receding from its traditional role as leader of the free world, China is filling the gap.

**Chapter 4** elucidates the report's conclusions and policy recommendations. The recommendations focus on government actions, especially by Congress, to address and counter China's rise as a technological power and its desire to proliferate its model of digital authoritarianism. This section recommends legislation that establishes a public-private consortium aimed at creating a United States 5G alternative to Chinese technologies, legislation which institutes a Digital Rights Promotion Fund to help organizations push back against China's use and weaponization of mass surveillance, and legislation that would found a cyber military service academy. The report calls for the President to lead a coalition of countries to counter China's digital authoritarianism and push for a free, stable, unfettered, and secure digital domain. These recommendations stem from the understanding that

Congress has a special responsibility, as the constitutionally mandated lawmaking body of the United States, to develop and institute laws that protect against the rise and spread of China and digital authoritarianism. Such a role is especially important at a time when the executive branch has done little to combat digital authoritarianism, leaving the United States, our allies, our partners, and the global community at risk from the proliferation of digital authoritarianism.

This report contains two annexes. Annex 1 discusses the Trump administration's various cyber efforts and how these efforts have been deficient in countering China's continued rise as both a global geopolitical player and technological rival. Annex 2 provides an explanation of the 5G battle occurring between the United States and China. This overview highlights how China is attempting to dominate the 5G space and the present gaps in U.S. policy regarding this critical issue.

## Chapter 1: Building the Model for Digital Authoritarianism Inside China

In his October 18, 2017 opening address to the 19th National Congress of the Chinese Communist Party (CCP, or the Party), General Secretary of the Communist Party of China and President of the People's Republic of China (PRC) Xi Jinping articulated a vision for restrictions in the digital domain. In the address, Xi stated:

> We will maintain the right tone in public communication…We will provide more and better online content and put in place a system for integrated internet management to ensure a clean cyberspace. We will implement the system of responsibility for ideological work… distinguish between matters of political principle, issues of understanding and thinking, and academic viewpoints, but we must oppose and resist various erroneous views with a clear stand.[12]

Xi's statement shows the CCP's broad objective: bolstering development of the Internet while mitigating the threats the Internet poses to CCP rule. Xi placed particular emphasis on the intent to ensure the CCP's control of ideas in cyberspace **by limiting access to information and ideas that run counter to the Party's ideology.** The promotion and preservation of CCP control of China's own digital domain undergirds the CCP's entire digital authoritarianism model. For the CCP to continue moving towards its long-term objectives of becoming the dominant player in the cyber domain and expanding its influence abroad, it must first ensure that it has pacified Chinese citizens and purged dissent. **In simple terms, China's digital authoritarianism starts at home.**

To accomplish this goal, the CCP has developed a unique model for digital authoritarianism implemented through a combination of technologies, regulations, and policies in four areas: (1) surveilling and tracking Chinese citizens, (2) exploiting and blocking data and content stored or transmitted on the digital domain, (3) implementing authoritarian cyber laws, and (4) directing massive investments in new technologies to secure the Party's future. The CCP uses these tools in concert with one another to shape the Chinese digital domain into a repressive, controlled space that stifles dissent, controls individual movement, curtails expression, flouts basic human rights for Chinese individuals, and helps enable and sustain the CCP's authoritarian rule.

### *The Surveillance State: How China Tracks its Citizens*

The CCP regime has long depended on its ability to track and surveil China's population to ensure its survival and promulgate its authoritarian rule. The Party has used various methods to surveil individuals living in China since the inception of the communist regime. Digital tools provide the CCP with a range of new options that greatly enhance its ability to monitor citizens, turning China into a surveillance state. Emerging technologies such as facial recognition, biometrics, and other cutting edge tools enable China to profile and categorize individuals quickly in massive quantities, track movements, and preemptively take action against those considered a threat in both the real

[12] Xi Jinping, General Secretary of the Chinese Communist Party (CCP) and President of the People's Republic of China (PRC), "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," Speech Delivered at the 19th National Congress of the Communist Party of China, Oct. 28, 2017, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

world and online.[13] The aforementioned technologies are combined with repressive regulations and burgeoning, omnipresent monitoring tools such as the Social Credit System currently being rolled out by the Chinese state.[14] This combination of technologies, tools, and regulations creates a structure where practically all citizens are surveilled, and those considered problematic to the regime face massive civil and political repression, including "mass arbitrary detention, forced political indoctrination, restrictions on movement, and religious oppression" as seen in Xinjiang.[15]

Facial recognition technology is a key tool used by the Party to monitor citizens. Chinese authorities combine traditional video surveillance with innovative big data analytics tools to allow the government to monitor its 1.4 billion citizens.[16] China is a world leader in the video surveillance industry. For example, two Chinese companies, the Hangzhou Hikvision Digital Technology Company (Hikvision) and the Zhejiang Dahua Technology Company (Dahua), together control one-third of the global market for video surveillance.[17] Companies such as Hikvision and Dahua have aided the buildout of an extensive closed-circuit television (CCTV) infrastructure in China.[18] China currently is deploying more than 200 million cameras throughout the country, and an estimated 560 million are expected to be installed by 2021.[19] The cameras themselves are useful to Chinese authorities, but the integration of cameras with burgeoning artificial intelligence (AI) programs, which allows authorities to churn through massive amounts of data and identify individuals more rapidly, makes the system far more effective and repressive.[20]

China is quickly emerging as a global leader in integrating artificial intelligence and facial biometric data to bolster surveillance capabilities. Chinese companies, ranging from older industry stalwarts such as Hikvision to newer startups like Yitu Technology (Yitu) and Megvii Technology Limited (Megvii), are using emerging technologies to analyze vast troves of images and information

---

[13] *See, e.g.,* Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, Apr. 14, 2019; Josh Chin & Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal*, Dec. 19, 2017.

[14] Christina Zhou and Bang Xiao, "China's Social Credit System is pegged to be fully operational by 2020 — but what will it look like?," *ABC News*, Jan. 1, 2020; Hollie Russon Gilman & Daniel Benaim, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *New America*, Aug. 23, 2018, https://www.newamerica.org/weekly/chinas-aggressive-surveillance-technology-will-spread-beyond-its-borders/; Steve Mollman, "China's new weapon of choice is your face," *Quartz*, Oct. 5, 2019

[15] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 1 (May 2019); Steve Mollman, "China's new weapon of choice is your face," *Quartz*, Oct. 5, 2019; Hollie Russon Gilman & Daniel Benaim, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *New America*, Aug. 23, 2018, https://www.newamerica.org/weekly/chinas-aggressive-surveillance-technology-will-spread-beyond-its-borders/.

[16] World Bank, "China," https://data.worldbank.org/country/china (last visited Apr. 28, 2020).

[17] Editorial, *Konzept: 13 Tipping Points in 2018*, Deutsche Bank Research (January 2018), at 34, https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000459680/13_Tipping_points_in_2018.pdf.

[18] Danielle Cave et al., "Mapping more of China's tech giants: AI and surveillance," *Australian Strategic Policy Institute*, Nov. 28, 2019, https://www.aspi.org.au/report/mapping-more-chinas-tech-giants; Chris Buckley & Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York* Times, May 22, 2019; Ben Dooley, "Chinese Firms Cash in on Xinjiang's Growing Police State," *Agence France-Presse*, June 27, 2018.

[19] Amanda Lentino, "This Chinese Facial Recognition Start-Up Can Identify A Person in Seconds," *CNBC*, May 16, 2019; *The Economist*, "China: Facial Recognition and State Control," Oct. 24, 2018, https://www.youtube.com/watch?v=lH2gMNrUuEY (last visited Apr. 28, 2020); Thomas Ricker, "The US, like China, has about one surveillance camera for every four people, says report," *The Verge*, Dec. 9, 2019, https://www.theverge.com/2019/12/9/21002515/surveillance-cameras-globally-us-china-amount-citizens.

[20] Emily Feng, "How China Is Using Facial Recognition Technology," *NPR*, Dec. 16, 2019.

processed by cameras to strengthen facial recognition programs.[21] These programs support the underlying capabilities used to develop the databases that China's government and public security officials draw on to identify and monitor individuals. The databases rely on machine learning, a process in which "engineers feed data to artificial intelligence systems to train them to recognize patterns or traits."[22] The technology, however, is still imperfect. Accurate hits on recognizing individual faces depend on environmental factors, including lighting and the positioning of cameras.[23]

Technical flaws have not dissuaded the Chinese government from vastly expanding the scope and use of artificial intelligence for policing and surveillance, and the technology's efficacy continues to improve. The Chinese government aims to have a video surveillance network that is "omnipresent, fully networked, always working and fully controllable" by 2020.[24] Chinese government investment in these technologies is also slated to continue growing, with one expert stating that China's police is preparing to "spend an additional $30 billion in the coming years on techno-enabled snooping."[25] As China perfects these tools, it will acquire even more invasive capabilities for surveilling its people.

The CCP further augments its surveillance system with other important techniques that amplify surveillance capabilities. Chinese officials throughout the country are collecting and collating biometric data, such as DNA samples, fingerprints, voice samples, and blood types.[26] In a report on Xinjiang, Human Rights Watch (HRW) wrote that collecting this information "is part of the government's drive to form a 'multi-modal' biometric portrait of individuals and to gather ever more data about its citizens."[27]

The Chinese government has also extracted vast amounts of private data by using technologies to monitor activities and communications conducted over the Internet. For example, Chinese authorities force specific mobile applications on individuals in or entering Xinjiang.[28] One of these apps, Fengcai, downloads "all your text messages, contacts, call log history, calendar entries, and

---

[21] Australian Strategic Policy Institute, "Yitu," (last visited June 5, 2020), https://chinatechmap.aspi.org.au/#/company/yitu; Australian Strategic Policy Institute, "Megvii," (last visited June 5, 2020), https://chinatechmap.aspi.org.au/#/company/megvii; Danielle Cave et al., "Mapping more of China's tech giants: AI and surveillance," *Australian Strategic Policy Institute*, Nov. 28, 2019, https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

[22] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, Apr. 14, 2019.

[23] *Id.*

[24] Simon Denyer, "China's Watchful Eye," *The Washington Post*, Jan. 7, 2018.

[25] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, July 8, 2018.

[26] Sigal Samuel, "China is installing a secret surveillance app on tourists' phones," *Vox*, July 3, 2019, https://www.vox.com/future-perfect/2019/7/3/20681258/china-uighur-surveillance-app-tourist-phone; Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *The New York Times*, Feb. 21, 2019; Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 15 (May 2019); Phoebe Zhang, "China 'world's worst' for invasive use of biometric data," *South China Morning Post*, Dec. 5, 2019, https://www.scmp.com/news/china/society/article/3040710/china-worlds-worst-invasive-use-biometric-data.

[27] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 15 (May 2019).

[28] Sigal Samuel, "China is Installing a Secret Surveillance App on Tourists' Phones," *Vox*, July 3, 2019; Joseph Cox, "China Is Forcing Tourists to Install Text-Stealing Malware at its Border," *Vice*, July 2, 2019, https://www.vice.com/en_us/article/7xgame/at-chinese-border-tourists-forced-to-install-a-text-stealing-piece-of-malware.

installed apps…this sensitive data is then sent, unencrypted, to a local server."[29] Chinese authorities employ Wi-Fi sniffers, which collect unique identifying information of networked devices, like laptops and smartphones, and can be used to read people's emails.[30] Each of these new technologies and mechanisms, whether cutting-edge facial recognition software or a smartphone app, offers Chinese authorities useful information to help surveil the population. The consequences of China's accelerated development of technologies to strengthen the surveillance state are dire.

China's authoritarian use of surveillance technology is particularly pervasive and intrusive in Xinjiang autonomous region in northwest China. Xinjiang is home to 25 million people, of which approximately eleven million are Muslim Uyghurs.[31] In this region, China has deployed its surveillance apparatus on a massive scale in an effort to track the population living there.[32] While this apparatus affects everyone in Xinjiang, it has disproportionately targeted Uyghurs and other Muslim minorities. Chinese officials believe Uyghurs hold "extremist and separatist ideas."[33] China's targeting has led to extreme political and religious repression against these groups.[34]

Since 2014, China has promulgated an extensive surveillance ecosystem throughout Xinjiang as part of its "Strike Hard Campaign against Violent Terrorism."[35] China has placed a large amount of surveillance equipment along streets and neighborhoods, including at checkpoints in major metropolitan zones. Chinese authorities use them primarily to monitor Uyghurs.[36] By combining the cameras with facial recognition technology, Chinese authorities can increasingly track Uyghur activity down to the individual level.

Omnipresent monitoring has essentially stifled Uyghur freedom of movement in the region and eliminated any semblance of personal privacy. Simple activities, such as an individual tracked by a camera traversing farther than 300 meters from designated safe areas (often designated as an

---

[29] Sigal Samuel, "China is Installing a Secret Surveillance App on Tourists' Phones," *Vox*, July 3, 2019.
[30] Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018; Human Rights Watch, "Big Data Fuels Crackdown in Minority Region," February 26, 2018, https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.
[31] Michael Hardy, "In Xinjiang, Tourism Erodes the Last Traces of Uyghur Culture," *Wired*, Apr. 4, 2020, https://www.wired.com/story/xinjiang-uyghur-culture-tourism/; Bryan Wood & Brennan Butler, "What is happening with the Uighurs in China," *PBS News Hour*, Oct. 4, 2019.
[32] Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," *Council on Foreign Relations*, updated June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang; U.S. Department of State, "2018 Report on International Religious Freedom: China: Xinjiang," May 23, 2019, https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/ (last visited July 10, 2020); Sheena Chestnut Greitens et al., "Understanding China's 'preventive repression' in Xinjiang," *The Brookings Institution*, Mar. 4, 2020.
[33] Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," *Council on Foreign Relations*, updated June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang.
[34] *Id.;* U.S. Department of State, "2018 Report on International Religious Freedom: China: Xinjiang," May 23, 2019, https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/ (last visited July 10, 2020); Sheena Chestnut Greitens et al., "Understanding China's 'preventive repression' in Xinjiang," *The Brookings Institution*, Mar. 4, 2020.
[35] Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018; Jérôme Doyon, "Counter Extremism in Xinjiang: Understanding China's Community-Focused Counter-Terrorism Tactics," *War on the Rocks*, Jan. 14, 2019, https://warontherocks.com/2019/01/counter-extremism-in-xinjiang-understanding-chinas-community-focused-counter-terrorism-tactics/; Maya Wang et al., *"Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims*, Human Rights Watch, at 4 (Sept. 2018).
[36] Chris Buckley et al., "How China Turned a City into a Prison," *The New York Times*, Apr. 4, 2019; Ben Westcott, "Chinese government loads surveillance app onto phones of visitors to Xinjiang: report," *CNN*, July 3, 2019.

individual's home or workplace) triggers an alert to police of the individual's movement.[37] At key transit checkpoints, Chinese authorities use face scans to determine whether Uyghurs can travel by cross-referencing the photo taken at a checkpoint to internal databases.[38]

Surveillance also negatively affects Uyghurs' ability to practice their faith freely. The *Agence France-Presse* found that, in 2018, Hikvision won a contract for its cameras to watch 967 mosques in Xinjiang's Moyu county alone, and that authorities use these cameras to "ensure that imams stick to a 'unified' government script."[39]

In addition to video surveillance, Uyghurs must accept other repressive controls that impinge on their basic human rights in order to not run afoul of authorities. From 2016 to 2017, Uyghurs were tricked into providing biometric data to authorities as part of a misleading government health program in Xinjiang labeled "Physicals for All."[40] Tahir Imin, a Muslim who participated in the health check, underscored the repressive nature of the supposed health screenings, saying that authorities told him he did not have the right to ask about the test results after they drew his blood, scanned his face, recorded his voice, and took his fingerprints.[41] The forced acquisition of Mr. Imin's physical and genetic data underlines China's desire to scoop new data from those living in Xinjiang and file it for future use.

Chinese public security authorities also vigorously monitor telecommunications devices used by Uyghurs. Various news outlets report that the Chinese government mandates Uyghurs install an application on electronic devices that allows the government to surveil their online activities, a fundamental intrusion on online privacy.[42] The application, called JingWang, is specifically "built with no safeguards in place to protect the private, personally identifying information of its users" and capable of scanning and sending information stored on a device to a remote server.[43] While Chinese authorities state that the purpose of the application is to detect what authorities deem to be illegal terroristic or religious material, Sophie Richardson, the China Director of Human Rights Watch, rightly asserts that the application is simply a new technical mechanism for gathering vast quantities of data on people.[44] The total effect of these systems is a repressive, authoritarian regime

---

[37] Adile Ablet & Alim Seytoff, "Authorities Testing Facial-Recognition Systems in Uyghur Dominated Xinjiang Region," *Radio Free Asia*, Jan. 25, 2018.
[38] Darren Byler, "I researched Uighur society in China for 8 years and watched how technology opened new opportunities – then became a trap," *The Conversation*, Sept. 18, 2019, https://theconversation.com/i-researched-uighur-society-in-china-for-8-years-and-watched-how-technology-opened-new-opportunities-then-became-a-trap-119615; Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times*, Apr. 14, 2019.
[39] Ben Dooley, "Chinese Firms Cash in on Xinjiang's Growing Police State," *Agence France-Presse*, June 27, 2018.
[40] Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *The New York Times*, Feb. 21, 2019.
[41] *Id.*
[42] Joseph Cox, "Chinese Government Forces Residents To Install Surveillance App With Awful Security," *Vice*, Apr. 9, 2018, https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang.
[43] *Id.*
[44] Joseph Cox, "Chinese Government Forces Residents To Install Surveillance App With Awful Security," *Vice*, Apr. 9, 2019, https://www.vice.com/en_us/article/ne94dg/jingwang-app-no-encryption-china-force-install-urumqi-xinjiang; Yi Shu Ng, "China forces its Muslim minority to install spyware on their phones," *Mashable*, July 21, 2017, https://mashable.com/2017/07/21/china-spyware-xinjiang/#p2_q.Fw.DOqd.

designed to deprive Uyghurs and other ethnic minorities of their rights, turning cities such as Urumqi and Kashgar into veritable prison cities.[45]

The various elements of the surveillance apparatus in Xinjiang on their own provide important data to Chinese authorities, **but it is the centralization and rapid recall of the collected data that gives the authoritarian system increasing control and power.** This ability exists thanks in large part to the digital nature of the surveillance system, in which masses of data about individuals in Xinjiang are collected into central databases and rendered quickly retrievable by authorities, allowing them to uncover supposedly concerning behavior or respond swiftly to a situation.

China uses this digital process in Xinjiang, with police accessing information located on centralized servers from a mobile application.[46] The Integrated Joint Operations Platform (IJOP) is a central system developed by a subsidiary of China Electronics Technology Group Corporation (CETC), a major state-owned defense technology company in China. It integrates information from different "sources or machine sensors," such as video surveillance cameras or stolen Internet data, into "a massive dataset of personal information, and of police behavior and movements in Xinjiang."[47]

The centralized IJOP database syncs with the IJOP app, which authorities can access on a mobile device.[48] IJOP subsequently analyzes the data, although it is important to note that the level in which big data analytics plays a role in dissecting the data is unknown, and uses them to identify and predict patterns of behavior and, when necessary, notify police of people whom the data system categorizes as requiring investigation or even detention.[49] The IJOP app is the mechanism authorities use to communicate with the central information system and supplements the information going into the IJOP system, providing what Human Rights Watch (HRW) China Senior Researcher Maya Wang describes as "three broad functions: [the app] collects data, reports on suspicious activities or circumstances, and prompts investigative missions."[50] The IJOP sends alerts to police or government authorities to investigate suspicious activity, and through the app, authorities can send new information back to the IJOP, providing even more data to the system.[51] It

---

[45] *See* Chris Buckley et al., "How China Turned a City into a Prison," *The New York Times*, Apr. 4, 2019; Josh Chin & Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal*, Dec. 19, 2017.

[46] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 21 (May 2019); Human Rights Watch, "How Mass Surveillance Works in Xinjiang, China," May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang#:~:text=The%20Human%20Rights%20Watch%20report,of%20its%20%E2%80%9CStrike%20Hard%20Campaign (last visited July 10, 2020).

[47] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 20 (May 2019).

[48] Human Rights Watch, "How Mass Surveillance Works in Xinjiang, China," May 2, 2019, https://www.hrw.org/video-photos/interactive/2019/05/02/china-how-mass-surveillance-works-xinjiang#:~:text=The%20Human%20Rights%20Watch%20report,of%20its%20%E2%80%9CStrike%20Hard%20Campaign (last visited July 10, 2020).

[49] Maya Wang, *China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App*, Human Rights Watch, at 1, 19, 21, 22, 29 (May 2019).

[50] Nazish Dholakia, Media Desk Officer, Human Rights Watch, Interview with Maya Wang, "Interview: China's 'Big Brother' App," *Human Rights Watch*, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app.

[51] Nazish Dholakia & Maya Wang, "Interview: China's 'Big Brother' App - Unprecedented View into Mass Surveillance of Xinjiang's Muslims," *Human Rights Watch*, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app.

is through this cyclical, data-driven process that authorities in Xinjiang can truly implement digital authoritarianism in the region, as the sheer amount of information collected by authorities and the ability to understand that information in detail offer the Chinese government "the possibility of real-time, all-encompassing surveillance" that flouts basic human rights to privacy.[52]

The surveillance system in Xinjiang has aided in the detention of possibly more than 2 million Uyghurs, ethnic Kazakhs, and members of other Muslim groups in Xinjiang, according to the U.S. State Department.[53] Chinese officials have labeled these detention facilities as "vocational skills training centers" to "deradicalize" those suspected of extremism.[54] However, these centers are little more than arbitrary prison camps designed for political indoctrination. Uyghurs and other ethnic minorities imprisoned in internment camps are subject to abuse, squalid and unsanitary living conditions, lack of sleep and food, and forced political indoctrination.[55] In her account to *CNN*, Sayragul Sauytbay, a former employee at one of the detention facilities in Xinjiang who fled to Kazakhstan, recalls a CCP official telling her the primary objective of the detention system was to "turn the best of them [Uyghurs and other minorities] into Hans, while repressing and destroying the bad."[56] Sauytbay further describes that she suspected numerous human rights abuses, including sexual violence against female inmates and injections for non-compliant individuals.[57] Child separation due to forced detentions or exile is also a regular occurrence. Researcher Adrian Zenz highlights this separation process, writing that "[a]ccounts of Xinjiang Turkic Muslims in exile, including former detainees and their relatives, indicated that children as young as 2 years, with both parents in either internment or exile, were put into state welfare institutions or kept full-time in educational boarding facilities."[58] These accounts underline how China's surveillance state in Xinjiang abets the CCP's overt attempts to forcefully assimilate its ethnic minority populations into complying with the authoritarian government model proffered by Beijing.

While the authoritarian nature of the Chinese government's operations—especially against Uyghurs—in Xinjiang is alarming by itself, a second disturbing trend is the fact that China is supporting the development and use of technologies that conduct surveillance along racial and ethnic lines. Experts cited by the *New York Times* described China's usage of facial recognition to track Uyghurs as "the first known example of a government intentionally using artificial intelligence

---

[52] Nazish Dholakia & Maya Wang, "Interview: China's 'Big Brother' App - Unprecedented View into Mass Surveillance of Xinjiang's Muslims," *Human Rights Watch*, May 1, 2019, https://www.hrw.org/news/2019/05/01/interview-chinas-big-brother-app; United Nations, *UN Declaration of Human Rights*, *United* Nations, 3rd Session, (Dec. 10, 1948), https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf. Article 12 of the UN Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.*

[53] U.S. Department of State, "2018 Report on International Religious Freedom: China: Xinjiang," May 23, 2019. https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/ (last visited July 10, 2020).

[54] Eva Dou, "China Acknowledges Re-Education Centers for Uighurs," *The Wall Street Journal,* Oct. 10, 2018.

[55] Matt Rivers & Lily Lee, "Former Xinjiang Teacher Claims Brainwashing and Abuse Inside Mass Detention Centers," *CNN*, May 9, 2019.

[56] *Id.*

[57] *Id.*

[58] Adrian Zenz, "Break Their Roots: Evidence for China's Parent-Child Separation Campaign in Xinjiang," *The Journal of Political Risk, Vol. 7, No. 7* (July 2019), http://www.jpolrisk.com/break-their-roots-evidence-for-chinas-parent-child-separation-campaign-in-xinjiang/.

for racial profiling."[59] China accomplishes racial classification by instructing facial recognition AI to categorize individuals based on social definitions of race or ethnicity.[60] While Beijing argues that sorting individuals via race or ethnicity is necessary to combat terrorism or quell "ethnic violence" in Xinjiang, China's use of emerging technologies and big data for racial profiling sets a terrifying precedent for how to effectively repress vulnerable populations and serves as a potential model for other authoritarians around the globe.[61]

In Xinjiang, Chinese government and police authorities retain what amounts to near absolute control of the entire ICT domain, and, through that control, have been able to repress and subjugate Uyghurs and other ethnic minorities in the region. It is important to note that, while all of China experiences some form of surveillance due to the CCP's authoritarian principles, the severity of controls in Xinjiang are not yet fully present throughout the rest of China. However, Xinjiang is the proving ground for China's digital authoritarianism model, and it serves as a clear example of how the CCP plans to use the digital domain to maintain and strengthen its authoritarian hold over the entire country. This plan may start to come into focus as early as 2020, as the Chinese government begins to implement a unified Social Credit System that captures all 1.4 billion citizens.[62]

China's Social Credit System is an intrusive tool used by all levels of the Chinese government to regulate corporate and citizen behavior. Various entities at the local or city level, such as police departments or health bureaus, gather swaths of behavioral information and data on individuals.[63] This data, which can range from jaywalking to donating blood, is then submitted to local databases.[64] Relevant information collected on individuals is also sent to the national level via the National Credit Information Sharing Platform (NCISP), in which the central government maintains a master database that other state agencies can access.[65] With this information on hand and a whole-of-government approach, the Social Credit System allows China to more robustly manage individual behavior and punish those deemed problematic by placing them on blacklists or no-fly lists.[66] Although presented in a more sanitized manner to entire Chinese populace, the Social Credit System opens up greater opportunities for the Chinese government to oppress all citizens in a manner similar to what the people in Xinjiang face, and the rapidity with which the government is moving forward in implementing these new authoritarian models of surveillance shows how important the issue is to the CCP.

### *The Censorship Apparatus: Exploiting and Blocking Digital Content*

China's burgeoning surveillance state offers CCP authorities the ability to observe and maintain social control over its citizens and represents a fundamental component of its digital

---

[59] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *The New York Times,* Apr. 14, 2019.
[60] *Id.*
[61] *Id.*
[62] Interview of Georgette Kerr, Vice President of Plurus Strategies, Aug. 16, 2019; World Bank, "China" https://data.worldbank.org/country/china (last visited Apr. 28, 2020).
[63] Kendra Schaefer & Ether Yin, *Understanding China's Social Credit System*, Trivium China, at 24 (Sept. 23, 2019), http://socialcredit.triviumchina.com/wp-content/uploads/2019/09/Understanding-Chinas-Social-Credit-System-Trivium-China-20190923.pdf.
[64] *Id.*
[65] *Id.* at 3, 24.
[66] *Id.*

authoritarianism model. A second, equally identifiable aspect of China's internal digital authoritarianism is the CCP's efforts at controlling flows of data. The CCP has spent decades building tools, mechanisms, and the infrastructure needed to cultivate a system for direct control of the content accessed by those in China. China's control over content has stunted political movements and silenced public criticism domestically by stifling access to a free Internet and tailoring CCP propaganda so that it efficiently targets the Chinese population.[67]

One of the fundamental fears of China's leadership when Internet access first arose in China in the 1990s was the technology's potential to introduce uncontrolled sources of information that could undermine CCP control by providing Chinese citizens with greater access to uncensored information and easier, more rapid communication.[68] To combat the possibility of the Internet operating as a democratizing force in China, China's Ministry of Public Security initiated the Golden Shield Project and debuted it in 2000.[69] Also known as the Great Firewall, it is central to the CCP's censorship efforts and uses a set of Internet traffic screening tools to filter out websites and content deemed inappropriate for China's Internet.[70] These tools span technical mechanisms, such as DNS poisoning, blocking the use of virtual private networks (VPN), and blocking IP addresses, to more human-based oversight, including monitors employed by the Ministry of Public Security.[71] Since its inception, the Great Firewall in China has developed into a complex censorship apparatus, essentially creating an entirely separate version of the Internet.[72]

More recently, Chinese companies have begun implementing emerging technologies, such as AI, to strengthen these censorship capabilities further through the automation of its monitoring and censorship processes.[73] China has also developed a culture of self-censorship.[74] The Chinese government requires Chinese firms to self-regulate content on their servers and platforms. For example, the *New York Times* noted in 2010 that major technology companies such as Baidu "employ throngs of so-called Web administrators to screen their search engines, chat rooms, blogs and other

---

[67] *See, e.g.,* Michael Anti, "Behind the Great Firewall of China," *TedGlobal2012* (video), *TED*, June 2012, https://www.ted.com/talks/michael_anti_behind_the_great_firewall_of_china/transcript?language=en#t-128890; Kenneth Roth, "China's Global Threat to Human Rights," *Human Rights Watch Global Report*, 2020.

[68] *See, e.g.,* Ping Punyakumpol, "The Great Firewall of China: Background," *Torfox* (A Stanford Project), *Stanford University*, June 1, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html; Nina Hachigian, "China's Cyber-Strategy," Foreign Affairs (Mar./Apr. 2001).

[69] Ping Punyakumpol, "The Great Firewall of China: Background," *Torfox* (A Stanford Project), *Stanford University*, June 1, 2011.

[70] *Id.*

[71] Oliver Farnan et al., "Poisoning the Well – Exploring the Great Firewall's Poisoned DNS Responses," *WPES '16: Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, Oct. 2016, at 95, https://dl.acm.org/doi/pdf/10.1145/2994620.2994636; Cate Cadell, "Amid VPN crackdown, China eyes upgrades to Great Firewall," *Reuters*, July 20, 2017; Robert McMahon & Isabella Bennett, "U.S. Internet Providers and the 'Great Firewall of China,'" *Council on Foreign Relations*, Feb. 23, 2011; Marty Hu, "The Great Firewall: a technical perspective," Torfox (A Stanford Project), *Stanford* University, May 30, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/martyhu/index.html.

[72] *See, e.g.,* "China Media Bulletin: 2019 internet freedom trends, Shutterstock censorship, Huawei "safe cities" (No. 140)," *Freedom House*, https://freedomhouse.org/report/china-media-bulletin/2020/china-media-bulletin-2019-internet-freedom-trends-shutterstock (last visited July 10, 2020).

[73] Yuan Yang, "Artificial intelligence takes jobs from Chinese web censors," *Financial Times*, May 22, 2018.

[74] Ping Punyakumpol, "The Great Firewall of China: Background," *Torfox* (A Stanford Project), *Stanford University*, June 1, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html

content for material that flouts propaganda directives."[75] A Chinese state media report said in 2013 that the government then employed approximately two million civilians who monitor social media and other Internet traffic to prevent social unrest and criticism of the government.[76]

The consequences of China's government enforcing tight censorship include (1) a population that is unaware of, or unable to acquire, accurate information about its government's policies and actions; and (2) continued consolidation of CCP rule. The Great Firewall has blocked digital news media content created by major international outlets not approved by the CCP.[77] According to Freedom House's analysis of Chinese censorship directives, China heavily censors news ranging from health and safety to "taboo subjects" such as the Cultural Revolution and Tiananmen Square.[78] Freedom House states that censorship against international news outlets is so prevalent that:

> Many international news outlets, especially those with Chinese-language websites, are blocked. For example, the *New York Times*, *Reuters*, and the *Wall Street Journal* have been censored for years, while the websites of the *Washington Post* and the *Guardian* were newly blocked in June 2019, likely as part of the government's efforts to tighten its grip on the flow of information surrounding the 30th anniversary of the Tiananmen Square crackdown.[79]

This censorship has aided the CCP's efforts to ensure that those living in China only receive information approved by the Party, a fundamental aspect of maintaining its status in China's public domain.

U.S. social media platforms such as Facebook, Instagram, Twitter, WhatsApp, Pinterest, and YouTube have also been blocked entirely from China's servers.[80] While censorship of these platforms has had the intended effect of barring many of those living in China from accessing information that would be deemed offensive to the Party, this censorship has also generated a second critical outcome. **Foreign technology platforms are restricted from operating in China, allowing Chinese platforms that offer similar services to thrive and expand into new markets.[81] Thanks to this market inefficiency, China now retains some of the most valuable Internet companies in the world by market capitalization, including Alibaba, Tencent, and Baidu.**[82] These companies essentially provide the panoply of Internet services wanted in China.

---

[75] Michael Wines et al., "China's Censors Tackle and Trip Over the Internet," *The New York Times*, Apr. 7, 2010.
[76] Katie Hunt & CY Xu, "China 'employs 2 million to police internet,'" *CNN,* Oct. 7, 2013; Google Translate: "Internet public opinion analyst: It's note about deleting posts," *Beijing News*, Oct. 3, 2013, http://epaper.bjnews.com.cn/html/2013-10/03/content_469152.htm?div=-1.
[77] Gerry Shih, "China adds Washington Post, Guardian to 'Great Firewall' blacklist," *The Washington Post*, June 8, 2019.
[78] "Freedom on the Net 2019: China," *Freedom House*, https://freedomhouse.org/country/china/freedom-net/2019 (last visited May 15, 2020); Sarah Cook, "The News China Didn't Want Reported in 2017," *The Diplomat*, Jan. 27, 2018.
[79] "Freedom on the Net 2019: China," *Freedom House*, https://freedomhouse.org/country/china/freedom-net/2019 (last visited May 15, 2020); Gerry Shih, "China adds Washington Post, Guardian to 'Great Firewall' blacklist," *The Washington Post*, June 8, 2019.
[80] "Freedom on the Net 2019: China," *Freedom House*, https://freedomhouse.org/country/china/freedom-net/2019 (last accessed May 15, 2020); Sherisse Pham, "China adds Pinterest to list of banned sites," *CNN*, Mar. 17, 2017; GreatFire.Org, "Censorship of Alexa Top 1000 Domains in China," https://en.greatfire.org/search/alexa-top-1000-domains (last visited June 26, 2020).
[81] *See, e.g.,* Tim Wu, "China's Online Censorship Stifles Trade, Too," *The New York Times*, Feb. 4, 2019.
[82] J. Clement, "Market value of the largest internet companies worldwide 2019," *Statista*, June 3, 2020, https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/; Tim Wu,

Alibaba offers e-commerce services, and Tencent delivers social media, entertainment, and gaming, negating the need for other platforms where information flows freely.[83] The consequences of this are a Chinese population that is reliant on platforms that further cement the CCP's control of the digital domain.

China's censorship extends beyond simply separating China's Internet from outside information. China's censors are using offensive tools and aggressive tactics that reach far beyond scrubbing and blocking data to ensure robust censorship. Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, asserts that the Chinese government used an attack tool, which they label the "Great Cannon," to extend the reach of China's censorship.[84] The Great Cannon, while co-located within the Great Firewall, is a "separate offensive system" that "hijacks traffic to (or presumably from) individual IP addresses, and can *arbitrarily replace unencrypted content as a man-in-the-middle*."[85] China used the Great Cannon to conduct Distributed Denial of Service (DDoS) attacks on servers rented by GreatFire.org, an advocacy nonprofit that challenges China's Great Firewall, and GitHub pages run by GreatFire.org in 2015.[86]

China's use of an offensive cyber tool for censorship purposes is revelatory because it shows China taking action beyond its borders to ensure censorship within its borders. China is also cracking down on tools that ordinary Chinese citizens use to overcome the Great Firewall, such as virtual private networks.[87] In January 2019, the *Financial Times* showed how China is cracking down on individual use of VPN tools. The *Financial Times* highlighted how a Chinese man, Zhu Yunfeng, received a significant fine for accessing foreign websites and using the VPN Lantern, as well as how another individual, Pan Xidian, received a jail sentence for VPN use and composing "inappropriate" Twitter posts.[88] Providers of these tools are receiving even stiffer sentences, such as Wu Xiangyang, who in 2017 received a five and a half year jail sentence and 500,000 yuan fine (approximately $70,650) for selling software that circumvented China's Internet censorship controls.[89] The result of these efforts is a censorship system that can rely on a variety of continually evolving tools to ensure that online and social media users can be targeted if they post comments that the government and Party deem politically sensitive. Everyday citizens consequently retain fewer avenues to acquire non-CCP approved information.

---

"China's Online Censorship Stifles Trade, Too," *The New York Times*, Feb. 4, 2019; Simon Denyer, "China's Scary Lesson to the World: Censoring the Internet Works," *The Washington Post*, May 23, 2016.

[83] Australian Strategic Policy Institute, "Tencent," https://chinatechmap.aspi.org.au/#/company/tencent (last visited June 5, 2020); Australian Strategic Policy Institute, "Alibaba," https://chinatechmap.aspi.org.au/#/company/alibaba (last visited June 5, 2020).

[84] Bill Marczak et al., *China's Great Cannon*, The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto (Apr. 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/.

[85] *Id.*

[86] *Id.*

[87] Cisco, "What Is a VPN? - Virtual Private Network," https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (last visited June 7, 2019). A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. *Id.*

[88] Yuan Yang, "China Turns Up Heat on Individual Users of Foreign Websites," *Financial Times*, Jan. 7, 2019.

[89] Benjamin Haas, "Man in China Sentenced to Five Years' Jail for Running VPN," *The Guardian*, Dec. 21, 2017.

### *The Legal System: China's Implementation of Authoritarian Cyber Laws*

In a position paper titled "China's Digital Rise – Challenges for Europe," authors Kristin Shi-Kupfer and Mareike Ohlberg of the Mercator Institute for China Studies note that, when developing new technologies, an unofficial Chinese government slogan is "first develop, then regulate."[90] This unofficial slogan demonstrates that the government has prioritized the maturation of its emerging digital technologies and then, as they are integrated into society, regulates their use as needed. With China's continued rise in this domain, the Chinese government now is increasingly implementing stringent rules and regulations to ensure that the cyber domain remains compliant with Party strictures. The regulations China has implemented recently expand government control over cyberspace at the legal level, making its myriad authoritarian actions to quell dissent and promote Chinese propaganda seem lawful.

In November 2016, the 24th Session of the Standing Committee of the 12th National People's Congress passed the Cybersecurity Law of the People's Republic of China, fundamentally altering the cyber landscape in China.[91] Coming into effect on June 1, 2017, and enforced by the Cyberspace Administration of China (CAC) and other related ministries, the law affords government entities broad authority to regulate and control the digital environment in China.[92] In addition to the Cybersecurity Law, the Chinese government is layering various regulations on top of it to give the law both more clarity and teeth.[93]

While the Cybersecurity Law and relevant additional regulations put forth a variety of new stipulations on individuals and companies, there are a few provisions of the law and related regulations that are especially emblematic of China's effort at increasing social and political control of the digital domain. One of these is the repeated vague references in the Cybersecurity Law to national security needs, opening individuals and organizations to intrusive and potentially abusive reviews of cyber activity.[94] According to Georgette Kerr, a cyber-expert at Plurus Strategies, "the law and associated directives have compelled network operators to cooperate with law enforcement in addressing vaguely defined threats to national security [and] established intrusive national security reviews," seen in clauses such as Article 28.[95] Article 28 states that "network operators shall provide technical support and assistance to public security organs and national security organs that are

---

[90] Kristin Shi-Kupfer & Mareike Ohlberg, *China's Digital Rise: Challenges for Europe,* Mercator Institute for China Studies, Vol. 7, at 9 (Apr. 2019), https://www.merics.org/sites/default/files/2019-04/MPOC_No.7_ChinasDigitalRise_web_3.pdf.

[91] IT Advisory KPMG China, "Overview of China's Cybersecurity Law," *KPMG*, Feb. 2017, at 4, https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf; Samuel Stolton, "Chinese cybersecurity law is a 'loaded weapon,' senior US official says," *Euractiv*, Feb. 27, 2019, https://www.euractiv.com/section/cybersecurity/news/chinese-cybersecurity-law-is-a-loaded-weapon-senior-us-official-says/.

[92] Interview of Georgette Kerr, Vice President of Plurus Strategies, Aug. 16, 2019; Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect," *Lawfare*, June 1, 2017, https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

[93] Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect," *Lawfare*, June 1, 2017, https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect; Samm Sacks et al., "China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chain, Foreign Control (Translation)," *New America*, May 24, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/.

[94] Interview of Georgette Kerr, Vice President of Plurus Strategies, Aug. 16, 2019.

[95] *Id.*

safeguarding national security and investigating criminal activities in accordance with the law."[96] **The law in effect uses national security as a legal mechanism to assert its authoritarian control over data flows in China in new ways.** The law additionally affords the government even more dystopian powers in special circumstances dictated by the State Council. Under Article 58 of the law, authorities can "take temporary measures regarding network communications in a specially designated region, such as limiting such communications," further underscoring how the 2017 law fully empowers the Chinese government to control the digital domain anytime the government claims such control is necessary.[97]

The implementation of the Cybersecurity Law also imposes serious controls and restrictions on foreign companies operating in China. Jack Wagner, an Asia analyst at PGI Intelligence writing in *The Diplomat*, notes that "several of the provisions… have become a cause for concern among foreign companies."[98] For example, Wagner highlights data localization rules in the law, under which foreign companies would need to store data on Chinese servers.[99] Due to data localization laws, firms would either need to "invest in new data servers in China which would be subject to government spot-checks, or incur new costs to hire a local server provider, such as Huawei, Tencent, or Alibaba, which have spent billions in recent years establishing domestic data centers as part of Beijing's 12th Five-Year Plan (2011-2015)."[100] Neither of these options are positive for companies looking to operate in China, as they open up sensitive information to intrusive snooping by Chinese authorities.

Another key issue stemming from China's burgeoning legal structures pertaining to the digital domain is the continued erosion of online anonymity. Samm Sacks and Paul Triolo, writing in *Lawfare*, describe how the CAC added four regulations in August and September of 2017 regarding online activity that effectively reduce online anonymity. These four regulations are 1) the Internet Forum Service Management Regulation, 2) the Internet Threat Comments Service Management Regulation, 3) the Internet User Public Account Information Services Management Regulation, and 4) the Management Rules of Internet Group Information Services.[101] The regulations disallow online anonymity by requiring "foreground voluntary name, background real name." This requirement means that users can choose a screen name or appear anonymous, but their actual identity information will still be stored with the Ministry of Public Security.[102] Sacks and Triolo note that, by reducing anonymity online, Chinese authorities receive more real data to add to their burgeoning databases on citizen behavior such as the Social Credit System, and by extension, further their oversight of the population.[103] Similarly, in November 2018, the government implemented new regulations granting "the Ministry of Public Security (MPS) broad powers over the computer networks of companies in China."[104] The rule, labeled "Regulations on Internet Security Supervision

---

[96] Rogier Creemers et al., "Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]," *New America*, June 29, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[97] *Id.*

[98] Jack Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat*, June 1, 2017.

[99] *Id.*

[100] *Id.*

[101] Samm Sacks & Paul Triolo, "Shrinking Anonymity in Chinese Cyberspace," *Lawfare*, Sept. 25, 2017, https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace.

[102] *Id.*

[103] *Id.*

[104] Insikt Group, "China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems," *Recorded Future*, Feb. 8, 2019, https://www.recordedfuture.com/china-cybersecurity-measures/.

and Inspection by Public Security Organs," provides MPS with new opportunities to conduct on site and remote site inspections of company computers, copy user information, have police backup during inspections to ensure company compliance, and monitor company adherence to censorship laws.[105]

Although the Chinese government may be reacting to some valid cybersecurity concerns in building and growing the legal frameworks surrounding cyber activity, it is no accident that this framework simultaneously provides legitimacy to China's authoritarian actions in the digital domain. As seen above, the various laws and regulations implemented by the Chinese government provide censors, law enforcement, intelligence agencies, and other entities with legal cover to impinge on privacy rights and conduct undue searches and seizures of information contained or passed in cyberspace. **The ramifications of the promulgation of China's digital laws include the establishment of an Internet governance framework that ensures, at the most fundamental level, CCP regime survival and operates as a direct contrast to the systems and laws promulgated by the U.S. and its allies.**

### *China's Investment in Technologies Predicated on Authoritarian Principles*

China's growing promotion of digital authoritarianism has coincided with its rise as a technological leader. These technologies, as demonstrated above, make surveillance and censorship both easier and stronger than ever before for CCP authorities. **As such, the rise of digital authoritarianism in China is facilitated by the continued development of new technologies consistent with authoritarian principles.** Consequently, the CCP continues to emphasize investment and innovation in new technologies, which will further strengthen its ability to exercise authoritarian rule in China.[106]

China's focus on investing in cyber and digital technologies comes from the highest echelons of CCP leadership, who have advocated new technologies as critical to China's rise as a global power. The Made in China 2025 initiative was a state-led industrial policy intended "to make China dominant in global high-tech manufacturing" by using "government subsidies, mobiliz[ing] state-owned enterprises, and pursu[ing] intellectual property acquisition to catch up with—and then surpass—Western technological prowess in advanced industries."[107] The policy prioritizes ten major sectors, of which one is new information technology.[108] Made in China 2025 operated as a ten-year plan driving China's industrial development, and its prioritization of the technologies within the digital domain accentuates the CCP's desire to strengthen Chinese-made ICT products and services. Additionally, China's Internet Plus policy, also unveiled in 2015, "aims to capitalize on China's huge

---

[105] *Id.*

[106] *See, e.g.,* Sophia Yan, "Chinese surveillance grows stronger with technology that can recognise people from how they walk," *Telegraph*, Nov. 6, 2018; Statement of William Carter, Deputy Director and Fellow, Technology Policy Program, *Chinese Advances in Emerging Technologies and their Implications for U.S. National Security*, Hearing before the U.S. House of Representatives Armed Services Committee, Jan. 9, 2018, at 2, 6.

[107] James McBride & Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" *Council on Foreign Relations,* May 13, 2019. *See also* Emily Crawford, "Made in China 2025: The Industrial Plan that China Doesn't Want Anyone Talking About," *PBS*, May 7, 2019.

[108] Press Release, State Council of the People's Republic of China, "Made in China 2025," May 19, 2015, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

online consumer market by building up the country's domestic mobile Internet, cloud computing, massive amounts of data (big data), and the Internet of Things sectors."[109]

CCP leaders have also delivered statements further backing China's emphasis on developing its cyber capabilities. General Secretary Xi, in an October 9, 2016 Politburo meeting on cyber and IT issues, asserted that China "must accelerate the advancement of domestic production, indigenous and controllable substitution plans, and the building of secure and controllable information technology systems."[110] Wang Huning, a member of the Standing Committee of the Politburo, relayed Xi's stance on information technology development in December 2017, saying "[CCP] General Secretary Xi Jinping emphasized the need to…deepen Internet and information technology, build a cyber superpower, and advance society through a digital China; and to advance Internet, big data, artificial intelligence, and data economy, etc."[111]

In addition to highlighting China's desire to strengthen information technologies, CCP leaders' statements often denote the need for sanitizing cyberspace from what the Party believes to be toxic content. Chen Yixin, the Secretary-General of the CCP's Legal Affairs Commission, highlighted this priority in January 2019, stating that a "small incident can form into a vortex of public opinion" on the Internet.[112] Zhuang Rongwen, Vice Minister of the Central Propaganda Department, and Director of the Central Cybersecurity and Informatization Office and State Internet Information Office, provided additional context to China's desire to control the digital domain in September 2018 with the assertion that:

> The Internet has become a main battlefield, main battleground, and most forward position in propaganda and public opinion work. To grasp leadership authority in online ideological work, we must not only give full rein to the main force role of Party members, cadres, and mainstream media editors, pushing the main forces onto the main battlefield; we must also give full rein to the dominant role of the majority of Internet users, and fight a people's war for the governance of the online environment.[113]

**To CCP leadership, the digital domain is a space that must be controlled by the Party. As such, development of new digitally enabled technologies must operate in line with Party**

---

[109] Meia Nouwens & Helena Legarda, *Emerging technology dominance: what China's pursuit of advanced dual-use technologies means for the future of Europe's economy and defence innovation*, China Security Project at MERICS and The International Institute for Strategic Studies, at 5 (Dec. 2018); Press Release, State Council of the People's Republic of China, "China unveils Internet Plus action plan to fuel growth," July 4, 2015, http://english.www.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm.

[110] Michael Martina, "Xi Says China Must Speed Up Plans for Domestic Network Technology," *Reuters*, Oct. 9, 2016. *See also* "The Political Bureau of the Central Committee of the Communist Party of China Conducted the 36th Collective Study on the Implementation of the Cyber Power Strategy," *Xinhua News Agency*, Oct. 9, 2016, http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm (translated from Chinese).

[111] Graham Webster et al., "Wang Huning's Speech at the 4th World Internet Conference in Wuzhen," *New America*, Dec. 13, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/wang-hunings-speech-4th-world-internet-conference-wuzhen/.

[112] Chris Buckley, "2019 Is a Sensitive Year for China. Xi is Nervous," *The New York Times*, Feb. 25, 2019.

[113] Rogier Creemers et al., "Translation: China's New Top Internet Official Lays Out Agenda for Party Control Online," *New America*, Sept. 24, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/.

**principles. Without such control, CCP leaders fear these technologies could weaken the CCP's hold over its citizens.**

The CCP has implemented industrial policies with massive investments in technology and lucrative conditions for Chinese firms operating in digital fields. China's research and development spending grew by more than 17% each year from 2010 to 2017 and in 2018 hit a record high of 2.19 percent of GDP.[114]

These investments have only continued to accelerate. China has spent incredible amounts of resources bolstering startups working in the surveillance field. The *New York Times* reported that, in May 2018, "the upstart A.I. company SenseTime raised $620 million, giving it a valuation of about $4.5 billion. Yitu raised $200 million [in June 2018]. Another rival, Megvii, raised $460 million from investors that included a state-backed fund created by China's top leadership."[115] The European Union Chamber of Commerce in China, in its "China Manufacturing 2025" report, tells a similar story of how China is boosting its domestic telecommunications industry. The report notes that:

> The Chinese Government has used a variety of policy instruments to support the development of its domestic telecommunications equipment industry. One of the most prominent has been the use of catalogues of domestic high-technology products, as well as an equivalent list for exports. Firms whose products are included in these catalogues receive benefits, such as preferential tax rates and low-interest loans from state-owned banks.[116]

China's firms have found that operating in zones that promulgate digital authoritarianism in China is an extremely profitable business. In Xinjiang, Hikvision received approximately $290 million for security related contracts, including a "social prevention and control system" and a program implementing facial-recognition surveillance in and around mosques.[117] Combined with Dahua's own contracts in Xinjiang, Hikvision and Dahua have won "at least $1.2 billion in government contracts for 11 separate, large-scale surveillance projects across Xinjiang."[118] The fact that Chinese firms are receiving such strong returns for working in fields that fundamentally promote authoritarian rule in China highlight Chinese leadership's willingness to invest in technologies that enable greater social and digital control.

China's leadership firmly believes that the country is on a path towards becoming a global power capable of exerting influence practically anywhere, and that a core aspect of achieving this goal is

---

[114] "China's spending on R&D rises to historic high," *Xinhua* News, Sept. 7, 2019, http://www.xinhuanet.com/english/2019-09/07/c_138373248.htm; Niall McCarthy, "China Is Closing The Gap With The U.S. In R&D Expenditure," *Forbes*, Jan. 20, 2020; Zhang Jun, "Will China Be the Next Tech Powerhouse? Maybe with the Next 20 Years of Sustained Investment," *South China Morning Post*, Aug. 1, 2018, https://www.scmp.com/comment/insight-opinion/united-states/article/2157728/will-china-be-next-tech-powerhouse-maybe-next.

[115] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, July 8, 2018.

[116] *China Manufacturing 2025*, European Union Chamber of Commerce in China, at 26 (2017), http://docs.dpaq.de/12007-european_chamber_cm2025-en.pdf.

[117] Ben Dooley, "Chinese Firms Cash in on Xinjiang's Growing Police State," *Agence France-Presse*, June 27, 2018. *See also* Chris Buckley & Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York Times*, May 22, 2019.

[118] Charles Rollet, "In China's Far West, Companies Cash in on Surveillance Program that Targets Muslims," *Foreign Policy*, June 13, 2018.

dominance in the digital domain. For China's government, this dominance starts at home, and its current policies and investments underscore the CCP's focus on strengthening the domestic base for information technologies.

## Chapter 2: Exporting Digital Authoritarianism – China on the Global Cyber Stage

China's leadership is increasingly confident that its governing model for the digital space represents the future of the domain and is doing its best to convince governments around the world that this is the case. Digital authoritarianism in China is enabling the CCP to impose considerable control over its population and the information accessible to those in the country, providing the regime with increased security from democratizing forces and further opportunities for economic and technological growth. As China continues to perfect the tools that comprise its model of digital authoritarianism, its leaders have become more aware of the geopolitical and economic benefits of exporting both the technologies and the methods of digital authoritarianism to perpetuate its model of extensive censorship and automated surveillance.[119]

Chinese leaders are using information and communications technology (ICT) and digital media to increase their power abroad as well as at home, including by building on the Belt and Road Initiative's (BRI) infrastructure, trade, training, and investment links between China and more than 60 other countries.[120] At the first BRI forum in May 2017, Chinese President Xi Jinping announced that China would integrate big data into the multi-billion dollar BRI enterprise to create the "digital silk road of the 21st century."[121] China has also begun to install fiber optic networks across the globe, setting the stage to assert its presence in the ICT sector and facilitate the export of digital authoritarianism.[122]

When examining China's digital efforts abroad, a subtle yet important distinction between China's fundamentally economic activities and its more subversive and damaging endeavors that aid in the expansion of digital authoritarianism must be made. While China's attempts to gain a larger market in the digital domain and to outcompete the United States in certain technological spaces represent a significant concern for U.S. economic interests, those efforts within a free international market do not necessarily represent a national security concern. What does raise critical national security concerns is when China's digital efforts erode democratic values and enable the rise of digital authoritarianism around the world. At best, China is selling digital technology that has remarkable capacity for surveillance and control to authoritarian or authoritarian-leaning countries with no second thought for the consequences. At worst, China is pairing its economic investment with aggressive outreach and training on Internet governance and domestic regulations to further inculcate authoritarian values and methods of social control.

---

[119] Adrian Shahbaz, *Freedom of the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[120] Andrew Chatzky & James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, last updated Jan. 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative; Adrian Shahbaz, *Freedom of the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

[121] Xi Jinping, CCP General Secretary, Remarks at "Work Together to Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road," Beijing, May 14, 2017; Andrew Chatzky & James McBride, "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, last updated Jan. 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[122] Adrian Shahbaz, *Freedom of the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Susan Crawford, "China Will Likely Corner the 5G Market—and the US Has No Plan," *Wired*, Feb. 20, 2019.

### *Exporting Technologies and Expanding Digital Authoritarianism*

The Digital Silk Road announcement only formalized efforts already underway by China to expand into foreign markets. For example, in 2015, China's third-largest telecom company, China Telecom Group (CTG), announced the creation of its Africa and Middle East headquarters, having already expanded its network capabilities in the UAE, South Africa, Kenya, Egypt, and Nigeria.[123] It planned to continue growing its network through deals with local companies such as the Wananchi Group, East Africa's leading telecommunications operator.[124]

The CTG announcement marks just one of the steps China and Chinese businesses have taken to extend into the developing world, efforts met with increasing success. Not only has China been willing to go into smaller, under-served markets, Chinese companies have been able to offer more cost-effective equipment than Western companies, as well as financial support that comes directly from the Chinese government.[125] According to Mark Natkin, founder and managing director of the Beijing-based consultancy Marbridge, Chinese telecom vendors "identified opportunities in developing nations" where they could "leverage their price advantage to develop relationships that vendors from rich countries [couldn't] be bothered with."[126] He goes on to describe China's approach as a long-term strategy based on building the core network and banking on the likelihood that doing so gives its companies a foothold to win follow-on contracts for upgrades and expansions.[127]

Huawei, the subject of many headlines during the past few years, is a prime example. In 1996, the Chinese government gave Huawei the status of "national champion" and ensured it would have easy access to financing and high levels of government subsidies—$222 million in government grants in 2018.[128] Government support has enabled Huawei to offer prices for its network equipment that are below other companies' prices, allowing Huawei to quickly gain market advantage. In the Netherlands, for example, Huawei undercut its competitor, the Swedish firm Ericsson, by underbidding for a contract to provide network equipment for the Dutch national 5G network by 60 percent.[129] Two industry officials who spoke to *The Washington Post* on the condition of anonymity held that Huawei's price was so low that, absent the subsidies the company had been provided,

---

[123] Rudradeep Biswas, "Global: China Telecom Global Expands Footprint in Africa and Middle East," *Telecom Talk*, June 9, 2015, https://telecomtalk.info/global-china-telecom-global-expands-in-africa-and-middle-east/137520/.
[124] *Id.*; "CTG Signs Deal with Wananchi Group for Major Fiber Infrastructure Construction Project," *China Telecom Group*, Mar. 18, 2015, https://www.chinatelecomglobal.com/data/file/2016/20160509171658535.pdf.
[125] Executive Research Associates, *China in Africa: A Strategic Overview,* at 51 (Oct. 2009), https://www.ide.go.jp/library/English/Data/Africa_file/Manualreport/pdf/china_all.pdf
[126] Marbridge Consulting, "Management," https://www.marbridgeconsulting.com/management.html (last visited June 1, 2020); Executive Research Associates, *China in Africa: A Strategic Overview*, at 50 (Oct. 2009).
[127] Executive Research Associates, *China in Africa: A Strategic Overview,* at 50 (Oct. 2009).
[128] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; Ellen Nakashima, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," *The Washington Post*, May 29, 2019; Jeffrey Melnik, "China's 'National Champions' Alibaba, Tencent, and Huawei," *Education About Asia*, Vol. 24, Fall 2019, https://www.asianstudies.org/wp-content/uploads/chinas-national-champions-alibaba-tencent-and-huawei.pdf.
[129] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; Ellen Nakashima, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," *The Washington Post*, May 29, 2019.

Huawei would have been unable to even produce the necessary network parts.[130] Some countries also receive low-interest loans from Chinese state-owned banks to use Huawei equipment.[131]

The result has been near-complete dominance in some regions. For example, in Africa Huawei has built about 70 percent of the 4G networks, and in cases such as Zambia, it is developing the country's entire telecommunications infrastructure.[132] More broadly, Chinese technology now serves as the "backbone of network infrastructure" in several African countries, and Chinese firms like Huawei, ZTE, and China Telecom are the major players in erecting the infrastructure needed for next generation technologies across the African continent.[133] In Kenya alone, Huawei has built more than 3,500 mobile base stations (the antennas that receive and transmit radio frequencies which make mobile communications possible) and installed 4,000 kilometers of fiber optic cable.[134]

Today, Huawei operates in more than 170 countries and is the second-largest smartphone seller in the world, just behind Samsung, but ahead of Apple.[135] Robert Atkinson, President of the Information Technology and Innovation Foundation (ITIF), a U.S. think tank, states that Huawei's research and development investments surpass any other company worldwide.[136] Beyond consumer electronics, Huawei offers telecommunications equipment and cloud services.[137] Furthermore, Huawei owns more patents for 5G infrastructure than any of its competitors.[138]

Huawei's investments in research and development have positioned it to build the next-generation 5G infrastructure in Africa, Asia, and Latin America. Alarmingly, even governments close to the

---

[130] Ellen Nakashima, "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible," *The Washington Post*, May 29, 2019.
[131] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019.
[132] Amy Mackinnon, "For Africa, Chinese-Built Internet Is Better Than No Internet at All," *Foreign Policy*, Mar. 19, 2019; Wesley Rahn, "Will China's 5G 'Digital Silk Road' Lead to an Authoritarian Future for the Internet?," *DW*, Apr. 26, 2019.
[133] Chiponda Chimbelu, "Investing in Africa's tech infrastructure. Has China won already?," *DW*, May 3, 2019.
[134] Huawei, *Huawei Kenya Sustainability Report 2018*, (2018), at 8, https://www.huawei.com/minisite/explore-kenya/pdf/huawei_kenya_csd_report_v2.pdf; "Huawei Kenya launches first Sustainability Report Highlighting Efforts to Expand Broadband Nationwide and Solutions to Drive Kenya's Digital Transformation," Huawei, Sept. 7, 2019, https://www.huawei.com/ke/press-events/news/ke/2019/huawei-kenya-launches-first-sustainability-report; Ericsson, "Base stations and networks," https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/responsible-business/radio-waves-and-health/base-stations-and-networks (last visited June 30, 2020). As a note, there are different numbers provided regarding the number of mobile base stations built by Huawei from these two citations. The 2018 report states that the number of stations built is 3,500, while the press release gives the number 3,5000. This report assumes that the number 3,5000 is a typographical error and uses the number of 3,500.
[135] Huawei, "About Huawei," https://www.huawei.com/us/about-huawei (last visited June 1, 2020); Jusy Hong, "Global smartphone shipments fall for seventh consecutive quarter in Q2, even with limited impact from US Huawei ban," *Informa*, Aug. 5, 2019, https://technology.informa.com/616273/global-smartphone-shipments-fall-for-seventh-consecutive-quarter-in-q2-even-with-limited-impact-from-us-huawei-ban; Counterpoint, "Global Smartphone Market Share: By Quarter," https://www.counterpointresearch.com/global-smartphone-share/ (last visited June 30, 2020).
[136] Wesley Rahn, "Will China's 5G 'Digital Silk Road' Lead to an Authoritarian Future for the Internet?," *DW*, Apr. 26, 2019; Information Technology & Innovation Foundation, "Robert D. Atkinson," https://itif.org/person/robert-d-atkinson (last visited June 1, 2020).
[137] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; Huawei, "About Huawei Cloud," https://www.huaweicloud.com/en-us/about/about_us.html (last visited June 30, 2020).
[138] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019; *Who is leading the 5G patent race*, IPlytics, at 4 and 5 (Nov. 2019), https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf.

United States are weighing whether to integrate Huawei technologies into their infrastructure despite security concerns. For example, the ruling party of Germany in early 2020 backed a position paper that pushed for more stringent regulation of foreign technologies in its 5G networks but did not ban the use of Huawei components.[139] Furthermore, Germany's three primary telecommunications firms, while deciding to remove Huawei from its core networks, will continue to utilize Huawei technologies on peripheral radio access networks.[140] Brazil, another U.S. partner, faces an upcoming decision on whether Huawei should be further involved in Brazil's infrastructure as Brazil prepares to auction spectrum for 5G in late 2020.[141] In July 2019, Brazil's Vice President Hamilton Mourao told reporters that the country would not restrict Huawei on 5G, extending a decade-long relationship.[142] In an example of that relationship, Huawei supports an Internet of Things laboratory in São Paulo state and is looking to build a smartphone assembly plant.[143] While security concerns have been raised by Eduardo Bolsonaro, a lawmaker and son of Brazil's president, it remains to be seen how Brazil manages Huawei's involvement in its domestic 5G moving forward, especially in light of Foreign Minister Ernesto Araujo reportedly arguing for a Huawei 5G ban to President Bolsonaro.[144] Meanwhile, Mexico and Argentina plan to start Latin America's first 5G networks in 2020 and are considering allowing Huawei participation.[145]

Huawei's 5G push continues to see success in other countries, especially ones in China's Belt and Road Initiative, highlighting the company's ability to dominate the 5G space by providing networks for prices estimated to be 30 percent less than its competitors.[146] For example:

- Malaysia is not barring Huawei from spectrum bids relating to its 5G rollout, saying that security decisions will be made by its "own safety standards";[147]
- In Thailand, Huawei offered to build a tech training center in Bangkok as a means of enticing Thailand to allow Huawei to build its 5G network;[148]
- In Italy, Huawei offered to provide cloud computing services that would link Italian hospitals both with each other and with hospitals in Wuhan in response to the COVID-19 pandemic;[149]

---

[139] Andreas Rinke, "Merkel's conservatives stop short of Huawei 5G ban in Germany," *Reuters*, Feb. 11, 2020.
[140] Douglas Busvine & Thomas Seythal, "Telefonica Deutschland picks Ericsson for 5G core network," *Reuters*, June 2, 2020.
[141] Anthony Boadle, "Huawei role in Brazil 5G up to national security chief: regulator," *Reuters*, Feb. 18, 2020.
[142] "Defying US, Brazil Allows Huawei to Move Forward with 5G Network," *Al Jazeera*, July 15, 2019.
[143] Oliver Stuenkel, "Huawei Heads South: The Battle over 5G Comes to Latin America," *Foreign Affairs*, May 10, 2019.
[144] Anthony Boadle, "Huawei role in Brazil 5G up to national security chief: regulator," *Reuters*, Feb. 18, 2020; Eduardo Baptista, "China-Brazil trade on track, but Huawei tension may be threat to relations," *South China Morning Post*, June 21, 2020, https://www.scmp.com/news/china/article/3089903/china-brazil-trade-track-huawei-tension-may-be-threat-relations.
[145] Oliver Stuenkel, "Huawei Heads South: The Battle over 5G Comes to Latin America," *Foreign Affairs*, May 10, 2019; Andres Schipani et al., "Latin America resists US pressure to exclude Huawei," *Financial Times*, June 9, 2019.
[146] Lindsay Maizland & Andrew Chatzky, "Huawei: China's Controversial Tech Giant," *Council on Foreign Relations*, June 12, 2019.
[147] Joseph Sipalan & Krishna N. Das, "Malaysia to choose 5G partners based on own security standards," *Reuters*, Feb. 17, 2020.
[148] Apornrath Phoonphongphiphat, "Huawei sweetens 5G offer in Thailand with tech training center," *Nikkei Asian Review*, November 18, 2019, https://asia.nikkei.com/Spotlight/5G-networks/Huawei-sweetens-5G-offer-in-Thailand-with-tech-training-center;
Takashi Kawakami, "China closes in on 70% of world's 5G subscribers," *Nikkei Asian Review*, May 12, 2020, https://asia.nikkei.com/Spotlight/5G-networks/China-closes-in-on-70-of-world-s-5G-subscribers.
[149] Theresa Fallon, "China, Italy, and Coronavirus: Geopolitics and Propaganda," *The Diplomat*, Mar. 20, 2020.

- Unnamed sources reported in March 2020 that as part of its 5G rollout, France's cybersecurity agency, ANSSI, will allow Huawei equipment to be used for non-core elements of France's network;[150]
- Russia is building out its 5G network with Huawei's help;[151]
- *The Washington Post* reported that Huawei is building out North Korea's wireless network.[152] Huawei stated that it does not have a business presence in North Korea, but did not dispute the reporting done by *The Washington Post*;[153]
- Even some small U.S. rural telecom companies have used Huawei equipment.[154]

By building out so much of the digital infrastructure in the developing world, China could end up dominating a large portion of the global communications market, positioning it to potentially pressure other governments or conduct espionage.[155] Indeed, multiple governments that purchase or rely on Chinese technologies also enact tough restraints on free speech or engage in illiberal activities, such as spying on political opponents, and there have been suspicious data transfers from Chinese-built IT systems.[156] For example, in 2017, technicians working at the African Union headquarters in Addis Ababa, Ethiopia, discovered that servers in the building, built by a Chinese company with Chinese funding, had for years been transmitting massive quantities of data to China, making even the most sensitive material vulnerable to Chinese exploitation.[157] Despite these incidents and diplomatic warnings, however, many countries—both developing and developed—calculate that access to low-cost, good-quality data networks and hardware outweighs the potential risks.

As noted above, China's export and infrastructure efforts around the globe represent an economic concern for the United States. However, China's export of digital technology in and of itself is not the key issue, as it is only the groundwork upon which digital authoritarianism can flourish. What really advances this censorship and surveillance system is China providing countries with social control systems that run on exported digital technologies, including relevant training and expertise.

---

[150] Mathieu Rosemain & Gwénaëlle Barzic, "Exclusive: France to allow some Huawei gear in its 5G network – sources," *Reuters*, Mar. 12, 2020.
[151] Zak Doffman, "Huawei Just Launched 5G In Russia With Putin's Support: 'Hello Splinternet'," *Forbes*, Sept. 1, 2019.
[152] Ellen Nakashima et al., "Leaked documents reveal Huawei's secret operations to build North Korea's wireless network," *The Washington Post*, July 22, 2019; Emily Stewart, "A New Reason to Worry About Huawei: It's Been Building North Korea's Wireless Networks," *Vox*, July 22, 2019, https://www.vox.com/recode/2019/7/22/20704196/huawei-north-korea-washington-post-sanctions-panda.
[153] Ellen Nakashima et al., "Leaked documents reveal Huawei's secret operations to build North Korea's wireless network," *The Washington Post*, July 22, 2019.
[154] Jeanne Whalen, "Huawei helped bring Internet to small-town America. Now its equipment has to go," *The Washington Post*, Oct. 10, 2019.
[155] See, e.g., Zak Doffman, "CIA Claims It Has Proof Huawei Has Been Funded By China's Military and Intelligence," *Forbes*, Apr. 20, 2019; Isobel Asher Hamilton, "Researchers Studied 25,000 Leaked Huawei Resumes and Found Troubling Links to the Government and Spies," *Business Insider*, July 8, 2019, https://www.businessinsider.com/huawei-study-finds-connections-between-staff-and-chinese-intelligence-2019-7.
[156] Steven Feldstein, "When it Comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge," *War on the Rocks*, Feb. 12, 2020, https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/; Josh Chin, "The Internet, Divided Between the U.S. and China, Has Become a Battleground," *The Wall Street Journal*, Feb. 9, 2019.
[157] Joan Tilouine & Ghalia Kadiri, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin," *Le Monde*, Jan. 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html; Mailyn Fidler, "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts," *Council on Foreign Relations*, Mar. 7, 2018.

In its report, *Freedom on the Net 2018*, Freedom House highlights how, during 2018, the Chinese government hosted media officials from dozens of countries for seminars on its system of censorship and surveillance.[158] Outside experts have little visibility into the details of these trainings, but governments who participate frequently return home to pass cybersecurity laws very similar to those in China.[159] Furthermore, Chinese companies have supplied many governments—at least some of which have poor human rights records or a tendency towards autocracy—with advanced facial recognition technology and data analytics tools that can be easily exploited by repressive governments and intelligence services.[160] For example:

- The Chinese startup CloudWalk is partnering with the Zimbabwean government on a mass facial recognition program in Zimbabwe;[161]
- Huawei is advising Kenya on its information and communication technology (ICT) Master Plan and Vision 2030;[162]
- In Mauritius, Huawei is installing 4,000 cameras;[163]
- Zambia is spending $1 billion on Chinese-made telecommunications, broadcasting, and surveillance technology;[164]
- Chinese start-up Yitu bid for a contract for facial recognition cameras in Singapore and opened its first international office in Singapore in January 2019.[165]

These examples highlight a few Chinese efforts to expand digital authoritarianism. To more fully show how China's approach of economic advancement and authoritarian outreach is extending digital authoritarianism to new countries, this report delves into four case studies that underscore China's efforts to not only provide technologies to other nations, but also to work with these countries to perfect methods of social control that imitate China's own patterns of digital authoritarianism.

### *Case Study: Venezuela*

The regime of disputed Venezuelan president Nicolas Maduro takes full advantage of Chinese hardware and services in its effort to control Venezuelan citizens. Venezuela has Internet and

---

158 Adrian Shahbaz, *Freedom on the Net 2018: The Rise of Digital Authoritarianism*, Freedom House (Oct. 31, 2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

159 *Id.*. Vietnam, Uganda, and Tanzania all introduced cybersecurity laws resembling China's following such seminars. *Id. See Also* Abdi Latif Dahir, "China is Exporting its Digital Surveillance Methods to African Countries," *Quartz Africa*, Nov. 1, 2018; Josh Chin, "The Internet, Divided Between the U.S. and China, Has Become a Battleground," *The Wall Street* Journal, Feb. 9, 2019.

160 Daniel Benaim and Hollie Russon Gilman, "China's Aggressive Surveillance Technology Will Spread Beyond Its Borders," *Slate*, Aug. 9, 2018.

161 Shan Jie, "China exports facial ID technology to Zimbabwe," *Global Times*, Apr. 12, 2018, http://www.globaltimes.cn/content/1097747.shtml; Abdi Latif Dahir, "China is Exporting its Digital Surveillance Methods to African Countries," *Quartz Africa*, Nov. 1, 2018.

162 Abdi Latif Dahir, "China is Exporting its Digital Surveillance Methods to African Countries," *Quartz Africa*, Nov. 1, 2018; Huawei, "Kenya," https://www.huawei.com/us/about-huawei/sustainability/win-win-development/social-contribution/seeds-for-the-future/kenya (last visited June 7, 2020).

163 Sheridan Prasso, "China's Digital Silk Road is Looking More Like an Iron Curtain, *Bloomberg,* Jan. 10, 2019.

164 *Id.*

165 Anna Gross et al., "Chinese tech groups shaping UN facial recognition standards," *Financial Times*, Dec. 1, 2019; Amanda Lentino, "This Chinese facial recognition start-up can identify a person in seconds," *CNBC*, May 16, 2019.

mobile networking equipment, intelligent monitoring systems, and facial recognition technology developed and installed by Chinese companies, and regime officials have traveled to China to participate in seminars on information management.[166] The regime uses these technologies to censor and control its critics by blocking social media platforms and political content, using pro-regime commentators to manipulate online discussions, stifling content critical of Maduro, increasing surveillance of citizens, tracking and detaining government critics, and accessing the data of human rights organizations.[167]

ZTE helped the regime create Venezuela's *Carnet de la Patria* (Fatherland Card). Critics have labeled the card as a new option for the Maduro regime to exert increased social control over its population (such as determining who receives subsidized food or health services), especially against those the regime considers political opponents.[168] The initial idea began more than a decade ago as a standardized ID for voting or opening a bank account.[169] However, as Venezuela's economic and political crisis deepened, the regime used it to track *Comités Locales de Abastecimiento y Producción* (Local Committees for Supply and Production, or CLAP) boxes, the subsidized food packages the government began distributing in 2016.[170] ZTE in 2017 also received an undisclosed portion of $70 million to build out a centralized database and mobile payment system for the card in an effort to bolster "national security."[171] By late 2018, a team of ZTE employees was embedded in a special unit of Venezuela's state telecommunications company that oversees the management of the database.[172] According to employees of the entity that manages the card system, the database stores birthdays, family information, employment and income, property owned, medical history, state benefits received, presence on social media, political party membership, and voting records.[173] To encourage people to sign up for the card, the Maduro regime has granted "cash prizes to cardholders for performing civic duties, like rallying voters."[174] However, the regime also made it mandatory for anyone wanting to receive public benefits such as medicine, subsidized fuel, and pensions.[175] Once the card became the way to sign up for much-needed services, its adoption was generally assured, and the Maduro regime claims that over half of the population retains a Fatherland Card.[176]

---

[166] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018; Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[167] "Venezuela / Protests: UN and IACHR Rapporteurs condemn censorship, arrests and attacks on journalists," *UN Human Rights – Office of the High Commissioner*, Apr. 26, 2017, https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21535&LangID=E; Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018; "Freedom on the Net 2019: Venezuela," *Freedom House*, https://freedomhouse.org/country/venezuela/freedom-net/2019 (last visited July 10, 2020); Moises Rendon & Arianna Kohan, "The Internet: Venezuela's Lifeline," *Center for Strategic and International Studies*, Dec. 4, 2019.
[168] Laura Vidal, "Venezuelans fear 'Fatherland Card' may be a new form of social control," *The World*, Dec. 28, 2018, https://www.pri.org/stories/2018-12-28/venezuelans-fear-fatherland-card-may-be-new-form-social-control.
[169] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018.
[170] Jim Wyss & Cody Weddle, "Venezuela's Maduro aims to turn empty stomachs into full ballot boxes," *Miami Herald*, May 16, 2018. *See also* Press Release, U.S. Department of Treasury, "Treasury Disrupts Corruption Network Stealing From Venezuela's Food Distribution Program, CLAP," July 25, 2019.
[171] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018.
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*; Jim Wyss & Cody Weddle, "Venezuela's Maduro aims to turn empty stomachs into full ballot boxes," *Miami Herald*, May 16, 2018.

Using information gathered through enrollment and card transactions, the regime is creating and growing a database that could be a powerful tool for identifying, harassing, and silencing Maudro's critics. Current and former employees of Cantv, Venezuela's state telephone and Internet provider, told *Reuters* that the card still only records if a person voted—not how they voted—but there is evidence that government agencies are tracking whether government employees are voting.[177] ZTE is also supporting the Maduro regime by taking on projects that government-owned enterprises can no longer manage. As of 2015, ZTE was helping build six emergency response centers monitoring Venezuela's major cities, and since 2016 it has been working to centralize the government's video surveillance.[178]

### *Case Study: Central Asia*

In April 2019, the Uzbek government signed a $1 billion deal with Huawei to expand surveillance operations in the country.[179] At the time, the capital city of Tashkent had 883 cameras that authorities used to record and analyze movements while automatically reporting road violations such as speeding.[180] Under the new agreement, Huawei will upgrade the cameras to "digitally manage political affairs."[181] Similarly, Huawei aided the implementation of Tajikistan's "safe city" project in Dushanbe in 2013, providing $22 million (primarily a $20.91 million loan) for the installation of cameras along roads and overseeing monuments and parks.[182] China also owns TK mobile, one of the five telecommunications providers in Tajikistan, and Huawei is the main technology supplier for Kyrgyzstan's top telecommunication providers.[183] Although the Kyrgyz government withdrew from Huawei's $60 million "safe cities" project in March 2018, it later chose a Russian company, Vega, to implement the first phase of a similar traffic monitoring system in November 2018.[184]

### *Case Study: Ecuador*

The Ecuador example illustrates how, even if democratic institutions prevail, vestiges of China's influence persist. Former Ecuadorian President Rafael Correa, the autocratic leftist and ally of former Venezuelan President Hugo Chavez, left office in 2017 but the surveillance system he installed remains in use.[185] Correa learned of China's surveillance technology after Ecuadorian

---

[177] Angus Berwick, "How ZTE Helps Venezuela Create China-Style Social Control," *Reuters Investigates*, Nov. 14, 2018.
[178] *Id.*
[179] "Huawei and CITIC Guoan invest over US$1 billion to develop Uzbekistan's digital infrastructure," *Xiangshi Xinwen Wang* (*Detailed News)* via *Silu Xin Guancha (Silk Road New Observer)*, Apr. 26, 2019, http://web.siluxgc.com/UZ/20190426/16656.html (translated from Chinese); Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019.
[180] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019.
[181] *Id.*
[182] *Id.*; Liu Ruowei, "Millions of Roads, Safety First: The Central Asian 'Safe City' project is here!," *Silu Xin Guangcha (Silk Road New Observer)* on WeChat, Feb. 13, 2019, https://mp.weixin.qq.com/s/z3l_UHX40W8OIJi61HaomA (translated from Chinese).
[183] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019; "Announcement on providing guarantee for holding subsidiaries," *ZTE Corporation*, May 11, 2019, https://www.zte.com.cn/mi_imgs/global/investor_relations/349268/P020120917408589110191.pdf.
[184] Yau Tsz Yan, "Smart Cities or Surveillance? Huawei in Central Asia," *The Diplomat*, Aug. 7, 2019; "The Kyrgyz government suddenly announced the termination of the "smart city" project, China's Huawei has not yet responded," *Kabar*, Mar. 18, 2015, http://cn.kabar.kg/news/2-8/ (translated from Chinese); "Vega successfully completes first round of Safe City program in Bishkek," *Vega*, May 20, 2019, https://www.vega.su/press-room/?ELEMENT_ID=2216 (translated from Russian).
[185] "Ecuador 'rejects unlimited election terms', blocking Correa return," *BBC*, Feb. 5, 2018.

officials visiting Beijing for the 2008 Olympics received a tour of Beijing's surveillance system.[186] Three years later, the Ecuadorian government began installing a system of high-powered cameras throughout the country for the stated purpose of reducing crime.[187] This system sends images to 16 monitoring centers that employ more than 3,000 people.[188] China guaranteed state funding and loans for the project, and in return, Ecuador committed to exporting "large portions of its oil reserves" to China, underscoring another key point: China's utilization of predatory lending and technological knowledge to receive other benefits.[189]

Two Chinese companies, Huawei and China National Electronics Import & Export Corporation (CEIEC), primarily built Ecuador's surveillance system.[190] In addition to recording events, the monitoring system offers Ecuadorian authorities the ability to track phones and, according to the *New York Times*, may be equipped with facial-recognition capabilities in the future.[191] As part of the process of fully integrating these technologies into Ecuador's infrastructure, China engaged in a training operation in which Ecuadorian officials visited China and Chinese engineers educated Ecuadorian engineers on how to manage the system.[192] The Ecuador project created a toehold in the region: Ecuador's decision to install the equipment prompted the Venezuelan and Bolivian governments to follow suit, and soon after, Venezuela installed a larger version that aimed to include 30,000 cameras.[193]

Although Correa's successor, President Lenin Moreno, has worked to reverse many of Correa's autocratic policies, the surveillance system is still operational and holds the potential for abuse. When *New York Times* reporters had the opportunity to see in person the 800-camera operation in Quito, there were only 30 police officers available to check camera footage, and anecdotal reports suggest crimes continue to take place in plain view of cameras.[194] Moreover, the recordings are also available to Ecuador's domestic intelligence agency, the National Intelligence Secretariat (SENAIN), which has a history of harassing and tracking political opponents.[195] Indeed, given the small number of police available to monitor crime-prone locations, the system is probably better suited to spying on individuals than fending off criminality.

### *Case Study: Zimbabwe*

China is also leveraging the deployment of surveillance technology overseas to improve its products' functionality. Studies have shown that facial recognition systems developed in Western nations tend

---

[186] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[187] *Id.*
[188] *Id.*
[189] *Id.*; Clifford Krauss & Keith Bradsher, "China's Global Ambitions, Cash and Strings Attached," *The New York Times*, July 24, 2015.
[190] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[191] *Id.*
[192] *Id.*
[193] *Id.*; "Venezuela will replicate the Ecuadorian model of the Integrated Security System Ecu-911," *National Service for Risk and Emergency Management of Ecuador*, Dec. 25, 2013, https://www.gestionderiesgos.gob.ec/venezuela-replicara-modelo-ecuatoriano-del-sistema-integrado-de-seguridad-ecu-911/.
[194] Paul Mozur et al., "Made in China, Exported to the World: The Surveillance State," *The New York Times*, Apr. 24, 2019.
[195] *Id.*

to perform better on Caucasian faces and those developed in East Asian nations tend to perform better on their respective populations.[196] While Western technology companies are grappling with how to teach machines about race, their Chinese counterparts are using their customer base in Africa to help develop advanced capabilities that differentiate by race.[197] For example, in March 2018, the Zimbabwean government agreed to a partnership to develop facial recognition programs in the country with CloudWalk Technology, a startup located in Guangzhou.[198] Additionally, Zimbabwe entered into a Memorandum of Understanding with Hikvision in which the Chinese company would donate facial recognition cameras and software for use at border posts, airports, and state entry points in Zimbabwe.[199] Partnerships such as these provide Chinese companies with the opportunity to develop and refine their databases with different ethnicities and demographics, in Zimbabwe's case a majority-Black population, while enticing the country with technological modernization.[200] A key consequence of such partnerships, according to *Quartz* reporter Lynsey Chutel, is Chinese companies "getting ahead of US and European developers" on facial recognition.[201]

### *A Global Challenge*

The situations described above are key examples of how China is using economic and, more importantly, geopolitical and outreach tools to stimulate the growth of digital authoritarianism in new markets and nations. Although most China tech-watchers agree that the use of Chinese surveillance and censorship systems around the world is growing, they differ on how many are in use, and, given the proliferation of Chinese-built telecommunications equipment, how widely their use may ultimately reach. According to Steven Feldstein, former Deputy Assistant Secretary of State at the Bureau for Democracy, Human Rights, and Labor, "Huawei alone is responsible for providing AI [artificial intelligence] surveillance technology to at least fifty countries worldwide."[202] When Huawei's efforts are combined with Hikvision, Dahua, and ZTE's efforts, Chinese companies supply AI surveillance technology in sixty-three countries, thirty-six of which are part of BRI.[203] Experts are still trying to assess the long-term consequences of China's technological expansion; Feldstein also notes that China is exporting AI-equipped surveillance technology to governments ranging from closed authoritarian systems to flawed democracies.[204] In an article on the proliferation of Chinese-made surveillance systems, *Foreign Policy* cites a Huawei study, which has been removed

---

[196] P. Jonathon Phillips et al., *An Other-Race Effect for Face Recognition Algorithms*, Association for Computing Machinery (Feb. 2011), https://dl.acm.org/doi/10.1145/1870076.1870082; Steve Lohr, "Facial Recognition is Accurate, if You're a White Guy," *The New York Times*, Feb. 9, 2018; Clare Garvie & Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," *The Atlantic*, Apr. 7, 2016.

[197] Lynsey Chutel, "China is Exporting Facial Recognition Software to Africa, Expanding its Vast Database," *Quartz Africa*, May 25, 2018.

[198] *Id.*; Zhang Hongpei, "Chinese Facial ID Tech to Land in Africa," *Global Times*, May 17, 2018, http://www.globaltimes.cn/content/1102797.shtml; Shan Jie, "China exports facial ID technology to Zimbabwe," *Global Times*, April 12, 2018, http://www.globaltimes.cn/content/1097747.shtml.

[199] Farai Mudzingwa, "Government Acknowledges Facial Recognition System In The Works," *TechZim*, June 13, 2018, https://www.techzim.co.zw/2018/06/government-acknowledges-facial-recognition-system-in-the-works/.

[200] Lynsey Chutel, "China is Exporting Facial Recognition Software to Africa, Expanding its Vast Database," *Quartz Africa*, May 25, 2018.

[201] *Id.*

[202] Steven Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace*, Sept. 17, 2019.

[203] *Id.*.

[204] *Id.;* Steven Feldstein, "China is Exporting AI Surveillance Technology to Countries Around the World," *Newsweek*, Apr. 23, 2019.

from the company's website, in which "the company boasted that it had already deployed its 'Safe City' system in 230 cities around the world, for more than 90 national or regional governments."[205]

Due to China's efforts at proliferating the technologies and methodologies of digital authoritarianism, the United States finds itself in an intensifying battle over the global ICT sector. China's export of ICT infrastructure, its ability to deliver lower-priced, reliable access to telecommunications network technology, and its competitive edge in 5G combine to mount a strong challenge to the U.S. to become the biggest provider of 5G services to the world. Not only do these efforts provide China with a competitive edge both commercially and, in a potential conflict, militarily, they also offer even greater leverage to push client countries to adopt the Chinese approach to the Internet and the regulation of speech. Consequently, the United States must proactively defend a free, democratic model for the digital domain and Internet governance and push back against China's malign activities abroad.

However, it is not enough for the United States to take a purely defensive posture against China's digital authoritarianism. **It is critical that the United States government stimulate technological innovation in the United States by increasing government research and development funding, adopting a more extensive industrial policy, developing and attracting superior talent to the United States' technology sector, strengthening bilateral and multilateral technology initiatives with like-minded allies and partners, and ensuring a competitive advantage for domestic companies in overseas markets**. By doing so, the United States and its allies can open up more opportunities to create and deploy emerging technologies that can outcompete Chinese products and services and thereby undercut its ability to export digital authoritarianism. If the United States does not develop and implement an all-encompassing strategy for combatting China and its cyber efforts, the United States will cede the global cyber domain to our Pacific adversary and open up a future in which digital authoritarianism becomes the global norm, leaving the United States and its allies vulnerable and placing countless more individuals under the thumb of digital authoritarianism.

[205] Bojan Stojkovski, "Big Brother Comes to Belgrade," *Foreign Policy*, June 18, 2019.

## Chapter 3: Institutionalizing Digital Authoritarianism – China at International Fora

In addition to using heavily-subsidized technology to purchase political influence in countries around the world, China continues to use diplomacy and various international domains to further its authoritarian goals. Its objective: to set the rules and norms around the governance of digital technologies. From the United Nations (UN) to the World Trade Organization (WTO), China has used its political and economic muscle to shape the international standards surrounding the digital domain in favor of a more authoritarian view of the world.

Since General Secretary Xi came into power in 2012, the cyber realm has become an increasingly important strategic domain.[207] Adam Segal of the Council on Foreign Relations wrote that, since then, the CCP's goals have been threefold: "limit the threat that the Internet and the flow of information may pose to domestic stability and regime legitimacy; shape cyberspace to extend Beijing's political, military, and economic influence; and counter US advantages in cyberspace while increasing China's room to maneuver."[208]

According to a report prepared for the United States-China Economic and Security Review Commission in 2018, China uses:

> [A] comprehensive techno-nationalist strategy that coordinates Chinese efforts to gain leading roles in international standards organizations while also using state funding to allow Chinese companies to undersell their competitors in developed economies and win infrastructure contracts in developing markets, ensuring that its indigenously-developed technologies and standards become widely adopted with or without international recognition.[209]

Above all else, China is heavily focused on ensuring its digital sovereignty, as indicated by its presence as the second "principle" (following "peace" as the first) in their 2017 International Strategy of Cooperation on

*Definition - Digital Sovereignty*

At the Opening Ceremony of the International Workshop on Information and Cyber Security in June 2014, Vice Foreign Minister Li Baodang stated that sovereignty in cyberspace, which this report refers to as digital sovereignty, comprises the following factors: "states[']  own jurisdiction over the ICT infrastructure and activities within their territories; national governments are entitled to making public policies for the Internet based on their national conditions; no country shall use the Internet to interfere in other countries' internal affairs or undermine other countries' interests."[206]

---

[206] Press Release, Vice Foreign Minister Li Baodong, "Address by Vice Foreign Minister Li Baodong at the Opening Ceremony of the International Workshop on Information and Cyber Security," June 5, 2014, https://www.fmprc.gov.cn/mfa_eng/wjbxw/t1162458.shtml.

[207] *See, e.g.,* James A. Lewis & Simon Hansen, *China's Cyberpower – International and domestic priorities,* Australian Strategic Policy Institute, at 1 (Nov. 2014), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/SR74_China_cyberpower.pdf?R7nGofs8ZdT2nhDIb6NqAekikBTLuC9m.

[208] Adam Segal "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

[209]John Chen et al., *China's Internet of Things,* Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, by SOS International (SOSi), at 69 (Oct. 2018).

Cyberspace.[210] In the strategy, the Cyberspace Administration of China (CAC) and the Ministry of Foreign Affairs argues for digital sovereignty and states that "[n]o country should pursue cyber hegemony."[211] It appears, as evidenced by its efforts in a number of different international forums, that China's idea of not pursuing "cyber hegemony" applies to every country other than China.

### *The United Nations*

At the United Nations, China has played a counterproductive role in efforts to build consensus on a free and fair future of cyberspace. China's behavior echoes its consistent undermining of UN efforts that could highlight its own poor human rights record.[212]

In 2011, China—along with Russia, Tajikistan, and Uzbekistan—submitted a draft resolution on an international code of conduct for information security to the 2011 United Nations General Assembly.[213] The resolution, which was later enhanced and resubmitted in 2015 by a slightly larger group of Shanghai Cooperation Organization (SCO) member countries, emphasizes the sovereignty and stability of individual states within the digital space to the extent that it raises significant human rights concerns, detailed below.[214] The resolution explicitly says it aims to "push forward the international debate on international norms on information security, and help forge an early consensus on this issue."[215] In other words, the resolution is China's attempt to make itself the leader on these norms.

Both the 2011 and 2015 versions of the draft resolution commit the signatories to "curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic, and social stability, as well as their spiritual and cultural environment."[216] According to Milton Mueller of the Internet Governance Project at the Georgia Institute of Technology School of Public Policy, this section would:

> [G]ive any state the right to censor or block international communications for almost any reason. Such as…Facebook mobilizations against dictators, dissident blogs, etc.

---

[210] Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace – March 2017," Mar. 1, 2017, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

[211] *Id.*

[212] *See, e.g.,* Lindsay Maizland, "Is China Undermining Human Rights at the United Nations?" *Council on Foreign Relations*, July 9, 2019.

[213] Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (93), *U.N. General Assembly, 66th Session*, Sept. 14, 2011, https://undocs.org/A/66/359.

[214] Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91), *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723; *See, e.g.,* Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto*, Sept. 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[215] *Id.*

[216] Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (93), *U.N. General Assembly, 66th Session*, Sept. 14, 2011, https://undocs.org/A/66/359. *See also* Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91), *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723.

> "Undermining the spiritual and cultural environment" in particular could be used to filter out any views a government didn't like, and could even be used for trade protectionism in cultural industries.[217]

The significant revisions between the 2011 Code of Conduct and the 2015 Code of Conduct involve several references to a report by the 2012 UN Group of Governmental Experts (GGE), *Developments in the Field of Information and Telecommunications in the Context of International Security*.[218] The GGEs, which fall under the United Nations Office for Disarmament Affairs and consist of selected member states, have initiated six separate working groups since 2004 to "examine[] existing and potential threats in the cyber-sphere and possible cooperative measures to address them," with each group's work intended to build upon the last.[219]

The GGEs have been viewed as the best tool to achieve success—albeit incremental—at the UN on democratic digital standards.[220] However, contrary to that view, the report by the GGE established in 2012 was favorably referenced by the China-led SCO's Code of Conduct resolution several times in 2015.[221] According to Sarah McKune, Senior Legal Advisor at the Citizen Lab, SCO states looked favorably on that GGE's report because of the "recognition of sovereignty and territoriality in the digital space."[222] The SCO's newfound appreciation for the 2012-13 GGE in their resolution may have led to the increased disputes in a later GGE—the 2016-2017 GGE—that collapsed discussions and prevented the Group from issuing a consensus report at its conclusion.[223] Following the 2016-17

---

[217] Milton Mueller, "Russia & China propose UN General Assembly Resolution on 'information security,'" *Internet Governance Project – Georgia Tech University*, Sept. 20, 2011, https://www.internetgovernance.org/2011/09/20/russia-china-propose-un-general-assembly-resolution-on-information-security/.

[218] *See* Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (93), *U.N. General Assembly, 66th Session*, Sept. 14, 2011, https://undocs.org/A/66/359; Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91), *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723; U.N. General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – Note by the Secretary-General, 68th Session, Agenda item 94 (June. 24, 2013), https://undocs.org/A/68/98.

[219] United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security – December 2018," https://www.un.org/disarmament/ict-security/ (last visited July 15, 2020). *See also* United Nations Office for Disarmament Affairs (UNODA), "Fact Sheet: Developments In the Field of Information and Telecommunications in the Context of International Security," Jul. 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf.

[220] *See, e.g.,* John Sullivan, Deputy Secretary of State, Remarks at the "Second Ministerial Meeting on Advancing Responsible State Behavior in Cyberspace," New York, New York, Sept. 23, 2019.

[221] "Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the Secretary-General (91)" *U.N. General Assembly, 69th Session*, Jan. 13, 2015, https://undocs.org/A/69/723; *See, e.g.*. Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto*, Sept. 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[222] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," *The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto*, Sept. 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.

[223] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?," *The Diplomat,* July 21, 2017.

GGE dissipation, the United States led a resolution to authorize the creation of a new 2019-21 GGE, which continues to meet periodically and is expected to conclude in May 2021.[224]

In addition to the GGEs, China may find another short-term mechanism to push its agenda of digital authoritarianism in the Open-Ended Working Group (OEWG). In December 2018, the UN General Assembly adopted the formation of the Internet-focused OEWG that Russia proposed.[225] The OEWG was supposedly convened "with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent."[226] To some, the establishment of the OEWG could be an avenue whereby China, Russia, and their SCO allies can challenge the progress made by the GGEs and attempt to influence the United Nations in favor of their more authoritarian digital policies.[227]

### *World Trade Organization*

In addition to leveraging its global influence to shape international cyberspace guidelines at the UN, China also seeks to use its influence to subvert World Trade Organization regulations and norms on digital commerce. In contrast to the United States' focus on addressing digital trade issues, China appears unwilling to come to an agreement at the WTO over what digital trade agreements should look like, intending to halt decisions that, if enacted, could encroach on its domestic digital governance.[228] China prefers that data flows and data storage be subjects for exploratory discussions, rather than commitments.[229] Further, as Nigel Cory at the Information Technology and Innovation Foundation argued, "China's approach to digital trade is largely focused on applying existing WTO rules (which are increasingly irrelevant) and a few narrow, non-binding technical provisions."[230]

Most existing rules related to digital trade have not been updated since the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce in 1996, almost 25 years ago.[231] The Chinese government employs the current, broad rules to its advantage. One example of this is China's heavy emphasis on data localization, which governments

---

[224] United Nations, "Group of Government Experts," Dec. 2018, https://www.un.org/disarmament/group-of-governmental-experts/; Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *Council on Foreign Relations*, Nov. 15, 2018.

[225] Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," *Council on Foreign Relations*, Nov. 15, 2018; Elaine Korzak, "What's Ahead in the Cyber Norms Debate?," *Lawfare*, Mar. 16, 2020, https://www.lawfareblog.com/whats-ahead-cyber-norms-debate.

[226] U.N. General Assembly, *Resolution Adopted by the General Assembly on 5 December 2018 (96)*, 73rd Session, Agenda item 96 (Dec. 11, 2018), https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

[227] Emilio Iasiello, "OEWG or GGE – Which Has the Best Shot of Succeeding?" *Technative*, Dec. 5, 2019, https://www.technative.io/oewg-or-gge-which-has-the-best-shot-of-succeeding/.

[228] *See, e.g.,* Nigel Cory, *Why China Should be Disqualified from Participating in WTO Negotiations on Digital Trade Rules,* Information Technology and Innovation Foundation (Mar. 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

[229] Congressional Research Service, *Internet Regimes and WTO E-Commerce Negotiations*, at 35, Jan. 28, 2020.

[230] Nigel Cory, *Why China Should be Disqualified from Participating in WTO Negotiations on Digital Trade Rules,* Information Technology and Innovation Foundation (Mar. 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

[231] *Id.*; United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998*, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce (last visited June 15, 2020).

can use to increase control of, and capture more value from, data produced within national borders.[232]

The effects of China's protectionism on global trade are concerning because, as Daniel Castro and Alan McQuinn at the Information Technology and Innovation Foundation wrote in 2015, data protectionism like what is practiced by China threatens:

> [N]ot just the productivity, innovation, and competiveness of tech companies, but all companies with an international presence. In today's global economy, it is common for businesses to process data from customers, suppliers, and employees outside the company's home country. Data protectionism makes such data processing much more difficult, if not impossible.[233]

### *World Internet Conference*

Eager to establish its technical prowess on the world stage, China decided to launch its own global digital technology conference in 2014, which was hosted by the Cyberspace Administration of China.[234] Titled the "World Internet Conference," its goal was to "help build a cyberspace community with a consensual shared destiny and an ethic of respecting differences."[235]

One of the Chinese government's goals in this first conference was to have attendees sign the "Wuzhen Declaration," a nine-point document that echoed several official Chinese government goals, which they hoped would become the consensus of the attendees.[236] However, events did not go according to plan. As reported by the *Wall Street Journal*, the draft:

> [W]as slipped around the midnight hour Friday under the hotel room doors of attendees. It appeared to largely reflect a singular view: the watchful language used by Chinese President Xi Jinping. Chinese officials had argued at the two-day meeting of Chinese officials and local and foreign Internet executives that Beijing should have sovereignty over the Internet in China and must keep it under tight control.[237]

The plan to push an agreement through at the last minute was not successful, and the *Wall Street Journal* reported that at the end of the conference, the Wuzhen Declaration "was left unmentioned in the final speeches."[238]

---

[232] *See, e.g.,* "Data Governance Part One: Emerging Data Governance Practices," *Foreign Policy*, May 13, 2020.
[233] Daniel Castro & Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, Information Technology & Innovation Foundation, at 9 (Feb. 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf. *See also* Matthieu Pélissié du Rausas et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," McKinsey and Company, May 2011, http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.
[234] World Internet Conference, "2014 WIC Overview," Nov. 12, 2015, http://www.wuzhenwic.org/2015-11/12/c_46284.htm.
[235] *Id.*
[236] Catherine Shu, "China Tried To Get World Internet Conference Attendees To Ratify This Ridiculous Draft Declaration," *TechCrunch*, Nov. 21, 2014, https://techcrunch.com/2014/11/20/worldinternetconference-declaration/; World Internet Conference, "Draft Wuzhen Declaration," Nov. 21 2014, https://www.scribd.com/document/247566581/World-Internet-Conference-Draft-Declaration.
[237] James T. Arredy, "China Delivers Midnight Internet Declaration Offline," *The Wall Street Journal,* Nov. 21, 2014.
[238] *Id.*

The next year, President Xi attended the second World Internet Conference in person.[239] There, Xi used his opening remarks to lament the failures of the current system of Internet governance and argue that the world should "respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing."[240]

The participation of international technology companies at the World Internet Conference has also been a key aspect of China's efforts within this fora, although companies' involvement in the conference has been controversial. According to the World Internet Conference's official website, "prominent Internet figures from nearly 100 countries" have attended the conferences, including representatives from technology companies.[241] Such participation drew criticism from Roseann Rife, the East Asia Research Director at Amnesty International, who has long called for technology companies to reject China's Internet rules, stating that "Chinese authorities are trying to rewrite the rules of the internet so censorship and surveillance become the norm everywhere."[242]

Fortunately for the defenders of a free and open Internet, China has not achieved its goals through the World Internet Conference. According to Adam Segal, "[d]espite a significant investment of time, money, and political capital, the reach and influence of the World Internet Conference remain limited to China's friends. Most of the heads of government that have attended are from small states or the SCO."[243]

But China does not appear deterred. The 7th World Internet Conference, tentatively scheduled for the fourth quarter of 2020, is titled the "Light of Internet" Expo.[244] The press release announcing the conference says it is "expected to be a grand event for showcasing the latest technologies, products and applications around the world."[245]

### *International Standards-Setting Bodies*

Another realm that China seeks to influence, along with the major multilateral institutions, is global ICT standards-setting bodies. Global ICT rules of the road are set by several organizations, one of

---

[239] Adam Segal, "China's Internet Conference: Xi Jinping's Message to Washington," *Council on Foreign Relations*, Dec. 16, 2015.
[240] Xi Jinping, President of the People's Republic of China, Remarks at the "Opening Ceremony of the Second World Internet Conference," Wuzhen, China, Dec. 16, 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml; *See also* Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, at 9, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
[241] World Internet Conference, "World Internet Conference Overview of WIC," Nov. 10, 2015, http://www.wuzhenwic.org/2015-11/10/c_46113.htm (last visited July 10, 2020). *See also* Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, at 10, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
[242] Amnesty International, Asia and the Pacific, Internet and Social Media, "Tech Companies Must Reject China's Repressive Internet Rules," Dec. 15 2015, https://www.amnesty.org/en/latest/news/2015/12/tech-companies-must-reject-china-repressive-internet-rules/ (last visited July 10, 2020).
[243] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Institution*, June 2017, at 1, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf. SCO referenced in the quote is the Shanghai Cooperation Organization.
[244] World Internet Conference, "Fore-Notice on The Light of Internet Expo in the 7th World Internet Conference," Apr. 08 2020, http://www.wuzhenwic.org/2020-04/08/c_469136.htm.
[245] *Id.*

which is the 3rd Generation Partnership Project (3GPP), a private sector partnership composed of seven telecommunications standards development organizations.[246] 3GPP examines the range of technologies that make up mobile telecommunications, including radio access, core networks, cellular technologies, and services.[247] According to the U.S.-China Commission, "[t]he number of Chinese representatives serving in chair or vice chair leadership positions [in the 3GPP] rose from 9 of the 53 available positions in December 2012 to 11 of the 58 available positions in December 2017."[248] Due to this prominence in the organization's leadership, China has the capacity to influence the 3GPP to its advantage.[249]

Another entity heavily influenced by the Chinese is the International Telecommunications Union (ITU). According to its website, ITU "help[s] shape the future ICT policy and regulatory environment, global standards, and best practices to help spread access to ICT services."[250] Since 2014, the Secretary-General of the ITU has been Houlin Zhao, a former delegate at the Designing Institute of the Ministry of Posts and Telecommunications of China.[251] In addition to a former Chinese official being at the head of the ITU, Chinese firms and government research institutes held the largest number of chair and vice chair positions in the ITU's 5G-related standards-setting bodies, with eight of the 39 available leadership positions as of September 2018.[252] According to Michael O'Rielly of the U.S. Federal Communications Commission, the Chinese "have loaded up the voting to try to get their particular candidates on board, and their particular standards."[253]

Furthermore, it appears that as the head of the ITU, Secretary-General Zhao has used his position to strengthen China's digital influence around the world. The ITU-China agreement on aiding countries with communications networks resulted in ITU-China specific projects such as research and training centers for ICT in Afghanistan, a Trans-Eurasian Information Superhighway, and research and construction projects in Africa.[254] Secretary-General Zhao told *China Daily* that it is "highly likely" that he would sign another deal with the Export-Import Bank of China, and that working with China is critical for the ITU.[255] Finally, he added that China's Belt and Road is the perfect platform "to deliver services and help with ICT development around the globe by cooperating with China through the Initiative."[256]

Zhao Yonghong, Director-General of the Department of International Cooperation in the Ministry of Industry and Information Technology of the People's Republic of China, offered additional context on China's role in the ITU in September 2018. Zhao stated that the ITU should focus on "[s]trengthen[ing] the leading role of ITU in ICT technical standardization and further enhanc[ing]

---

[246] 3GPP, "About 3GPP," https://www.3gpp.org/about-3gpp (last visited July 6, 2020).
[247] *Id.*
[248] U.S.-China Economic and Security Review Commission, *2018 Annual Report to Congress*, at 455 (Nov. 2018).
[249] *Id.*
[250] International Telecommunication Union, "About International Telecommunication Union (ITU)," Feb. 19, 2020, https://www.itu.int/en/about/Pages/default.aspx.
[251] International Telecommunications Union, "Biography – Houlin Zhao," (last visited July 6, 2020), https://www.itu.int/en/osg/Pages/biography-zhao.aspx.
[252] U.S.-China Economic and Security Review Commission, *2018 Annual Report to Congress,* at 454 (Nov. 2018).
[253] Todd Shields & Alyza Sebenius, "Huawei's Clout Is So Strong It's Helping Shape Global 5G Rules," *Bloomberg,* Feb. 1, 2019.
[254] Kong Wenzheng, "ITU Vows to Join Hands with China," *China Daily*, May 24, 2019, www.chinadaily.com.cn/a/201904/24/WS5cbfbb1aa3104842260b7f2f.html.
[255] *Id.*
[256] *Id.*

its influence in the field of global standardization of emerging ICT technologies."[257] In fact, in 2012, China—along with other authoritarian regimes, like Russia and Saudi Arabia—introduced a proposal at the World Conference on International Telecommunications making ITU jurisdiction over the Internet more powerful.[258] Given China's leadership at the ITU, this proposal could strengthen China's control of the Internet.

China's strategy of using multilateral institutions to its advantage appears to have paid off at the ITU. Evidence of this success includes not only Zhao's support of Huawei, which in 2019 he defended against the United States' 5G security concerns by calling them driven by politics rather than evidence, but also China's ushering in of the proposed "New Internet Protocol" (New IP).[259] Some nations, including the United Kingdom, Sweden, and the United States, have raised concerns that China's New IP plan, if enacted, would fracture the global Internet and give state-run Internet Service Providers too much control.[260] The *Financial Times* reports that Huawei and other co-developers of New IP plan to promote the proposal at an ITU telecommunication conference in India in November 2020.[261] Zhao, as the head of the ITU, could influence whether the New IP is ratified.

However, there does appear to be some hope for democracies in the global battleground over control of international standards-setting bodies. In March 2020, the World Intellectual Property Organization—the United Nations organization created to lead the development of a balanced and effective international IP system—announced that Daren Tang, a Singapore national, won the nomination to become the new Director General.[262] Tang, who had the backing of the United States, was congratulated upon his election by Secretary Pompeo, who described him as "an effective advocate for protecting intellectual property [and] a vocal proponent of transparency and institutional integrity."[263]

The contest between Tang and his main opponent, the China-backed candidate Wang Binying, was a battle in the global digital arena between the United States and China.[264] In this case, and in what many hope will be an indication of future outcomes in the global competition between freedom and surveillance, the ideals of transparency and international cooperation won the day.

---

[257] "Top Contributors: Why China Supports ITU," *ITU News*, Sept. 20 2018, news.itu.int/top-contributors-why-china-supports-itu/.
[258] Chris Welch, "Russia, China, and Other Nations Draft Proposal to Give ITU Greater Influence Over the Internet," *The Verge,* Dec. 9 2012; Adi Robertson, "New World Order: is the UN about to take control of the internet?," The Verge, Nov. 29, 2012.
[259] Tom Miles, "Huawei Allegations Driven by Politics Not Evidence: U.N. Telecoms Chief," *Reuters,* Apr. 5 2019; Anna Gross & Madhumita Murgia, "China and Huawei Propose Reinvention of the Internet," *Financial Times,* Mar. 27 2020.
[260] Anna Gross & Madhumita Murgia, "China and Huawei Propose Reinvention of the Internet," *Financial Times,* Mar. 27 2020.
[261] *Id.*
[262] Nick Cummings-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times*, Mar. 4, 2020. *See also* The World Intellectual Property Organization, "What Is WIPO?" www.wipo.int/about-wipo/en/ (Last Visited May 21, 2020).
[263] Press Statement, U.S. Secretary of State Michael R. Pompeo, "Election of Daren Tang of Singapore as Director General of the World Intellectual Property Organization," Mar. 4 2020; Nick Cummings-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times*, Mar. 4, 2020.
[264] Nick Cumming-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times,* Mar. 4. 2020.

## Chapter 4: Conclusions and Recommendations

China's new model of digital authoritarianism, its international efforts to assert economic dominance in the digital domain, and its promotion of the adoption of a Chinese-inspired model of digital governance abroad, show its desire to alter and control the future of the digital domain. As described in Chapter 1, China is altering and controlling the digital domain domestically. It has developed and employed emerging technologies and techniques, ranging from blocking online content to utilizing facial recognition technologies that strengthen its surveillance systems, in order to suppress populations, individuals, and entities not aligned with the Chinese Communist Party (CCP).

While the CCP's use of the digital domain to maintain social control is problematic for those suffering in China, China's growing digital influence on the global stage creates a broader problem for the international community as China proliferates its technologies at a rapid rate around the globe, and in countries that span the spectrum of governance. As shown in Chapter 2, even countries that are staunch U.S. allies and stand for similar democratic and human rights values are entertaining the integration of Chinese technologies into their own digital infrastructures, such as 5G telecommunications, due to low costs, lack of viable alternatives, uncertainty about the future direction of the United States, and China's robust economic and diplomatic efforts.[265] As demonstrated in Chapter 3, China is leveraging its newfound influence to shape the rules of the road for the digital domain in ways that cater to digital authoritarianism and is antithetical to the United States' vision of how the Internet and cyber-enabled technologies should be used.

Indeed, three and a half years into the Trump administration, the United States is now on the precipice of losing the future of the cyber domain to China. If China continues to perfect the tools of digital authoritarianism and is able to effectively implement them both domestically and abroad, then China, not the United States and its allies, will shape the digital environment in which most of the world operates. Additionally, if the United States continues to cede its traditional role of diplomatic and technological leadership, the global growth of China's digital authoritarianism model presents a sinister future for the digital domain. At the grand strategic scale, if digital authoritarianism flourishes, China's importance on both the digital and global stages will continue to grow, allowing China to surpass the United States in the digital space and empowering China to create the future rules for digital governance.[266]

The spread of digital authoritarianism may also affect the United States' relationships with other countries as they determine how to balance their relationships with China, especially in the face of growing pressure to mirror China's authoritarian behavior in the digital domain. Furthermore, the basic human rights of individuals around the world, including U.S. citizens, could be negatively affected by a cyber domain that is reliant on Chinese technologies and values. As seen in places such as Xinjiang, personal privacy and civil liberties are threatened by China's digital authoritarianism model.[267] The global proliferation of China's digital authoritarianism model, if unchecked, will see

---

[265] Heather Stewart & Dan Sabbagh, "UK Huawei Decision Appears to Avert Row with US," *The Guardian*, Jan. 28, 2020.

[266] *See, e.g.,* John Chen et al., *China's Internet of Things,* Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, by SOS International (SOSi), at 69 (Oct. 2018).

[267] *See, e.g.,* Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," *Council on Foreign Relations*, updated June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang; U.S. Department of State, 2018 Report on

even more individuals fall under the control of authoritarians who use these technologies and techniques.

Despite China's various gains within the digital domain, such as its emerging technical capabilities and growing economic strength, there is still significant opportunity for the United States to adopt a genuinely competitive strategy and approach to China, to remain the global leader on cyberspace governance, and to reassert its leadership in areas where the technological gap between the United States and China has shrunk or disappeared. Accomplishing these goals will mark an important step in competing with China's digital authoritarianism, as opposed to merely denouncing it. Achieving the goal of securing a free digital domain and mitigating the threat of digital authoritarianism, however, will require a whole-of-government approach that leverages all aspects of the U.S. government, the private sector, and, critically, genuine partnerships with our partners and allies on the world stage. The Administration's current policy, which is detailed in Annex 1 of this report, is insufficient to combat China's digital authoritarianism, and its alienation of allies has further stunted the United States' ability to influence other countries away from China's digital authoritarianism model.

***Recommendations***

This report offers the following recommendations for more effective U.S. action to counter China's digital authoritarianism.

- ***Develop and Deploy Alternatives to Chinese 5G Technology with U.S. Allies****:* The United States lags behind China in developing and deploying cutting-edge 5G technologies, both domestically and abroad.[268] To provide an alternative, the U.S. should:
    - *Establish a Federally Funded Research and Development Center (FFRDC) on 5G*: Congress should pass legislation to establish an FFRDC that will examine how the United States can surpass China in the 5G development space. The FFRDC should examine U.S. technological strengths and weaknesses, as well as areas for immediate telecommunications development to provide an alternative to Chinese platforms and technologies.
    - *Create an Industry Consortium on 5G:* Congress should create a consortium comprised of leading U.S. telecommunications and technology companies that would be mandated to create the American 5G telecommunications alternative, exploring both cost-effective hardware and software solutions.
    - *Invest in Radio Access Network (RAN) Technologies:* Congress should provide new appropriations for RAN technologies.[269]

International Religious Freedom: China: Xinjiang, May 23, 2019, *available at* https://www.state.gov/reports/2018-report-on-international-religious-freedom/china-includes-tibet-xinjiang-hong-kong-and-macau/xinjiang/.

[268] Stu Woo, "In the Race to Dominate 5G, China Sprints Ahead," *The Wall Street Journal*, Sept. 7, 2019.

[269] "What are Radio Access Networks and 5G RAN?," *Verizon*, Feb. 2, 2020, https://www.verizon.com/about/our-company/5g/5g-radio-access-networks (last visited July 10, 2020). According to *Verizon,* "[c]ell phones use radio waves to communicate by converting your voice and data into digital signals to send through as radio waves. In order for your cell phone to connect to a network or the internet, it connects first through a radio access network (RAN). Radio access networks utilize radio transceivers to connect you to the cloud. Most base stations (aka transceivers) are primarily connected via fiber backhaul to the mobile core network." *Id.*

- *Establish a 5G Policy Coordinator within the White House*: The President should establish the position of a 5G Policy Coordinator tasked with coordinating the U.S. government's domestic and international 5G strategy.

❖ ***Limit the Spread of Malign Chinese Surveillance Technologies and Digital Authoritarianism****:* China is a leading developer and exporter of surveillance technologies, and continues to integrate new technologies that provide increasingly intrusive surveillance capabilities that can be misused by China or other state actors.

- *Establish a Digital Rights Promotion Fund:* Congress should establish and authorize a Digital Rights Promotion Fund, which will provide grants and investments directly to entities that support the promotion of a free, secure, stable, and open digital domain and fight against the authoritarian use of information and communications technologies. The fund will provide these groups, especially those existing in countries experiencing undue surveillance or other forms of digital authoritarianism, the resources needed to better push back against the spread of digital authoritarianism. Groups able to receive money would include:
  - Local activist organizations promoting a free digital domain and working to counter oppressive surveillance regimes in countries where digital authoritarianism is apparent or on the rise.
  - Nonprofit organizations that advocate for the adoption of international governance standards for the digital domain based on openness, transparency, and the rule of law, including the protection of human rights.
  - Think tanks and other institutional bodies that provide scholarship and policy recommendations for best paths forward to protect against the rise of authoritarian surveillance.
- *Establish an International Digital Infrastructure Corporation*: Congress should establish an independent, non-profit corporation with a clear and specific mandate to provide foreign countries with low-interest loans, grants, and other financing opportunities to purchase and implement U.S.-made digital infrastructure.
- *Authorize the Open Technology Fund*: Congress should fully authorize funds for the Open Technology Fund by passing S. 3820, the Open Technology Fund Authorization Act sponsored by Senators Robert Menendez, Marsha Blackburn, Ron Wyden, and Rick Scott.

❖ ***Strengthen the U.S. Digital Workforce****:* In order to compete and lead the digital space in the future, the United States will need an adaptable, innovative, and capable cyber workforce.

- *Establish a Cyber Service Academy*: Through legislative action, Congress should establish a new federal service academy similar to our other military service academies, with the specific aim of developing the future of our technology force. In addition to providing students a four year undergraduate education, the academy shall prepare students to become future military leaders in key digital and emerging technology fields, including robotics, artificial intelligence (AI), and cybersecurity.
- *Boost funding for STEM programs*: Congress should significantly increase federal spending on STEM programs, including Department of Defense (DoD)

funding in the National Defense Education program, funding for the National Science Foundation, and funding for the Minority Science and Engineering Improvement program within the Department of Education.

- ***Reinvigorate U.S. Diplomatic Leadership and Alliances, and Take a More Robust Role on the International Stage****:* China has made a concerted effort to change norms and practices to strengthen its position in various international fora regarding the digital domain.[270] China has additionally pushed economic development relating to technology in critical regions throughout the world.[271]
    - *Build a Coalition of Likeminded Allies on Critical Technology Issues:* The President should lead an international effort, in coordination with our allies and partners, to counter Chinese efforts to develop and proliferate digital domain products, technologies, and services that are not predicated on free, democratic values.
    - *Establish Mutual Cyber Defense Agreements*: The United States should approach likeminded nations to develop and establish mutual cyber defense and cooperation agreements that ensure national critical infrastructure, secure communications, trade relationships, and civil liberties are protected against cyber-attacks.
    - *Reassert U.S. Leadership in International Fora:* The President should establish a strategy for ensuring the United States holds chairmanships, serves as a leading voice, and operates as a key player in international fora such as the International Telecommunications Union or UN Group of Governmental Experts.
    - *Establish and Empower New Cyber Leadership within the State Department:* Congress should pass the Cyber Diplomacy Act of 2019, or similar legislation, that establishes a new office or bureau of cyber issues at the State Department, which shall report to the Under Secretary for Political Affairs.

[270] John Chen et al., *China's Internet of Things,* Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, by SOS International (SOSi), at 69 (Oct. 2018).
[271] *Id.*

## Annex 1: Understanding the Trump Cyberspace Policy

The United States is at a crossroads in regards to countering the implementation and growth of digital authoritarianism led by the regime in China. China's efforts to bring about the rise of digital authoritarianism hold the potential to fundamentally alter the landscape of information and communications technologies, as well as the legal and institutional underpinnings of these digital technologies, in ways that are incongruent with U.S. values and detrimental to U.S. and allied economic and security interests. Issues ranging from Chinese domination of the global information infrastructure and taking advantage of communications vulnerabilities, to using new technologies to assault basic human rights, to inhibiting U.S. economic and business opportunities abroad because of unreliable and exposed digital networks are all on the table if digital authoritarianism continues to proliferate unfettered.

It is imperative for the United States to perform its role as the leading force in developing, sustaining, and promulgating a global digital order based on openness, transparency, and the rule of law, including the protection of human rights. If the United States and other democratic countries are unable or unwilling to work to reverse the concerning trend of China's rising digital authoritarianism, we will cede the future of the global digital order to China and other authoritarian regimes. This annex examines President Trump and his Administration's efforts and policies, as well as recent Congressional actions, regarding cyberspace and whether these actions effectively curb China's digital authoritarianism.

### *National Security Policy Documents*

In September 2018, the Trump administration released its National Cyber Strategy (NCS). As a foundational policy document for the Administration, the NCS sets the stage for how the United States views the current climate within the cyber domain and how, broadly, they tackle issues that arise. The Trump administration frames the cyber domain as one where the United States is "in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks."[272] Such a characterization builds upon the labeling in the Trump administration's National Security Strategy (NSS), which describes China's exploitation of data and its alleged attempts to spread features of its authoritarian system, including corruption and the use of surveillance technology.[273]

By framing China and the cyber domain this way, the Trump administration fits the issues contained in cyberspace within one of the principal characteristics of its national security strategy: that the United States is in a great-power competition with key adversaries. The NCS proceeds to specifically label China as one of the entities that is challenging the United States within the cyber domain.[274] While the document falls short of directly identifying the Chinese Communist Party's use of digital authoritarianism as a national security threat, the NCS articulates a need to defend against authoritarian states utilizing security or terrorism concerns to erode a free and secure Internet.[275]

The NCS breaks U.S. cyber strategy into four pillars. These pillars are:

---

[272] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 2.
[273] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.
[274] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 2.
[275] *Id.*, at 24.

1) Protect the American People, the Homeland, and the American Way of Life – involving issues such as protecting U.S. networks, critical infrastructure, and data, combatting crime, and pushing government innovation;
2) Promote American Prosperity – including promoting America's advantage in the digital economy, maintaining U.S. leadership on cyber issues, and strengthening the U.S. workforce;
3) Preserve Peace through Strength – featuring deterring malign cyber activities and enhancing norms of state behavior;
4) Advance American Influence – containing extending a free and interoperable Internet globally and building international cyber capacity.[276]

From these four platforms flow priority actions meant to target certain issues, ranging from building a proposed cyber deterrence initiative, to "promot[ing] and maintain[ing] markets for United States ingenuity worldwide," to maintaining United States leadership in emerging technologies.[277] Due to China's continued growth within the cyber domain, many of these priority actions in effect target digital authoritarianism in some way. For example, the NCS outlines a need to broadly engage global partners, international organizations, and civil society to protect Internet freedom and improve international cyber capacity.[278] Critical to this effort is the need for the U.S. to reinforce the openness, interoperability, and reliability of the Internet.[279] The plan calls for investment in the communications infrastructure and cybersecurity capacities of partner states to not only enhance the Cyber Deterrence Initiative, but also to ensure their Internet capabilities align with U.S. interests and standards of Internet freedom.[280]

There are other mechanisms espoused in the NCS that could play a role in combatting China's digital authoritarianism that are not explicitly linked to the topic. One such example is how a primary objective of "promoting American prosperity" in the NCS is to "preserve U.S. influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency."[281] The purpose of this objective is to "foster a vibrant and resilient digital economy" through prioritizing innovation and maintaining U.S. leadership in emerging technologies.[282]

---

[276] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 6, 8, 10, 14, 16, 17, 20, 21, 24, 25, and 26; Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.
[277] President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 15, 21, 25.
[278] *Id.*, at 25 and 26. According the National Cyber Strategy, cyber capacity building involves "the United States build[ing] strategic partnerships that promote cybersecurity best practices through a common vision of an open, interoperable, reliable, and secure Internet that encourages investment and opens new economic markets. In addition, capacity building allows for additional opportunities to share cyber threat information, enabling the United States Government and our partners to better defend domestic critical infrastructure and global supply chains, as well as focus whole-of government cyber engagements." *Id.*
[279] *Id.*, at 24.
[280] *Id.*, at 21 and 26. Espoused in the Administration's 2018 National Cyber Strategy, the Cyber Deterrence Initiative is an effort "to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior." To achieve this goal, "the United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors." *Id.* at 21.
[281] *Id.*, at 14.
[282] *Id.*, at 14-15; Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.

Another key issue put forth by the NCS to help the United States better compete in the digital marketplace and fight back against digital authoritarianism is strengthening its leadership on innovation and developing emerging technologies.[283] One of the primary aspects for driving U.S. technological development leadership is to promote the free flow of data across borders that push against authoritarian governments' attempts to localize data under the guise of national security, and, along that vein, the NCS asserts that the Administration will promote "open, industry driven standards, innovative products, and approaches that permit global innovation and the free flow of data while meeting the legitimate security needs of the U.S."[284] Additionally, the NCS aims to ensure the United States counters behavior that acts against U.S. interests, saying in its third pillar that the administration would use "all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation."[285]

### *Administration Efforts*

China continues to rapidly expand its digital authoritarianism model and make gains on the United States in becoming the dominant player on a range of critical technologies, placing U.S. leadership on cyber issues at risk. In response to the gains in Chinese technological development, the Trump administration has turned to punitive measures, using sanctions as a weapon against China. As China's technology sector begins to achieve global significance, several of its players have found themselves on the front lines of the U.S.-China trade war and atop U.S. sanctions lists.[286] Most notably, one of China's largest companies, Huawei, has been the target of U.S. sanctions and restrictions as the U.S. seeks to pre-empt potential cyber threats.[287] The Trump administration has referred to Huawei as a national security threat, cited the telecommunications giant's close ties to the Chinese government, its repeated intellectual property theft, and its violations of U.S. sanctions on Iran as reasons for Huawei to be excluded from U.S. markets, and encouraged others to take similar steps.[288]

Although U.S. suspicions of Huawei can be traced as far back as 2012, recent actions are supposedly meant to demonstrate a more aggressive U.S. posture towards the company and the Chinese

---

[283] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019.
[284] *Id.*; President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 14.
[285] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; President Donald J. Trump, *National Cyber Strategy of the United States of America*, The White House, Sept. 2018, at 21.
[286] Kiran Stacey et al., "US blacklists 28 Chinese entities in trade war escalation," *Financial Times*, October 8, 2019; Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," *The New York Times*, May 15, 2020.
[287] Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," *The New York Times*, May 15, 2020; Associated Press, "US Adds New Sanction on Chinese Tech Giant Huawei," *US News and World Report*, May 16, 2020.
[288] Ana Swanson, "U.S. Delivers Another Blow to Huawei With New Tech Restrictions," *The New York Times*, May 15, 2020; David Goldman, "What Did Huawei do to Land in Such Hot Water with the US?" *CNN,* May 20, 2019; Federal Communications Commission, "FCC Bars Use of Universal Service Funding for Equipment and Services Posing National Security Risks," Nov. 22, 2019; Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation, 85 Fed. Reg. 27610, Jan. 3, 2020; Dan Strumpf & Patricia Kowsmann, "U.S. Prosecutors Probe Huawei on New Allegations of Technology Theft," *The Wall Street Journal,* Aug. 29, 2019; Julian E. Barnes and Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *The New York Times*, Mar. 17, 2019.

technology sector as a whole.[289] In May 2018, the Pentagon banned the sale of Huawei and ZTE phones on U.S. military bases.[290] Later that year, Huawei's CFO (and daughter of its founder), Meng Wanzhou, was arrested in Canada at the United States' request for allegedly violating U.S. sanctions on Iran.[291] On May 15, 2019, President Trump issued Executive Order 13873 on Securing the Information and Communications Technology and Services Supply Chain, which declared:

> The threat of foreign adversaries to U.S. ICT technologies—through creating and exploiting vulnerabilities in technology and services, and "the unrestricted acquisition or use in the United States of information and communications technology or services, designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries"—constitutes an "unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[292]

Following the Executive Order issuance, the United States in May 2019 placed Huawei and 68 of its affiliates on the Bureau of Industry and Security's Entity List via authorities in the Export Control Reform Act of 2018's Export Administration Regulations, and subsequently in August added 46 additional entities, in an effort to restrict their access to U.S. markets.[293] In May 2020, the administration unveiled new rules requiring foreign semiconductor makers to obtain a U.S. license to ship Huawei-designed semiconductors produced using U.S. technology to Huawei.[294] More broadly, the United States has sought to mount pressure on allies and partners such as Germany and the UK to restrict Huawei equipment in their 5G infrastructure plans due to security concerns.[295] These efforts, however, have produced mixed results at best, and may well have been counterproductive, at least in the short-term, as seen in Chapter 2 of this report.

Unfortunately, contradictory U.S. policy implementation has hampered the impact of punitive measures to change China's behavior. This contradiction can be seen in the Commerce Department's provision of temporary licenses to Huawei despite the administration's stated need and previous actions for increasing scrutiny of Huawei transactions.[296] The Commerce Department unveiled that the:

---

[289] Sean Keane, "Huawei ban timeline: Uber rival hits AppGallery store as it moves towards self-sufficiency," *CNET,* June 25, 2020; Pam Benson, "Congressional report: U.S. should 'view with suspicion' two Chinese companies," *CNN*, Oct. 8, 2012.
[290] Sean Keane, "Huawei ban timeline: Uber rival hits AppGallery store as it moves towards self-sufficiency," *CNET,* June 25, 2020; Katie Collins, "Pentagon bans sale of Huawei, ZTE phones on US military bases," *CNET*, May 2, 2018.
[291] Press Release, U.S. Department of Justice, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," January 28, 2019; Dan Bilefsky, "Extradition Hearings Begin for Meng Wanzhou, Huawei Officer Held in Canada," *The New York Times*, Jan. 20, 2020.
[292] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; President Donald J. Trump, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*, The White House, May 15, 2018; U.S. Department of Commerce - Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316, Nov. 27, 2019.
[293] Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43493, Aug. 21, 2019; Addition of Entities to the Entity List, 84 Fed. Reg. 22961, May 21, 2019.
[294] Frank Bajak, "US adds new sanction on Chinese tech giant Huawei," *Associated Press*, May 16, 2020.
[295] Julian E. Barnes & Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *The New York Times*, March 17, 2019.
[296] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; Addition of Entities to the Entity List, 84 Fed. Reg. 22961, May 21, 2019.

> Bureau of Industry and Security (BIS) issued a 90-day Temporary General License to allow for the completion by August 19th of contracts entered into before May 16th. On August 15th, BIS issued an additional General License to allow for some engagement with Huawei and its affiliates to continue.[297]

While a variety of factors enter into how BIS decides whether a company should receive certain export or transfer waivers, the provision of multiple waivers to Huawei and other entities fundamentally conflicts with the Administration's stated desire to mitigate the risks associated with increased proliferation of Huawei technologies. Consequently, episodes such as this one highlight how the Administration's policy and actions are not in sync, damaging the United States' ability to push back on essential levers of China's digital authoritarianism system.

For its part, Huawei has loudly decried U.S. actions taken against the company, through both legal challenges and public statements. For example, the company filed a suit against the FCC for a ruling in November 2019 blocking the use of federal funds to purchase Huawei products, saying "it fails to offer Huawei required due process protections."[298] The company has questioned the United States' motives for targeting Huawei, asserting that the United States "is leveraging its own technological strengths to crush companies outside its own borders. This will only serve to undermine the trust international companies place in US technology and supply chains."[299] Huawei has even accused the U.S. of illegal behavior such as hacking its systems and threatening its employees.[300]

In response to the growing threats posed by digital authoritarianism, the federal government has taken steps towards improving U.S. cybersecurity capabilities. In 2018, President Trump signed the Cybersecurity and Infrastructure Security Agency Act into law, establishing the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS).[301] CISA's mission is to "lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.[302] The agency's formation is a step toward securing U.S. domestic cyber infrastructure; however, as an agency within DHS, its mandate does not extend into the international realm, and therefore is unlikely to be able to play a role in pushing back against China's spread of digital authoritarianism around the globe.

The State Department, which oversees international diplomatic efforts regarding the cyber domain, does not currently have the structure needed to effectively tackle China's growing influence in the digital sphere. In 2018, the State Department released proposals to establish a Bureau of Cyberspace Security and Emerging Technologies (CSET), which would consolidate and strengthen U.S. diplomatic efforts to secure cyberspace and digitally enabled technologies, reduce risks of cyber

---

[297] Congressional Research Service, Research Conducted for Committee Staff, Sept. 30, 2019; Temporary General License: Extension of Validity, Clarifications to Authorized Transactions, and Changes to Certification Statement Requirements, 84 Fed. Reg. 43487, August 21, 2019; Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43493, Aug. 21, 2019.
[298] Norman Pearlstine et al., "The War Against Huawei," *Los Angeles Times*, Dec. 19, 2019; Colin Lecher, "The FCC votes to block Huawei from billions in federal aid," *The Verge*, Nov. 22, 2019.
[299] Eileen Yu, "Huawei rebukes US attempts to stymie foreign competition with chip rule," *ZDNet*, May 18, 2020.
[300] Dan Strumpf & Chuin-Wei Yap, "Huawei Accuses the U.S. of Cyberattacks and Staff Threats," *The Wall Street Journal*, Sept. 3, 2019.
[301] Cybersecurity and Infrastructure Security Agency, "About CISA," https://www.cisa.gov/about-cisa (last visited May 10, 2020).
[302] *Id.*

conflict, and boost America's cyber competitiveness.[303] In the proposal, the Bureau would operate under the office of the Under Secretary for Arms Control and International Security Affairs.[304] However, the rollout was stalled in Congress due to negotiations over the bureau's placement and a lack of clarity over its mandate.

One alternative to CSET—the Cyber Diplomacy Act of 2019—was introduced in Congress by Representatives McCaul (R-TX-10) and Engel (D-NY-16) in January 2019.[305] The Cyber Diplomacy Act would create an Office of International Cyberspace Policy (OICP), operating under the State Department's Under Secretary of Political Affairs. In addition to advising the State Department on cyberspace policy, the office would engage in diplomatic efforts to reinforce international cybersecurity, promote Internet access and freedom, and counter international cyber threats. The bill directly calls out China for promoting international norms of Internet behavior that restrict critical freedoms. In addition, the bill requires the OICP to produce annual country reports on human rights practices relating to the Internet, particularly emphasizing online censorship and political repression.[306]

[303] Sean Lyngaas, "State Department Proposes New $20.8 million Cybersecurity Bureau," *Cyberscoop,* June 5, 2019, https://www.cyberscoop.com/state-department-proposes-new-20-8-million-cybersecurity-bureau/.
[304] U.S. Department of State, Congressional Budget Justification Appendix 1: Department of State Diplomatic Engagement, Fiscal Year 2021.
[305] Cyber Diplomacy Act of 2019, H.R. 739 (116th Congress, introduced Jan. 24, 2019).
[306] *Id.*

## Annex 2: The United States and 5G

One of the most prominent and pressing issues facing the United States regarding the future of the digital domain is the development and deployment of 5G telecommunications technologies. 5G technologies, following on fourth generation (4G) and LTE technologies, provide a number of improvements to the capabilities of previous generations, including increased data transfer rates in a fixed period of time, also known as bandwidth, and enhanced connectivity capabilities, such as ultra-low latency (the delay between when data is sent from one device on a network and received by another).[307] 5G technologies are deployed in new ways compared to their predecessors: while previous generations used large cell towers to transmit signals, 5G can also use small cells (radio access points) that are about the size of a picnic cooler or mini fridge, creating greater cellular density and faster deployment.[308] 5G networks are also critical to enabling the proliferation of the Internet of Things (IoT) devices.[309] Such enhanced capabilities will not only reshape cellular communications and facilitate the development of emerging technologies, but will also fundamentally alter how industries and societies that rely on connectivity to data sources operate.[310]

While the spread of 5G technologies will provide many positive impacts for society and industry, China is pursuing avenues to manipulate the capabilities endowed by these new technologies. As noted earlier in the report, China has made significant inroads in the development and deployment of 5G. China's efforts, as a number of former military leaders elucidate in an April 3, 2019, letter, present "grave concerns" to the United States, our allies, and our partners.[311] The letter states that a widely adopted Chinese-developed 5G network "provide[s] near-persistent data transfer back to China," would mean U.S. reliance on Chinese technologies for critical military communications, and will "advance a pernicious high-tech authoritarianism."[312] These comments underscore that a 5G infrastructure built on Chinese technologies will promote digital authoritarianism around the globe, and consequently, why the United States must pursue mechanisms to mitigate China's influence in this digital sphere.

As 5G technology moves closer to global deployment, the U.S. has some technological disadvantages that have both commercial and security implications. The development of 5G networks will boost the rate of implementation for new and transformative technologies ranging from autonomous vehicles to smart cities to virtual reality.[313] There is much to gain from leading the

---

[307] Qualcomm, "Everything You Need to Know about 5G," https://www.qualcomm.com/invention/5g/what-is-5g (last visited May 13, 2020); Congressional Research Service, *Fifth Generation (5G) Telecommunications Technologies: Issues for Congress*, Jan. 30, 2019, at 1.

[308] "What is Small Cell Technology?," Verizon, Aug. 8, 2018, https://www.verizon.com/about/our-company/5g/what-small-cell-technology (last visited May 14, 2020); "Why 5G Can't Succeed Without a Small Cell Revolution," PwC, https://www.pwc.com/us/en/industry/tmt/assets/5g-small-cell-revolution.pdf (last visited May 13, 2020).

[309] Murali Venkatesh, "How 5G Networking Will Unleash the Full Potential of IoT," *Oracle*, Feb. 4, 2019, https://blogs.oracle.com/iot/how-5g-networking-will-unleash-the-full-potential-of-iot.

[310] Dan Patterson & Anisha Nandi, "5G explained: How it works, who it will impact, and when we'll have it," *CBS News*, Feb. 21, 2019; PwC, "Why 5G Can't Succeed Without a Small Cell Revolution," https://www.pwc.com/us/en/industry/tmt/assets/5g-small-cell-revolution.pdf (last visited May 13, 2020).

[311] Letter from Adm. James Stavridis et al., "Statement by Former U.S. Military Leaders," Apr. 3, 2019, https://www.lawfareblog.com/document-former-military-and-intelligence-officials-letter-5g-risks.

[312] *Id.*

[313] Randal Kenworthy, "The 5G and IoT Revolution is Coming: Here's What to Expect," *Forbes Technology Council*, Nov. 18, 2019.

pack in the global telecommunications race—and much to lose by lagging behind.[314]Although Europe dominated the development and implementation of 2G technologies, and Japan led on the deployment and adoption of 3G technologies, beginning in about 2016 the United States pulled ahead and led on the development and adoption of 4G.[315] Through a first-mover advantage provided by its innovation and implementation of 4G and LTE, and complemented by its competitive mobile device technologies, the United States was able to shape the global 4G ecosystem.[316] U.S. companies took advantage of the enhanced capabilities of the new network, developing devices, apps, and services that would dominate global markets.[317] This success led to a 70% growth of the U.S. telecommunications industry between 2011 and 2014, increasing industry jobs by 80% and boosting GDP.[318]

Yet whatever advantages the U.S. had in the innovation deployment of 4G and LTE networks are beginning to narrow in the new age of wireless development. A 2019 report by the Defense Innovation Board suggests that, due to several critical shortcomings in U.S. 5G development, it is unlikely the US will win the race to 5G.[319] A critical differentiator between 4G and 5G technologies is that 5G will leverage various segments of the electromagnetic spectrum: from the low to mid-band spectrum, or "sub-6", to the high-band spectrum, or "mmWave."[320] As the spectrum bands are the fundamental layers upon which the entire 5G network and infrastructure is built, the decision to develop technologies based on lower or higher frequencies is one of the most critical near-term choices for policy-makers and involves different levels of costs and investments.[321] For example, mmWave technologies are capable of faster and more secure data transmission, but require far greater infrastructure and monetary investments to set up, while the sub-6 band can cover broader areas with less risk of interruption and is able to "leverage existing 4G infrastructure."[322] Currently, the advantages of the sub-6 band, especially on costs and broad coverage, make it the most likely

---

[314] Statement of Peter Harrell, Center for a New American Security, *5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation*, Hearing before the United States Senate Committee on the Judiciary, May 14, 2019, at 2, https://s3.amazonaws.com/files.cnas.org/documents/Harrell-Judiciary-Testimony-May-14-2019.pdf?mtime=20190515171307.

[315] Recon Analytics, *How America's Leading Position in 4G Propelled the Economy*, at 6 (Apr. 16, 2018), https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.

[316] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 6 (Apr. 2019).

[317] Statement of Peter Harrell, Center for a New American Security, *5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation*, Hearing before the United States Senate Committee on the Judiciary, May 14, 2019, at 2, https://s3.amazonaws.com/files.cnas.org/documents/Harrell-Judiciary-Testimony-May-14-2019.pdf?mtime=20190515171307.

[318] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 7 (Apr. 2019); Recon Analytics, *How America's Leading Position in 4G Propelled the Economy*, at 6 (Apr. 16, 2018).

[319] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 7 (Apr. 2019).

[320] *Id.* at 8-11.

[321] Dave Andersen, "5G FAQ series: What's the difference between mmWave and sub-6 GHz spectrum?," *RootMetrics by IHS Markit*, Oct. 28, 2019, https://rootmetrics.com/en-GB/content/5g-faq-series-whats-the-difference-between-mmwave-and-sub-6-ghz-spectrum; Gabriel Brown, *White Paper: Exploring the Potential of mmWave for 5G Mobile Access,* Heavy Reading, at 3, 8, 10 (June 2016), https://www.qualcomm.com/media/documents/files/heavy-reading-whitepaper-exploring-the-potential-of-mmwave-for-5g-mobile-access.pdf.

[322] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 8, 10 (Apr. 2019).

near-term outcome for propagating a 5G ecosystem.[323] However, in the United States, portions of the sub-6 bands are owned by the government, somewhat limiting civilian and commercial use of that spectrum.[324]

The limits on spectrum have posed a number of problems to US near-term competitiveness in the 5G global ecosystem, not least of which is that Chinese companies have managed to outpace the U.S. in development and export of its 5G infrastructure. China has pursued infrastructure buildout based on the sub-6 spectrum band, and with its head start in the global deployment of its 5G infrastructure, has been able to attract a growing share of the global market with its promises of a high quality and low cost network.[325] Given the current higher costs and lower density of the mmWave spectrum range, many global players—including key U.S. allies and partners—have chosen to follow China's lead.[326] The consequences of China leading the buildout of the global 5G ecosystem are severe, and could include creating overseas security risks for Department of Defense operations and eroding competitive supply chains for the United States.[327] **It is critically important to note, however, that the United States could find a future advantage by leading on mmWave technologies, since 1) this band is the spectrum where ultra-fast innovations may arise and 2) a fully actualized 5G network will see devices seamlessly utilize and transition between both the sub-6 and mmWave bands.[328]**

Another reason the United States finds itself in greater competition with China on 5G deployment is that China has spent more on 5G development, implementing 198,000 5G-operable base stations domestically, with 500,000 more planned, and rapidly deploying 5G equipment and infrastructure around the world.[329] In Europe in particular, Huawei and ZTE have partnered with many countries to build their 5G networks despite US protests over security concerns, and Chinese-built network infrastructure continues to spread across the continent.[330] Within Congress and the Administration there is a bipartisan understanding of the threats posed by Chinese firms building the base layers of radio equipment and other telecommunications infrastructure upon which 5G operates. Unfortunately, there is a major gap in the United States government between rhetorical complaints

---

[323] *Id.*, at 10; Dave Andersen, "5G FAQ series: What's the difference between mmWave and sub-6 GHz spectrum?," *RootMetrics by IHS Markit*, Oct. 28, 2019, https://rootmetrics.com/en-GB/content/5g-faq-series-whats-the-difference-between-mmwave-and-sub-6-ghz-spectrum

[324] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 10 (Apr. 2019). It is important to note that while the government holds large portions of the sub-6GHz spectrum, there have been certain initiatives aimed at freeing up some of this spectrum, such as S. 19, the MOBILE Now Act introduced by Senators John Thune (R-ND) and Bill Nelson (D-FL) during the 115th Congress in 2018. *Id.*

[325] *Id.*, at 12, 21; Press Release, U.S. Department of Justice, "Attorney General William P. Barr Delivers the Keynote Address at the Department of Justice's China Initiative Conference," February 6, 2020.

[326] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 15 (Apr. 2019).

[327] *Id.* at 4.

[328] Monica Alleven, "SK Telecom, Ericsson demonstrate 5G connected BMW at 28 GHz," *Fierce Wireless*, Nov. 15, 2016, https://www.fiercewireless.com/tech/sk-telecom-ericsson-demonstrate-5g-connected-bmw-at-28-ghz; Bevin Fletcher, "New Samsung 5G phones can tap both sub-6 GHz and millimeter wave spectrum," *Fierce Wireless*, Feb. 12, 2020, https://www.fiercewireless.com/devices/new-samsung-5g-phones-can-tap-both-sub-6-ghz-and-millimeter-wave-spectrum.

[329] Jason Murdock, "China Planning 500,000 New 5G Base Stations as State Officials Say Construction Has 'Entered the Fast Lane'," *Newsweek*, Feb. 24, 2020; Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 13 (Apr. 2019).

[330] Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks and Opportunities for DoD*, Defense Innovation Board, at 13 (Apr. 2019).

about Chinese efforts to dominate the 5G domain and actual, tangible steps to counter China's government and industry on the issue.

Finally, the United States currently does not have a domestic 5G supplier for the equipment that makes up the Radio Access Network (RAN) for 5G.[331] Instead, countries seeking viable alternatives to Chinese 5G RAN infrastructure rely on companies such as Swedish company Ericsson, South Korea-based Samsung, or Finnish firm Nokia to build out core components of their layer of the 5G infrastructure.[332] While these companies do provide alternatives to Huawei, Chinese government subsidies to Huawei allow the company to sell products at far lower prices and offer low-cost financing, undercutting the competitiveness of other firms.[333] This combination of a lack of a U.S. domestic 5G alternative and China's monetary subsidies is leading to a 5G environment that lacks stable, secure U.S. infrastructure and products, and is increasingly problematic for U.S. security. To maintain U.S. security, it is therefore imperative that the United States find, develop, and pursue policies that open up pathways for United States industry to become a leading player in all facets of the 5G domain in the future.

[331] Tom Wheeler, "5G in Five (not so) Easy Pieces," *The Brookings Institution*, July 9, 2019; "What are Radio Access Networks and 5G RAN?," Verizon, Feb. 2, 2020, https://www.verizon.com/about/our-company/5g/5g-radio-access-networks (last accessed July 10, 2020).
[332] Tom Wheeler, "5G in Five (not so) Easy Pieces," *The Brookings Institution*, July 9, 2019.
[333] *Id.*

# EXHIBIT 37

Freedom House

# Key Findings

## 1

**Global internet freedom declined for the 12th consecutive year.** The sharpest downgrades were documented in Russia, Myanmar, Sudan, and Libya. Following the Russian military's illegal and unprovoked invasion of Ukraine, the Kremlin dramatically intensified its ongoing efforts to suppress domestic dissent and accelerated the closure or exile of the country's remaining independent media outlets. In at least 53 countries, users faced legal repercussions for expressing themselves online, often leading to draconian prison terms.

## 2

**Governments are breaking apart the global internet to create more controllable online spaces.** A record number of national governments blocked websites with nonviolent political, social, or religious content, undermining the rights to free expression and access to information. A majority of these blocks targeted sources located outside of the country. New national laws posed an additional threat to the free flow of information by centralizing technical infrastructure and applying flawed regulations to social media platforms and user data.

## 3

**China was the world's worst environment for internet freedom for the eighth consecutive year.** Censorship intensified during the 2022 Beijing Olympics and after tennis star Peng Shuai accused a high-ranking Chinese Communist Party (CCP) official of sexual assault. The government continued to tighten its control over the country's booming technology sector, including through new rules that require platforms to use their algorithmic systems to promote CCP ideology.

## 4

**A record 26 countries experienced internet freedom improvements.** Despite the overall global decline, civil society organizations in many countries have driven collaborative efforts to improve legislation, develop media resilience, and ensure accountability among technology companies. Successful collective actions against internet shutdowns offered a model for further progress on other problems like commercial spyware.

## 5

**Internet freedom in the United States improved marginally for the first time in six years.** There were fewer reported cases of targeted surveillance and online harassment during protests compared with the previous year, and the country now ranks ninth globally, tied with Australia and France. The United States still lacks a comprehensive federal privacy law, and policymakers made little progress on the passage of other legislation related to internet freedom. Ahead of the November 2022 midterm elections, the online environment was riddled with political disinformation, conspiracy theories, and online harassment aimed at election workers and officials.

## 6

**Human rights hang in the balance amid a competition to control the web.** Authoritarian states are vying to propagate their model of digital control around the world. In response, a coalition of democratic governments has increased the promotion of online human rights at multilateral forums, outlining a positive vision for the internet. However, their progress remains hampered by problematic internet freedom practices in their own countries.

# Introduction

By Adrian Shahbaz, Allie Funk, and Kian Vesteinsson

At home and on the international stage, authoritarians are on a campaign to divide the open internet into a patchwork of repressive enclaves. More governments than ever are exerting control over what people can access and share online by blocking foreign websites, hoarding personal data, and centralizing their countries' technical infrastructure. As a result of these trends, global internet freedom has declined for a 12th consecutive year.

Rising digital repression in many countries mirrored broader crackdowns on human rights over the past year. Nowhere was this clearer than in Russia, Myanmar, Libya, and Sudan, which experienced the world's steepest declines in internet freedom. Online censorship reached an all-time high, with a record number of governments blocking political, social, or religious content, often targeting information sources based outside of their borders. More than two-thirds of the world's internet users now live in countries where authorities punish people for exercising their right to free expression online.

Alarmingly, these antidemocratic abuses are not the only factor behind the splintering of the internet into national segments. Some governments are clearly cultivating a domestic digital space where state-endorsed narratives dominate and independent media, civil society, and already marginalized voices are more easily suppressed. But others are inadvertently contributing to country-based barriers through their efforts to tackle disinformation, protect user data, and deter genuine cybercrimes. Whatever the intention, however, the growing fragmentation of the internet comes with serious consequences for fundamental rights including freedom of expression, access to information, and privacy, particularly for people living under authoritarian regimes or in backsliding democracies.

Entrenched and aspiring authoritarian leaders sought to contain online dissent by preventing residents from reaching global information sources.

## A more fragmented internet

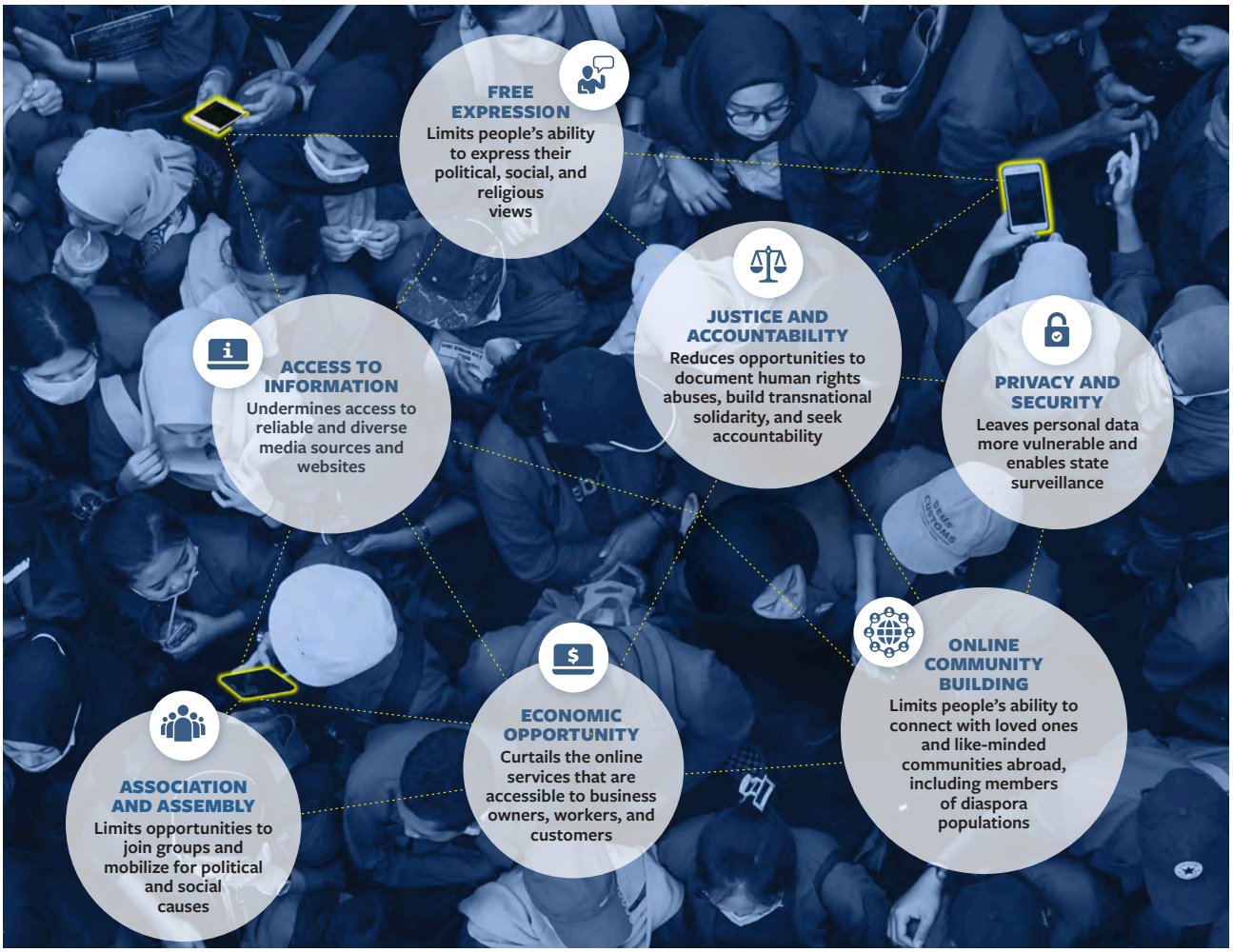
The internet has always been subject to some degree of fracturing along national borders, but increased state intervention in the last year has dramatically accelerated the process. This report identifies three main causes of fragmentation, all of which contributed to declining respect for human rights online: restrictions on the flow of news and information, centralized state control over internet infrastructure, and barriers to cross-border transfers of user data.

While the physical network of the global internet remains intact, a growing number of users only have access to an online space that mirrors the views of their government and its interests. Authorities in 47 of the 70 countries covered by *Freedom on the Net* have limited users' access to information sources located outside of their borders. Virtually all of these restrictions constitute clear infringements of the Universal Declaration of Human Rights, which codifies the right "to seek, receive, and impart information and ideas through any media and regardless of frontiers." In most cases, entrenched and aspiring authoritarian leaders sought to contain online dissent by preventing residents from reaching information sources based in countries with a greater level of media freedom.

This increasing fragmentation is part of a global, multifaceted competition for control over the digital sphere. For most of the period since the internet's inception, representatives of the private sector, civil society, and the technical community have participated in a consensus-driven process to harmonize security standards and technical protocols. This has resulted in a decentralized infrastructure that speaks a common language, enabling users to communicate with one another and access information regardless of location. Authoritarian powers

## FENCED IN: HOW INTERNET FRAGMENTATION HARMS HUMAN RIGHTS

The internet is more siloed than ever, preventing billions of people from exercising their human rights online.




have long sought to displace this multistakeholder model of internet governance with one that promotes cyber sovereignty, or greater control by states. Diplomats from China and Russia have made inroads at institutions like the International Telecommunication Union (ITU), seeking to transform the United Nations agency into a global internet regulator that advances authoritarian interests. Doing so would fundamentally alter the open internet, preventing billions of people from communicating with one another and accessing life-changing resources without explicit permission from their governments.

A cohort of democracies are pushing back. Having previously focused on a narrower set of economic and security interests linked to countering Beijing, the United States has more recently shown promising signs of reengagement in cyber diplomacy with the aim of promoting a positive vision of democracy in the digital age. The European Union (EU) has also moved forward with innovative and rights-respecting regulatory approaches to address harms that have been exacerbated by the internet. But many democracies have yet to significantly improve respect for online rights within their own borders. Of the 35 countries covered by this report that participated in the US-hosted Summit for Democracy, 13 experienced an internet freedom decline over the past year, as did 10 of the 18 *Freedom on the Net* countries that signed the US-led Declaration for the Future of the Internet. By adopting flawed policies at home, democracies risk undermining the very values they seek to defend abroad, while potentially cutting off residents of authoritarian countries from a freer and more open internet.

## Protecting human rights online through democratic resilience

The technologies associated with the global internet have fostered connections and common interests among different people and communities, facilitated more transparent and participatory governance, and brought tremendous direct and indirect economic benefits. However, the rapid digitization of media and communication has also generated new opportunities for manipulation, extremism, and repression. Policymakers have been too slow in addressing the hazards that accompany technological change, and their emphasis on state-level digital threats—grouped under terms such as information war, cyberwar, and trade war—has often elevated national security and economic considerations over the fundamental rights of individuals. The reality is that economic and security interests are directly linked to respect for individual rights.

Lasting solutions to disinformation, online harassment, and other harms presented by digital tools are unlikely to be achieved through a fragmentation of the internet. Simply imposing strict national laws onto a global information system is bound to be ineffective. Beijing's efforts to build and maintain a Great Firewall, for example, have done little to address societal concerns about privacy, cybersecurity, corporate malfeasance, false content, and abusive online behavior. It may be difficult to prevent Beijing, Moscow, and Tehran from persisting in their efforts to isolate their populations, but there remains an opportunity to convince many less repressive states that an open internet is in their best interest.

Greater focus should be placed on developing political and societal resilience in the face of these harms. Already, journalists, human rights defenders, and advocacy organizations have been at the forefront of many recent successes that strengthened democratic resilience in the digital sphere. Broad coalitions have bolstered international norms against internet shutdowns, which occurred in fewer countries over the past year. Collaborative investigations into the purveyors of surveillance software have resulted in growing awareness of an underregulated industry that continues to target state officials, journalists, activists, and members of diaspora communities. Whistleblowers have done the public a great service by exposing the inadequacies and failures of influential technology companies.

Democratic leaders should recommit to preserving the benefits of a free and open internet. True resilience requires new regulations that enshrine protections for human rights in the digital age, stronger multilateral coordination on cybercrime and corporate accountability, and deeper investment in civil society, which so often drives collective action to defend internet freedom and resist digital authoritarianism.

# Tracking the Global Decline

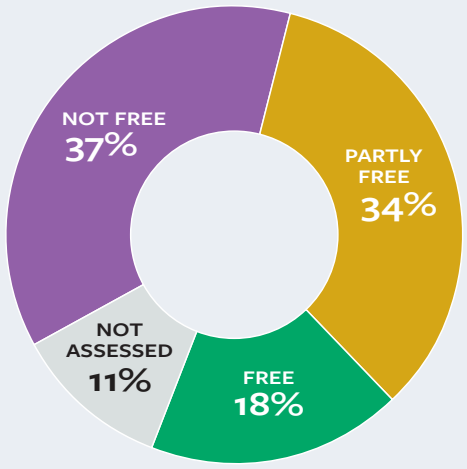
A rundown of prominent changes to countries' internet freedom scores

Global internet freedom has declined for the 12th consecutive year. The environment for human rights online deteriorated in 28 countries, though 26 countries registered net gains—the largest number of improvements since the inception of the project. The sharpest decline occurred in Russia, followed by Myanmar, Sudan, and Libya, while The Gambia and Zimbabwe experienced major improvements. The United States ranked ninth overall, and Iceland was once again the top performer. For the eighth consecutive year, China was found to have the worst conditions for internet freedom.

*Freedom on the Net* is an annual study of human rights in the digital sphere. The project assesses internet freedom in 70 countries, accounting for 89 percent of the world's internet users. This report, the 12th in its series, covered developments between June 2021 and May 2022. More than 80 analysts and advisers contributed to this year's edition, using a standard methodology to determine each country's internet freedom score on a 100-point scale, with 21 separate indicators pertaining to obstacles to access, limits on content, and violations of user rights. The *Freedom on the Net* website features in-depth reports and data on each country's conditions.

### GLOBAL INTERNET POPULATION BY 2022 FOTN STATUS

*Freedom on the Net* assesses 89 percent of the world's internet user population.




## The Kremlin's invasion of Ukraine puts internet freedom under threat

Internet freedom in Russia declined by seven points in the period surrounding the government's brutal invasion of Ukraine in February 2022, reaching an all-time low and representing this year's largest national decline in *Freedom on the Net*. Within weeks of the invasion, the Kremlin blocked Facebook, Instagram, and Twitter, depriving Russians of access to reliable information about the war and limiting their ability to connect with users in other countries. The government also blocked more than 5,000 websites, compelled media outlets to refer to the invasion as a "special military operation," and introduced a law prescribing up to 15 years in prison for those who spread "false information" about the conflict. The regime's increasing restrictions, both before and after the invasion was launched, significantly raised the risks associated with online activism and hastened the closure or exile of the country's remaining independent media outlets.

The Russian military's actions in Ukraine also undermined that country's internet freedom. In the southern city of Kherson, Russian troops forced service providers to reroute internet traffic through Russian networks during the spring and summer of 2022, leaving Ukrainian users without access to major social media platforms and a plethora of Ukrainian and international news sites. Though online media outlets have bravely continued to cover the invasion, their reporters faced great danger while carrying out their work. Several journalists affiliated with such websites were killed by Russian forces.

Internet freedom in Russia reached an all-time low following the government's brutal invasion of Ukraine.

The Ukrainian government and people have shown astonishing resilience during the invasion. Government officials and telecommunications companies worked together to repair internet infrastructure and ensure access to online resources and information, which can be life-saving in the midst of an armed conflict. Some 11,000 Starlink stations were deployed to provide satellite-based internet service as part of a collaboration involving the government, the US technology firm SpaceX, and other partners. Ukrainian telecom operators also enabled users to switch between carriers when their primary carrier's signal was unavailable, and they undertook major efforts to deliver Wi-Fi access to bomb shelters. Immediately after Russian forces invaded the country, the Ukrainian company Ajax Systems collaborated with the government to launch a mobile application—downloaded more than four million times as of March—that alerts users about incoming air raids.

## Coups and elections drive major declines and improvements

Internet freedom declined by five points in Myanmar, contributing to a precipitous 19-point decline over the past two years. The country now hosts the second worst environment for human rights online, outperforming only China. Since the military junta seized power from an elected civilian government in February 2021, it has cemented its censorship regime, blocking all but 1,200 websites, restricting access to major social media platforms, and imposing local internet shutdowns. The few online resources that remained accessible during the year were dominated by promilitary voices, and activists, journalists, and ordinary users continued to be forcibly disappeared, detained, and tortured. The junta compelled the Norwegian service provider Telenor to sell its operations in the country to a military-aligned company, fully consolidating its control over the telecommunications sector.

Russian police officers run toward a man holding a poster that reads "No War" during an unsanctioned protest at Moscow's Manezhnaya Square in front of the Kremlin on March 13, 2022. Hundreds of people were detained during the rally. (*Photo by Contributor/Getty Images*)

A man holds a poster featuring Hungarian Prime Minister Viktor Orban with an anti-surveillance message during a protest in Budapest, Hungary, on July 26, 2021. (*Photo by Marton Monus/Reuters*)

Sudan's score fell by four points after military leaders staged a coup and dissolved the country's transitional government in October 2021, marking a devastating setback for Sudanese democracy. The military voided articles of the interim constitution that protected fundamental rights and declared a state of emergency that lasted until May 2022. As Sudanese civilians mobilized mass protests in response, authorities restricted internet connectivity, blocked social media platforms, and assaulted and arrested journalists.

Internet freedom in Nicaragua dropped by three points amid an election in November 2021 that featured a harsh clampdown on opposition leaders, dissidents, and independent journalists. Repressive legislation such as the Cybercrime Law paved the way for increased self-censorship and lengthy prison sentences against critical users.

In Hungary, the status of internet freedom declined from Free to Partly Free, mirroring the country's broader democratic decline under the leadership of Prime Minister Viktor Orbán. During opposition primary elections in September and October 2021, in which voters chose candidates to challenge Orbán and his ruling party, cyberattacks from unknown sources plagued electronic voting systems and independent news outlets in the country.

Election organizers were forced to suspend voting after their computer system suffered an attack, and independent news sites were taken offline before the announcement of electoral results. Months earlier in July, an investigation revealed that at least three journalists had been targeted with Pegasus, an infamous spyware tool developed by the Israeli firm NSO Group.

In The Gambia, internet freedom improved by three points, contributing to a 23-point improvement since the end of former president Yahya Jammeh's repressive regime in 2017. Gambians mobilized online without restriction during the December 2021 presidential election, in which incumbent Adama Barrow secured a second term. The Barrow administration also passed a landmark law guaranteeing the right to public information, an important step for transparency and accountability.

## New and persistent threats to free expression worldwide

*Freedom on the Net* found that officials in at least 53 countries charged, arrested, or imprisoned internet users in retaliation for posts about political or social causes. In Libya, which suffered this year's third-largest score decline alongside Sudan, users who shared criminal commentary or reporting online have been forcibly disappeared before reemerging in detention. Rwandan authorities sentenced a YouTube commentator whose videos criticized the government to 15 years in prison in September 2021.

Authorities in at least 40 countries blocked social, political, or religious content online, an all-time high in *Freedom on the Net*. Internet users in Jordan reported that the website of the International Consortium of Investigative Journalists was briefly blocked in October 2021, after the organization published leaked financial documents that exposed the secret wealth of the country's king and other world leaders. In Belarus, authorities blocked the websites of civil society organizations throughout the coverage period, part of a wholescale assault on the groups that included raids, arrests, and forced closures.

In at least 22 countries, government officials blocked access to social media or communications platforms. Some blocks were imposed to coerce the companies into compliance with requirements that they open in-country offices, store data within the country, or otherwise change their operations in ways that facilitate enforcement of government censorship or data requests. In Uzbekistan, authorities blocked a range of international social media and messaging apps in July and November 2021 on the grounds that they failed to comply with localization requirements in a data protection law; access to most platforms was restored by August 2022. In March 2022, a judge on Brazil's Supreme Court reversed an order that would have banned Telegram, after the app agreed to remove content that was flagged as disinformation and announced that it would appoint a local representative. Nigerian officials rescinded a seven-month block on Twitter in January 2022, claiming that the company had agreed to establish a physical presence in the country.

> Progress in "swing states" like Brazil and India could ensure the survival of a free and open internet, or they could join authoritarian powers in promoting cyber sovereignty.

## The future of internet freedom in "swing states"

Countries including Brazil and Nigeria are often referred to as swing states due to their potential regional or global influence over the future of internet governance. They have oscillated between protecting and undermining human rights online, with many ranked Partly Free by *Freedom on the Net*. Progress in these countries could ensure the survival of a free and open internet, or they could join authoritarian powers in promoting the more closed model of cyber sovereignty.

Democratic institutions in some swing states intervened to protect human rights online during the coverage period. The Indian Supreme Court ordered the government to reevaluate the country's colonial-era sedition law, which has increasingly been used to charge online dissidents, in May 2022—even as political leaders sought to extend control over online content through problematic new legislation. Brazilian lawmakers enshrined the protection of personal data in the constitution in February 2022, a landmark action that elevated privacy rights above the whims of any government or simple legislative majority. But the decision came amid a contentious election year, in which President Jair Bolsonaro and his allies have bombarded the online space with false claims about electoral fraud. In October 2021, Kenya's highest court paused the implementation of an expansive biometric identity-card system until it could meet appropriate standards for data protection. President Guillermo Lasso of Ecuador vetoed provisions of a law that criminalized the disclosure of secrets online in June 2021, protecting digital media outlets from a serious legal threat.

Other countries in this group pursued practices that increased digital repression and undermined the diversity of the information space. In Tunisia, President Kaïs Saïed suspended parts of the constitution, imposed overly broad rules barring what the state deems to be "false" information, and oversaw the arrest of his online critics—an alarming turn for the country with the Arab world's highest internet freedom score. Indonesian authorities briefly blocked several websites after the coverage period, including Yahoo and PayPal, to force compliance with a repressive law that

## GLOBAL INTERNET USER STATS

Over **4.5 billion** people have access to the internet.

### According to Freedom House estimates:

**76%** live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues.

**69%** live in countries where authorities deployed progovernment commentators to manipulate online discussions.

**64%** live in countries where political, social, or religious content was blocked online.

**64%** live in countries where individuals have been attacked or killed for their online activities since June 2021.

**51%** live in countries where access to social media platforms was temporarily or permanently restricted.

**44%** live in countries where authorities disconnected internet or mobile networks, often for political reasons.

For the eighth consecutive year, China remained the world's worst environment for internet freedom.

requires companies to register with the government, appoint a local liaison, and remove content under tighter timelines.

## The world's most repressive online environment

For the eighth consecutive year, China remained the world's worst environment for internet freedom. Content related to the 2022 Beijing Olympics and the COVID-19 pandemic remained heavily censored during the coverage period, particularly as Shanghai residents shared their experiences amid a disastrous two-month lockdown that began in April 2022. The government also intensified censorship of online content related to women's rights and suppressed social media campaigns against sexual assault and harassment, including through the detention of tennis star Peng Shuai after she alleged on the social media platform Weibo that she was sexually assaulted by senior CCP official Zhang Gaoli. Separately, journalists, human rights activists, members of religious and ethnic minority groups, and ordinary users were detained for sharing online content, with some facing harsh prison sentences.

Government officials instituted new policies to tighten their control over Chinese technology companies. The main internet regulator issued guidance requiring platforms to align their content moderation and recommendation systems with "Xi Jinping Thought"—the official ideology of the current CCP leader. Another set of draft rules would impose heavy penalties on companies that enable Chinese internet users to bypass the Great Firewall. Meanwhile, the country's data protection framework, which took effect in November 2021, established baseline safeguards for personal data held by Chinese companies—though it failed to apply the same standards to data held or requested by the government.

## For the United States, progress abroad and stalemate at home

The administration of US president Joseph Biden made the promotion of internet freedom a top priority of its foreign

The lack of a comprehensive privacy law and incomplete reforms to surveillance rules have allowed government agencies to simply purchase Americans' data from shadowy brokers.

policy. In April 2022, the White House helped bring together more than 60 governments to sign the Declaration for the Future of the Internet, a nonbinding agreement to advance a positive vision of the internet. The US State Department established its Bureau of Cyberspace and Digital Policy, helped launch the Export Controls and Human Rights Initiative, and revealed that it would chair the Freedom Online Coalition in 2023. Similarly, the US Agency for International Development announced an investment of up to $20 million annually to dramatically expand its digital democracy work.

This flurry of activity on the global stage stood in stark contrast to the lack of movement at home. While internet freedom improved for the first time in six years, the change was marginal, and proposed laws that would strengthen human rights online and increase tech-related transparency made little progress. The continued lack of a comprehensive federal privacy law and incomplete reforms to surveillance rules have allowed government agencies to simply purchase Americans' data from shadowy brokers with little oversight or safeguards. The Supreme Court decision that overturned *Roe v. Wade* and denied a constitutional right to abortion also prompted renewed concerns about law enforcement access to location information, browsing histories, and other forms of data that could be used for criminal and civil investigations in US jurisdictions where legal access to reproductive health care is restricted.

During the coverage period, mass denial of the outcome of the 2020 presidential election by former president Donald Trump and his supporters, driven in part by online conspiracy theories and disinformation, polluted the information environment and seeped into the broader American political system. Election deniers have leveraged online support to mount viable candidacies for public office ahead of the November 2022 midterm balloting. Disinformation about stolen elections and supposed vulnerability to fraud has fueled calls for citizens to "protect" the vote by force if necessary. Election workers and administrators have reported receiving a barrage of online threats and harassment, leading large numbers of them to resign out of fear for their own safety. In effect, such disinformation and intimidation have undermined the basic security of US electoral mechanisms, provided Republican Party leaders in many states with a false justification for new antifraud measures that could restrict access to voting or distort the counting and certification processes, and set the stage for future unrest by eroding public trust in any unfavorable results.

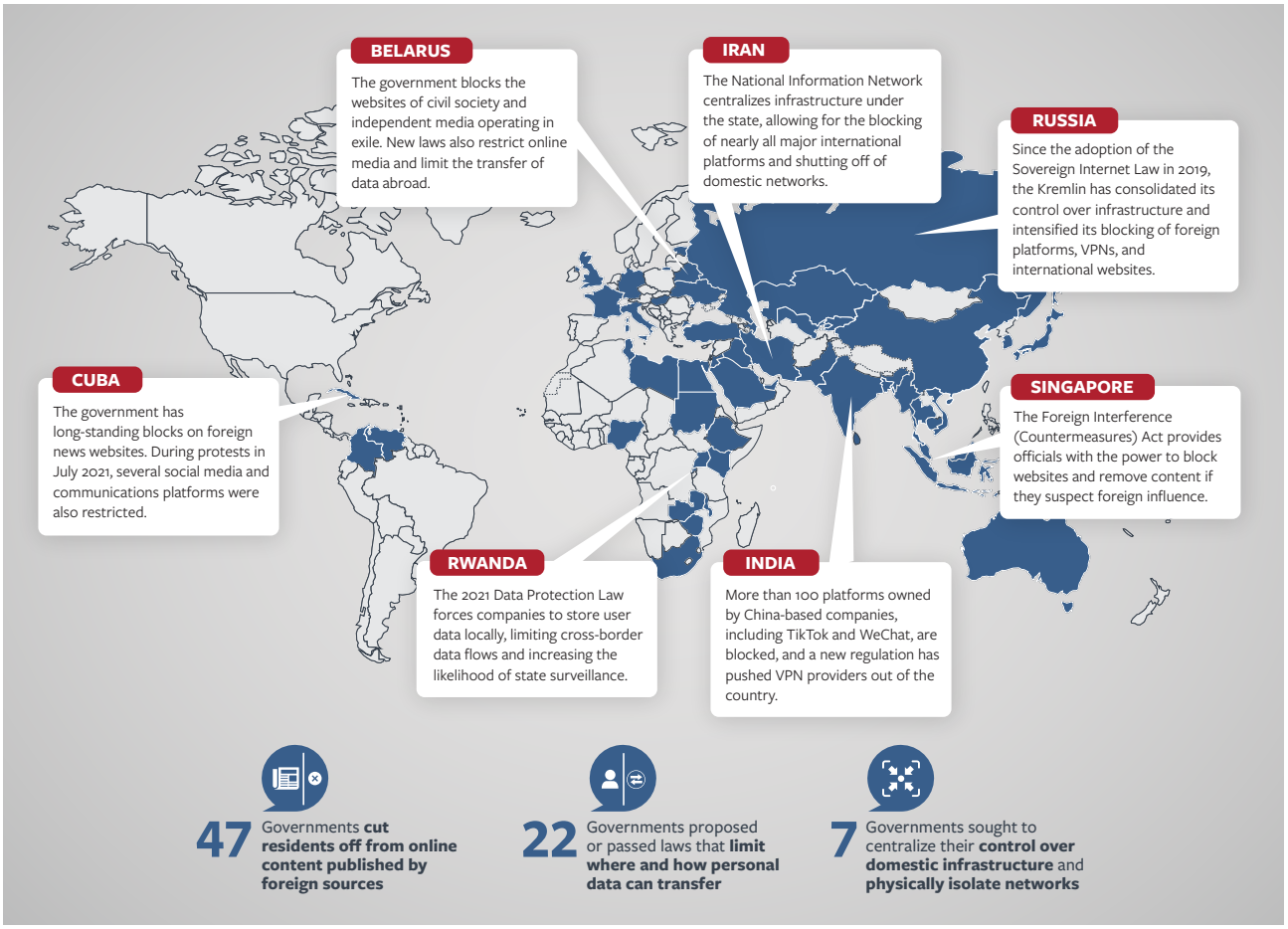
# The Shattering of the Global Internet

The internet is more fragmented than ever, preventing billions of people from exercising their human rights online. Authorities in over two-thirds of the countries surveyed in this report have used their legal and regulatory powers to limit access to foreign information sources, leaving residents in a domestic information space that is effectively shaped by the state. More governments are also passing legislation that places guardrails around the flow of user data across borders, with mixed consequences for the global internet and human rights. The most perilous laws purport to protect privacy even as they delegate oversight to regulators beholden to the political leadership or force data to be stored in less secure settings.

Few if any countries have taken the extreme step of disconnecting entirely from the global internet on a technical level. But a small number of authoritarian leaders are following the CCP in reengineering their domestic networks to allow greater control over technical infrastructure. Their success remains constrained by the daunting economic and

## A GLOBAL INTERNET SPLINTERED INTO PIECES

More governments are creating barriers to the flow of information across national borders.



societal costs of such measures, as well as the endurance of international norms supporting an open global internet.

The myriad of national regulations and practices that contribute to fragmentation—intentionally or not—are being imposed by governments across the democratic spectrum, but there are crucial distinctions. Authoritarian regimes in countries such as China, Iran, and Russia are seeking to wall their people off from the rest of the world. More democratic measures typically seek to enforce rights-protecting legislation that addresses abusive company behavior or genuine online harms. Though accomplished through state intervention, these policies are often paired with safeguards that allow for the continued flow of information and services across borders, so long as partners ensure a similar level of protection for users' rights.

## Isolating users from outside information

In response to both real and purported threats online, authorities in at least 47 countries cut residents off from the flow of news and information across borders. Some governments alleged foreign meddling to justify new censorial regulations, while others imposed localized shutdowns of internet service, plunging users into digital darkness in a bid to suppress information about human rights abuses. In tandem with this censorship, many political leaders bolstered support for state-aligned social media platforms that are more receptive to their demands.

The restrictions were largely imposed in countries that are designated as Not Free or Partly Free by *Freedom in the World*, demonstrating the extent to which both entrenched and aspiring authoritarian leaders rely on information controls to retain power. It is during perilous moments of political transition and possible transformation—such as protests, elections, and conflicts—that censorship of foreign information tends to intensify.

### *Blocking access to international websites, social media platforms, or the internet as a whole*

Authorities increasingly cut off domestic users from websites and social media platforms that serve international audiences. These national restrictions have a global impact, limiting connections to family members in other countries and the diaspora communities that use digital technologies to stay in touch with their countries of origin.

Since the February 2021 coup, Myanmar's military junta has cultivated a domestic intranet to help silence opposition to its takeover and consolidate its power. Residents can only access an estimated 1,200 websites and platforms through mobile connections. Facebook and Twitter—both popular with anticoup protesters and key tools for communicating with allies abroad—remain inaccessible. The junta has also imposed shutdowns of internet service in towns across the country, often coinciding with military offensives against ethnic militias, armed prodemocracy groups, or communities that are suspected of supporting them. In practice, these restrictions have limited the sharing of evidence of human rights abuses with external audiences, forced residents to rely on military-dominated information sources, and helped to contain civic mobilization and dissent.

In Ethiopia, internet access has been restricted in the Tigray Region since November 2020, when armed conflict broke out between the federal government and forces associated with the Tigrayan People's Liberation Front. The shutdown has prevented people in Tigray from sharing their stories and reporting on actions by combatants that human rights groups have described as mass atrocity crimes, limiting opportunities for accountability and global solidarity. Similarly in July 2021, as Cubans mobilized the largest antigovernment demonstrations in the country since the 1959 revolution, the authorities briefly restricted internet access and blocked WhatsApp, Telegram, and Signal. These steps prevented protesters from effectively using digital tools to coordinate protests, and they separated the movement from independent news outlets and Cubans based abroad, who had rallied support for the demonstrations on international social media platforms.

While the vast majority of governments that limited access to foreign content did so to maintain their own power or thwart accountability, a notable exception came from the EU. Brussels ordered each member state's telecommunications providers to block the websites of the Russian state media services RT and Sputnik. These sites certainly promote incendiary and false content, and international human rights standards permit limits on free expression under specific circumstances including armed conflict. However, the EU's broad ban restricted all content from these sites rather than more narrow information related to the war. It also lacked clear sunset provisions and was imposed without adequate oversight, transparency, and consultation with civil society and telecommunications companies. The EU's insufficient clarity and specificity left companies scrambling to determine how to comply, leading to uneven blocking among member

states. Furthermore, the ban set a flawed precedent for how democracies could respond to problematic information disseminated by other foreign state-owned news outlets, such as those based in Beijing.

### *Targeting circumvention technology*

Journalists, activists, and ordinary users in many countries have flocked to circumvention tools like virtual private networks (VPNs), which allow them to use the internet safely and anonymously while bypassing some forms of state censorship. In response, governments are increasingly blocking, criminalizing, or imposing regulatory requirements on the circumvention tools themselves.

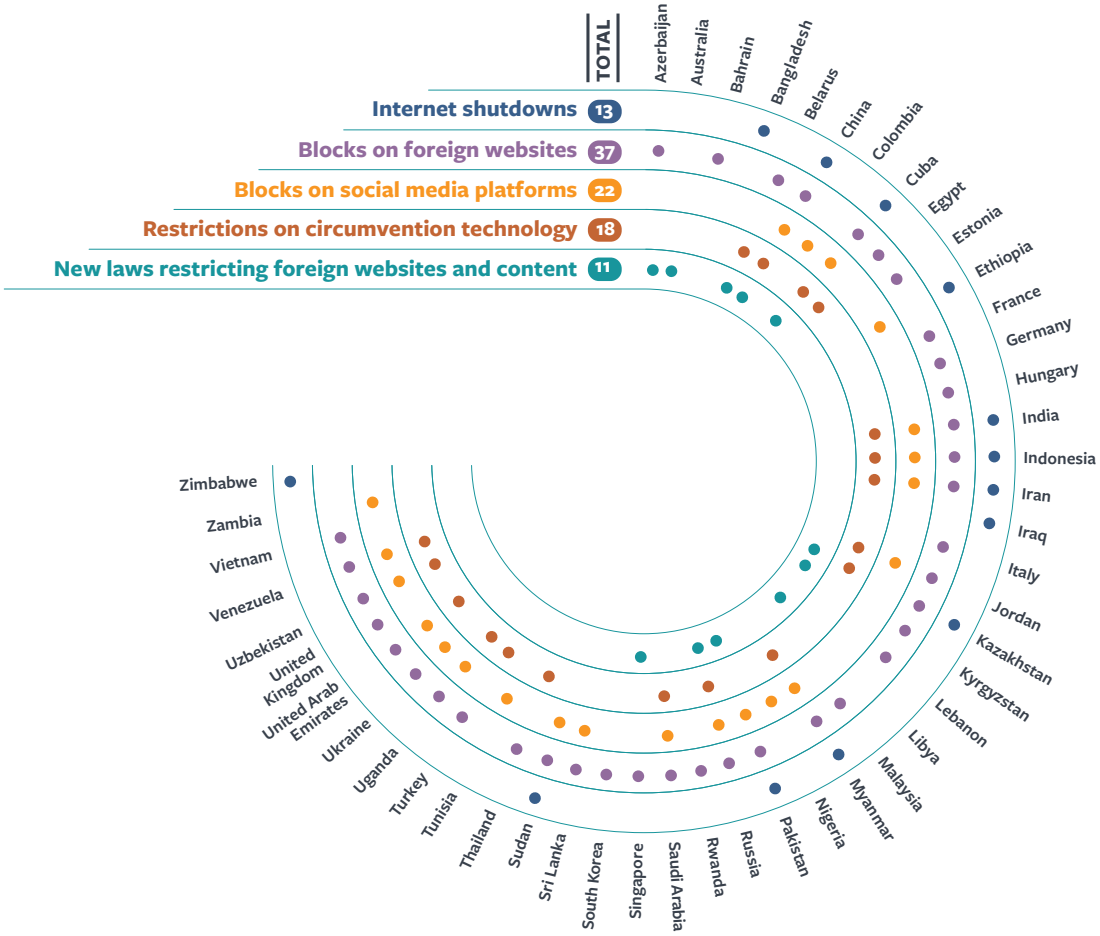
Blocks on circumvention technology escalated in moments of political tension during the coverage period, when access to the uncensored international internet would have boosted those seeking to change the balance of power. During Venezuela's November 2021 regional elections, in which opposition parties sought to challenge the authoritarian rule of Nicolás Maduro, service providers blocked VPNs and the anonymous web browser Tor, presumably on government orders, in addition to widespread blocking of international and independent Venezuelan media sites. Venezuelan internet users were cut off from critical information, particularly the reports of foreign media and election-monitoring groups.

In India, new regulatory requirements for VPN providers were introduced amid government censorship demands targeting US-based technology companies as well as a two-year block on communications platforms owned by China-based companies, including TikTok and WeChat. The VPN services will be required to maintain subscriber records, such as names and IP (internet protocol) addresses, for five years and furnish them to the government on request, with steep fines for noncompliance. International providers TunnelBear and Norton have since made their services unavailable to users in India. In nearby Myanmar, security officials have reportedly employed cruder tactics to deter people from using the technology: they have arbitrarily searched civilians' phones for evidence of VPNs, detaining individuals who are found to have downloaded them.

Cuban citizen Rolando Remedios displays a photo of his arrest, which took place during the widespread protests that occurred on the island in July 2021. (*Photo by Yamil Lage/AFP*)

## COUNTING THE WAYS GOVERNMENTS PLUNGE USERS INTO DARKNESS

In over two-thirds of countries covered by *Freedom on the Net*, authorities limited access to foreign information sources using at least one form of censorship.




### *Exploiting fears of foreign interference to inhibit independent media*

Authorities also invoked the specter of foreign interference to expand censorship of websites based abroad or those that receive foreign funding. Website owners or journalists living outside a given country often have more leeway to resist government pressure and produce unfettered reporting. By requiring websites and related companies to be based domestically or to accept only domestic funding, a state can enhance its capacity to control the local information space.

In October 2021, Singapore's government added the Foreign Interference (Countermeasures) Act (FICA) to its formidable arsenal of censorship powers. In the name of preventing foreign meddling in domestic politics, FICA authorizes officials to block websites and order social media companies and other sites to remove speech if they suspect that the content in question was influenced by a foreign actor. A regulatory body suspended the license of the citizen news site *The Online Citizen* within a day of the bill's introduction in Parliament, citing concerns about foreign funding.

A restrictive Azerbaijani media law that was adopted in February 2022 limits the foreign funding that media—defined broadly to include both news outlets and individuals—can accept and requires media operators to be based in the country. The law further clamped down on what was already a tightly controlled online media environment, with many Azerbaijani journalists forced to operate from abroad to avoid state persecution.

### *Propping up state-aligned and state-owned alternatives to international platforms*

Even as they increased pressure on foreign platforms over the past year, many repressive governments promoted pliant domestic alternatives as part of a strategy to create a siloed and politically tamed information environment. If users migrate to state-aligned platforms, the domestic political costs of blocking international services would be reduced, facilitating further fragmentation.

In China, the government has been fairly successful in pairing systematic censorship of foreign services with robust investment in domestic platforms that are beholden to the ruling party. A more diverse social media market, including the development of smaller and more local platforms that meet the needs of a particular community, is sorely needed around the world. But companies owned by or with close ties to authoritarian governments are more likely to censor unfavorable content and become vehicles for state disinformation than their counterparts based in more democratic contexts. These so-called parallel platforms are often less transparent in their operations and policies, and they may be better shielded from civil society advocacy, media investigations, and other forms of public scrutiny.

Moscow's strategy to reduce reliance on foreign social media companies includes a requirement that mobile phones carry preloaded domestic apps. Following the invasion of Ukraine in February 2022, blocks on Facebook, Twitter, and Instagram drove users to VK and Odnoklassniki, both run by a parent company that is partly owned by Kremlin allies. Yandex, a popular Russian search engine and rival of Google, reportedly prioritized disinformation narratives and downgraded the search results for sites that criticized the invasion. In 2022, in a bid to win larger user bases for Russian platforms, authorities reportedly offered influencers monthly payments if they switched to RuTube and Yappy, in lieu of YouTube and TikTok, and toed the government's editorial line.

The push toward domestic platforms often followed explicit or implicit attacks on the credibility of international platforms, further undermining trust in the global information space. In Turkey, many state agencies flocked to the WhatsApp alternative BiP in 2021, after the Meta-owned app introduced a problematic privacy policy update. BiP is owned by the mobile operator Turkcell, which the state's sovereign wealth fund controls. The platform has a growing user base in Bangladesh, Indonesia, Pakistan, and Bahrain.

## Increasing barriers to the cross-border flow of user data

In at least 22 countries covered by *Freedom the Net*, laws that limit where and how personal data can flow were proposed or passed during the coverage period. The affected countries span the democratic spectrum, including examples that are ranked Free, Partly Free, and Not Free by *Freedom in the World*. The transfer of data across jurisdictions is central to the functioning of the global internet and benefits ordinary users, including by improving internet speeds, enabling companies to provide critical services worldwide, and allowing the storage of records in the most secure data centers available.

As policymakers impose necessary privacy laws that safeguard sensitive information from commercial abuse, they may unintentionally drive fragmentation by creating a barrier between their own countries and those without similar standards. The ensuing patchwork of regulations could incentivize companies, particularly newer or smaller services, to concentrate their growth in certain countries, resulting in less diverse online ecosystems for users elsewhere.

The EU's 2018 General Data Protection Regulation (GDPR) permits the transfer of personal data only to jurisdictions with a sufficient level of protection in place. As more governments pursue laws that appear to align with GDPR standards, some have buried problematic obligations that either mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes. Such contradictory "data washing" measures ultimately fail to strengthen privacy and further fragment the internet.

In August 2021, the Chinese government passed a data protection law that regulates the commercial use of personal data, creating an important set of guarantees for the country's billion internet users. But the law does not restrict the government's misuse of data, and it mandates domestic data storage for some companies, opening the door to further state intrusion and exploitation and imposing additional onerous barriers on the flow of personal data.

In Rwanda, a data protection law passed in October 2021 requires companies to store data in the country unless

otherwise authorized by the country's cybersecurity regulator, rather than an independent data protection agency that is more insulated from law enforcement bodies. This localization clause leaves personal data vulnerable to abuse, particularly given that authorities have embedded agents in telecommunications companies for surveillance purposes and prosecuted dissidents based on their private messages.

Though modeled on the GDPR, the United Arab Emirates' new data protection law, in effect since January 2022, exempts government entities tasked with processing personal data from complying with baseline safeguards. While its constraints on commercial data access are welcome, the law leaves the privacy of residents at risk: authorities in the country still have sweeping powers to monitor communications and seize data from service providers.

## Breaking away from global infrastructure

Governments in at least seven countries, all of which are ranked Not Free in *Freedom in the World*, sought to centralize state control over domestic infrastructure and physically isolate their networks from the global internet during the coverage period. This form of fragmentation may be the least prevalent due to the exceptionally advanced technical and administrative capacities that it requires. It also entails considerable political will: infrastructural isolation presents economic costs to businesses operating domestically, can significantly slow down connection speeds, and deepens the risk to human rights. These challenges help explain why political leaders in countries with robust civic spaces, thriving technology sectors, and more pluralistic governance systems are less likely to impose such barriers.

The CCP and state-linked companies have cultivated the most sophisticated model of cyber isolation. Internet traffic from outside the country passes through centralized, state-controlled chokepoints, facilitating mass blocking, filtering, and surveillance. Following Beijing's path, the Iranian government has imposed state barriers between the local infrastructure and global traffic. In July 2021, authorities introduced the User Protection Bill to bolster the country's National Information Network, which has facilitated the restriction of access to international platforms and connections while directing users to domestic alternatives. The law would place the country's internet gateways under the authority of a working group that includes military and intelligence agencies.

> Fragmentation at the national level is part of a global battle for control over the internet.

The Russian government hastened its own progress toward infrastructural isolation over the past year. During a series of tests in June and July 2021, authorities claimed to have successfully separated the so-called RuNet from global connections, though technical experts remain skeptical. In April 2022, following his invasion of Ukraine, President Vladimir Putin appointed an interagency commission to pursue his goal of technical isolation.

The Cambodian government planned to route all international and domestic internet traffic through a single portal, dubbed the National Internet Gateway (NIG). This centralized chokepoint would allow authorities to censor content from around the world and surveil residents more easily. Cambodian officials unexpectedly delayed the NIG's implementation in February 2022, citing the COVID-19 pandemic and issues related to licensing and equipment installation. The decision came after extensive opposition to the NIG from the private sector, civil society, and experts at the United Nations.

## The competition to control the web

Fragmentation at the national level is part of a global battle for control over the internet. Led by Beijing and Moscow, diplomats from authoritarian countries have promoted their model of cyber sovereignty at multilateral institutions. As secretary general of the ITU, China's Houlin Zhao encouraged a shift of control over the setting of technical standards away from multistakeholder bodies, where civil society and other nongovernmental experts have more sway, and toward the ITU itself, where only governments have input.

During Zhao's tenure, in 2019 and 2020, the Chinese telecommunications giant Huawei introduced the New IP proposal, a plan to fundamentally alter the interoperability of the global internet's infrastructure by redesigning common protocols to facilitate greater state control over domestic networks. While initially voted down by ITU members, rebranded elements of the proposal have since reemerged

Zhao Houlin, secretary general of the International Telecommunication Union, speaks during the opening ceremony of 2021 World 5G Convention in Beijing in August 2021. (*Photo by VCG via Getty Images*)

in standards-setting bodies. Chinese officials also launched in July 2022 the World Internet Conference International Organization in Beijing, intended to serve as a "shared" global community that would determine technical standards and governance. The organization, stemming from an annual meeting of the same name that was first held in 2014, could create a new forum in which the Chinese government can promote and incentivize other governments to adopt its authoritarian model of digital control.

The Russian government has similarly leveraged international institutions to influence internet governance. At the United Nations in February 2022, negotiations began for a new cybercrime treaty, which was initially proposed by Russian diplomats and cosponsored by representatives from Belarus, Cambodia, China, North Korea, Myanmar, Nicaragua, and Venezuela—all ranked Not Free by *Freedom in the World*. Civil society has resoundingly condemned the proposed treaty as a new vector for digital repression. Moscow also joined Beijing in June 2021 to call for a more powerful ITU and endorse the right of each state to control its own "national segment of the internet." One Russian official explained the need for a more forceful version of the agency by claiming that the multistakeholder model of governance was "ineffective."

### *Democratic states step up globally*

Some democratic leaders have revived efforts to shape global digital standards that uphold fundamental freedoms, creating a much-needed counterweight to authoritarian efforts. After allowing ITU secretary general Zhao to run unopposed in 2014 and 2018, Washington nominated Doreen Bogdan-Martin to seek the post, and she defeated a candidate backed by Moscow in a September 2022 vote by member states. Two US-led initiatives, the Summit for Democracy and the Declaration for the Future of the Internet, have sought to solidify common norms as a basis for further action. Moreover, the United States has pledged to strengthen and expand the Freedom Online Coalition in its upcoming role as chair in 2023.

## PUTTING THE GLOBAL INTERNET BACK TOGETHER

Policymakers, regulatory bodies, and other state agencies should take broad action to protect human rights in the digital age.


Across the Atlantic, the EU and its member states have taken similar action. The Copenhagen Pledge on Tech and Democracy, led by the Danish government, uses a multistakeholder format by inviting governments, multilateral bodies, civil society, and the private sector together to protect human rights in the digital age. Separately, the EU's Digital Services Act (DSA) is a promising alternative to more censorial regulatory approaches and could serve as a global model. It strengthens transparency, limits advertising systems, and requires large platforms to provide data to independent researchers and organizations, which can then lead to more innovative and effective responses to online harms. The DSA also institutes a more inclusive coregulatory form of oversight and enforcement, including by using independent third-party auditors to review compliance, which can limit the risk of abuse.

However, the DSA framework features a problematic "notice-and-action" provision for companies to remove speech that is deemed illegal by EU authorities or member states, which could be abused to silence political, social, and religious speech. To limit this risk, Brussels and member states should clearly define and harmonize their definitions of what constitutes "illegal" speech in keeping with international law, and ensure that independent judicial authorities oversee any removal of content.

### *Harmonizing data protection to create a race to the top*

Greater policy coordination among democracies is vital to the protection of a free and open internet. In a promising sign from April 2022, the governments of Canada, Japan, the Philippines, Singapore, South Korea, Taiwan, and the United States established the Global Cross-Border Privacy Rules Forum to bridge regulatory discrepancies and promote the free flow of data under what it determines as "best practices" for data protection. The EU and the United States also made progress during the coverage period following the European Court of Justice's invalidation of the EU-US Privacy Shield framework in 2020, a ruling that limited transatlantic data flows due to concerns about US national security surveillance programs. In March 2022, the transatlantic partners announced an agreement on Privacy Shield 2.0, set to be formalized in late 2022, that includes a redress mechanism for EU residents who are concerned about privacy violations as well as new privacy commitments by US intelligence agencies.

Governments also proposed, passed, or began enforcement of data protection laws that are compatible with rights-respecting provisions from existing international frameworks, a practice that can minimize the effects of fragmentation. South Africa's data protection law, which entered into full force in July 2021, was drafted to harmonize with parts of the GDPR, as was Sri Lanka's, which passed in March 2022. Both laws put limits on the transfer of personal data across borders except in certain cases, including transfers to a country with adequate safeguards. Protecting privacy does not necessarily require limiting the physical location of data storage. For instance, the proposed American Data Privacy and Protection Act in the United States avoids focusing on where data can be transferred and instead adopts a data minimization approach that limits what can be collected, how it can be stored, and with whom it can be shared.

> Greater policy coordination among democracies is vital to the protection of a free and open internet.

### *Resisting internet fragmentation while protecting human rights*

The values of human rights and open societies are mutually reinforcing. When implementing rights-protecting laws, governments should seek to reduce friction by coordinating their efforts across borders and aligning them with international frameworks whenever possible. Ultimately, democratic officials, technology companies, and global civil society groups should aim to empower individuals to play a greater role in making online spaces more free, secure, and inclusive. This is the best way to ensure that human rights are upheld in the digital age.

# A Resilient Internet for a More Democratic Future

Twenty-six countries experienced net improvements in internet freedom over the past year, the highest such figure since the inception of *Freedom on the Net*. Though digital repression is undoubtedly becoming more sophisticated and entrenched into everyday life, responses from governments, civil society, and the private sector are beginning to yield results.

*Freedom on the Net* has identified proven strategies that marshal the structures, tools, and expertise necessary to prevent or address illiberal uses of technology by both domestic and foreign actors, as well as the broader societal harms that the internet often exacerbates. Some strategies provide short-term responses to instances of repression, while others build long-term mechanisms for accountability, governance, and oversight that can stave off the advance of authoritarianism over time. These approaches vary in effectiveness depending on a country's political context: building digital resilience in a backsliding democracy and doing so under an entrenched authoritarian regime involve different sets of challenges. Collectively, however, such efforts have the potential to reverse the global decline of internet freedom.

While success requires the participation of a range of actors, civil society has always been at the forefront. Nonprofit organizations, media groups, and human rights defenders with roots in a given country or region have played a leading role in first identifying and raising awareness of a problem, often tirelessly over years, and then creating a strategy to address it, with assistance from others who can organize the requisite financial and political resources. Governments, philanthropic foundations, private companies, and others with an interest in cultivating a free and open internet that works for all of its users should do their utmost to meaningfully engage with civil society groups that are involved in the fight against digital repression and internet fragmentation, providing funding, technical expertise, capacity building, and other support to advance their work.

> Civil society has played a leading role in first identifying and raising awareness of a problem, and then creating a strategy to address it.

## Working with the judiciary

In at least 28 countries covered by this report, courts protected internet freedom. In many cases, problematic laws were struck down, creating precedents to guide future state actions. Court intervention appears to be the most effective at fighting censorship and surveillance in countries ranked Free or Partly Free by *Freedom in the World*, where judicial authorities remain independent from or somewhat resistant to political control. Efforts to protect internet freedom should prioritize strengthening the independence of courts and building their capacity to parse the legal and technical concepts that arise in cases involving human rights online.

In one positive example, the Zambian human rights organization Chapter One Foundation sued the country's communications regulator after it blocked social media platforms during the August 2021 presidential election. As a result of the legal action, the regulator signed a consent agreement, pledging not to act outside its legal authority and making a commitment to strengthen transparency regarding any future restrictions on telecommunications platforms.

In India, multiple civil society and media groups engaged in strategic litigation in response to the government's censorial Information Technology Rules, and in August 2021 a court halted the enforcement of problematic provisions in the regulations as part of a suit filed by an organization representing broadcasters. In a more recent case, Mexico's Supreme Court invalidated a biometric mobile-phone registry in April 2022, strengthening people's ability to communicate

anonymously online. The decision came after civil society activists argued that the registry facilitated widespread surveillance, made personal data less secure, and contributed to social inequalities.

## Pushing the private sector into action

In at least 30 countries over the past year, the private sector moved to protect internet freedom. In many cases, technology companies acted in response to civil society pressure, whistleblower testimony, and media scrutiny. Such cajoling can be necessary, as private-sector efforts to protect internet freedom have been inconsistent and affected by competing demands—including the mass collection of user data that forms the core business model of international social media platforms.

Following the Kremlin's invasion of Ukraine, tech companies scrambled to protect vulnerable users and avoid inadvertent support for a war of aggression. Google, Twitter, and Meta all limited the ability of Russian state media to monetize content across their platforms. They also rolled out new safety features to reduce online risks, such as Meta's expansion of end-to-end encryption for Instagram users in Russia and Ukraine and

### A MULTIPRONGED APPROACH TO SAFEGUARDING HUMAN RIGHTS ONLINE

Collectively, these strategies can help reverse the global decline of internet freedom.

its introduction of ephemeral messages on the Messenger application for those in Ukraine. Twitter launched a Tor Onion service, allowing users in Russia to access the platform safely and anonymously after it was blocked by the government.

Under public pressure, social media companies have pushed back on the Indian government's efforts to increase control over online speech. After broad condemnation from civil society about its compliance with state censorship, Twitter resisted government orders to restrict content, including posts from Freedom House, before finally acquiescing in June 2022 after a company employee was threatened with criminal charges. Twitter then took the case to the judiciary, filing a lawsuit in July 2022 that could rein in the government's broad assertion of censorship powers.

The private sector has sometimes partnered with civil society, government actors, and academia to design innovative responses to online harms. In Taiwan, which faces a barrage of disinformation that can be traced to China, the popular Japan-based messaging application Line worked with civil society groups to develop a tool for users to report false information when it trends on the platform. The Taiwanese government launched a similar coordination effort following the Russian invasion of Ukraine, aiming to track war-related disinformation emanating from China.

## Driving government policy changes to restore internet freedom

Policymakers, regulatory bodies, and other government agencies in at least 26 countries took steps to protect human rights online during the coverage period. These measures strengthened institutional safeguards for free expression, access to information, and privacy, and defended internet users from manipulative corporate practices. In some cases, government officials were reacting to targeted advocacy campaigns by civil society organizations; in others, their actions were an indirect outcome of long-term civil society efforts to shape the public discourse about policy and regulatory responses to disinformation, harassment, corporate malfeasance, and other harms online.

> A multipronged effort including strategic litigation, evidence-based research, multilateral and bilateral engagement, and targeted advocacy has changed the behavior of governments imposing shutdowns.

The Gambian government enacted legislation in July 2021 that affirmed a right to access public information, empowering journalists, civil society organizations, and ordinary citizens to hold the government accountable for its performance. The law was drafted using a multistakeholder model, with Gambian and international civil society and the private sector providing input.

In Armenia, domestic and international civil society groups combined public condemnation with private advocacy to persuade the government to repeal a criminal defamation clause that was originally passed in July 2021. The legislation, which criminalized serious insults of government officials and public figures, was invoked throughout the year to prosecute users who shared critical commentary, especially about Prime Minister Nikol Pashinyan. Civil society activists aired their concerns in private meetings with diplomats and in Armenian news outlets, and their objections were then cited in a formal appeal to the Constitutional Court. Government officials agreed to exclude the provision from a new criminal code that took effect in July 2022, and committed to broad consultation with nongovernmental groups when developing media-related laws in the future.

Civil society called on democratic policymakers to ensure that the sanctions they imposed in response to the Russian invasion of Ukraine did not impede critical internet access. In a March 2022 letter, more than 35 internet freedom groups and experts, including Freedom House, alerted President Biden to the dangers and unintended consequences of restricting internet services for users in Russia and Belarus. Weeks later, the Treasury Department exempted telecommunications services from US sanctions related to the invasion.

Independent regulators sought guidance from civil society and other experts on how best to prevent companies from undermining the rights of internet users. In August 2022, after the coverage period, the US Federal Trade Commission announced that it was accepting advice from the public about whether new rules were needed to protect US residents

from corporate data collection. Such rules could allow the regulator to mitigate harms in the absence of comprehensive privacy protections under federal law.

## Progress on internet shutdowns

Internet shutdowns have long been a core tactic of digital repression. But this may be changing: the *Freedom on the Net* subscore pertaining to government restrictions on internet connectivity improved in 13 countries, the largest number of gains for a single indicator across the 21-question methodology this year. During the coverage period, governments in 14 of the 70 countries assessed shut off or throttled fixed or mobile internet services, compared with 20 countries in the report's 2021 edition and 22 in the 2020 edition. In countries where shutdowns continue to occur, they appear to be more localized and temporary, affecting fewer people for less time than past restrictions.

The trend suggests that a multipronged effort including strategic litigation, evidence-based research, multilateral and bilateral engagement, and targeted advocacy has helped to change the behavior of governments imposing shutdowns. For instance, researchers have illustrated that shutdowns take a toll on local economies, and they have been shown to correlate with higher levels of violence, undermining the argument that they are necessary to maintain peace and security. Lawsuits filed by civil society groups, journalists, and others have led to judicial interventions against connectivity restrictions, most recently in India in 2022 and Sudan in 2021.

Proactive advocacy aimed at both governments and internet service providers has succeeded in preventing possible shutdowns ahead of major events. For instance, members of the #KeepItOn coalition—comprising more than 280 civil society groups, including Freedom House, and led by the digital rights group Access Now—mobilized ahead of Kenya's general elections in August 2022 and Iraq's parliamentary elections in October 2021 to urge officials to maintain connectivity. Kenyan officials fulfilled their public commitments to refrain from restricting internet access, and no disruptions to internet access were reported in Iraq, unlike during the 2018 elections.

Kenyans track results from the presidential election in August 2022. The Independent Electoral and Boundaries Commission (IEBC) chairman declared Deputy President William Ruto the winner after a tight race. (*Photo by Boniface Muthoni, SOPA Images/LightRocket via Getty Images*)

Disproportionate surveillance remains one of the most obvious problems affecting democracies' internet freedom performance.

This sustained advocacy has contributed to a consensus at the multilateral level that shutdowns are unjustifiable and disproportionate. A UN report, commissioned by the Human Rights Council and released in 2022 to the General Assembly, incorporated civil society and private-sector input to outline recommendations on how to limit such censorship. The Freedom Online Coalition called for the immediate end of shutdowns in July 2021, launching an internet shutdown task force to design best practices for advocacy. The Group of Seven governments also publicly agreed in 2021 to cooperate in opposition to shutdowns when they are "politically motivated," although they reportedly softened their language after objections from the Indian government, a global leader in connectivity restrictions.

## The path to stronger rights protections and a more resilient internet

The success of the collective effort against service shutdowns offers a model for tackling other critical problems that are driving digital repression and the fragmentation of the open internet. Strategies that build on the work of civil society to mobilize change in the courts, among governments, and at tech firms can yield better protections for human rights online on both a national and a global scale, particularly when they enlist multilateral and multistakeholder institutions. Without such campaigns, however, the internet is likely to grow more splintered, obstructing the exchange of diverse views and innovative ideas, constraining people's ability to organize for political and social causes, and severing cross-border connections between communities.

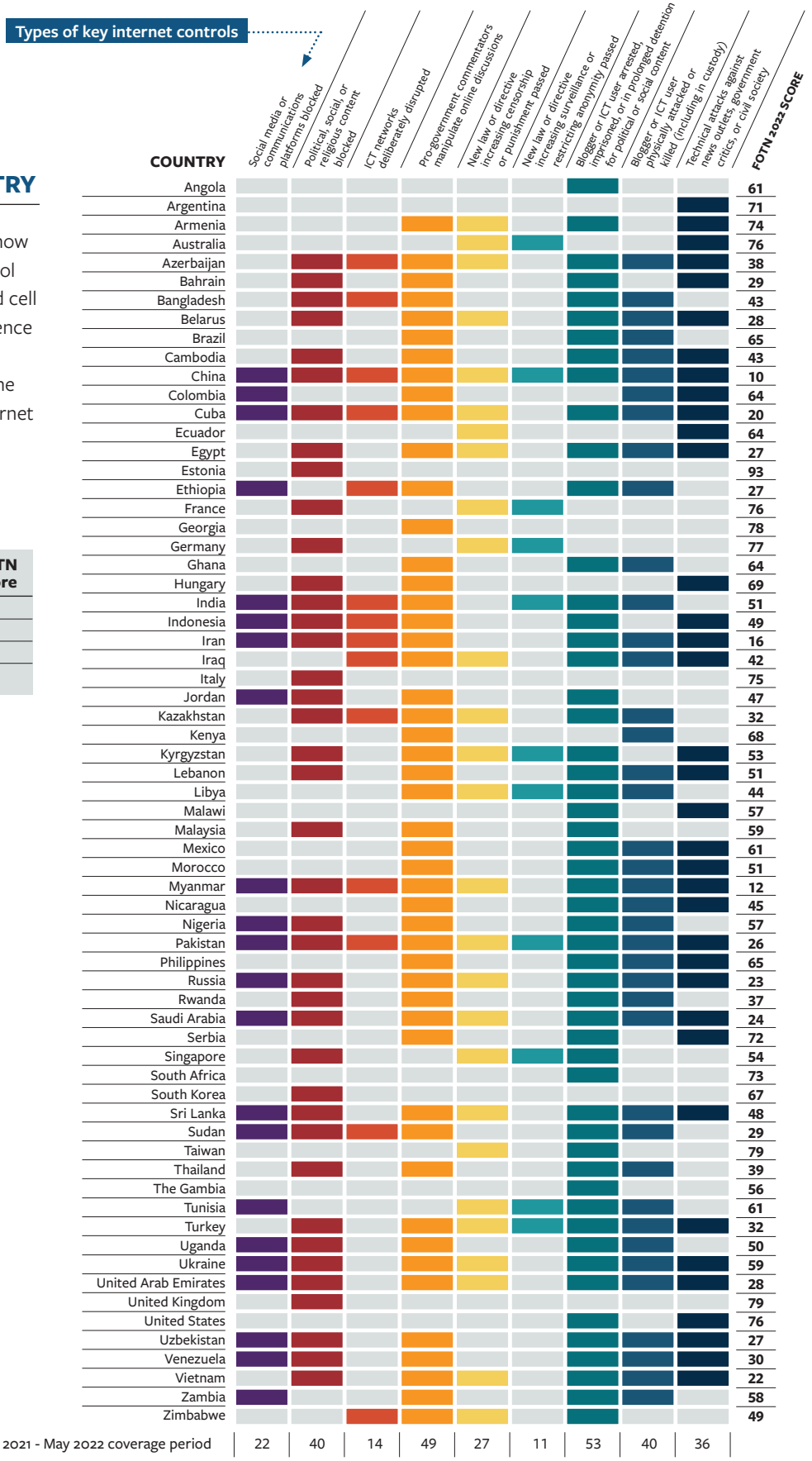
One advocacy effort has already identified its target: governments' purchase and deployment of intrusive commercial surveillance tools that violate the rights of internet users around the world. Technical researchers, human rights experts, and media investigations have recently documented the reach and abuses of the shadowy spyware industry, and governments have started to explore legal and regulatory restrictions on the sale of such products. These are welcome first steps, but more is needed.

Disproportionate surveillance remains one of the most obvious problems affecting democracies' internet freedom performance. Too often, rights considerations are disregarded in favor of the misguided belief that more intrusive tools and greater state access to data will necessarily contribute to a safer society. In addition to addressing the proliferation of spyware, democracies should impose robust controls on other forms of surveillance and protect end-to-end encryption, which limits the impact of such excessive monitoring. The coalition model for achieving digital resilience could be employed to focus much-needed public scrutiny on the question of which surveillance tools and practices are compatible with human rights. Such action would lay the groundwork for democracies to adopt rights-based regulations at home, clear the way for more coordinated and effective restrictions on the private surveillance market, and remove powerful and ever-evolving monitoring tools from the hands of abusive government actors, ultimately fostering a more democratic future.

## KEY INTERNET CONTROLS BY COUNTRY

Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during the report's coverage period of June 2021 to May 2022. The Key Internet Controls reflect restrictions on content of political, social, or religious nature.

| NO KEY INTERNET CONTROLS OBSERVED | FOTN Score |
|---|---|
| Canada | 87 |
| Costa Rica | 88 |
| Iceland | 95 |
| Japan | 77 |



# Recommendations

## FOR POLICYMAKERS

### *Protect privacy and security*

**Strictly regulate the use of surveillance tools and personal-data collection by government and law enforcement agencies.** Government surveillance programs should adhere to the International Principles on the Application of Human Rights to Communications Surveillance, a framework agreed upon by a broad consortium of civil society groups, industry leaders, and scholars for protecting users' rights. The principles, which state that all communications surveillance must be legal, necessary, and proportionate, should also be applied to biometric surveillance technologies and open-source intelligence methods such as social media monitoring. In the United States, lawmakers should reform or repeal existing surveillance laws and practices to better align with these standards, including those under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, and pass the bipartisan Fourth Amendment Is Not For Sale Act, which would require government agencies to obtain a court order before purchasing data from data brokers. Policymakers in the United States should also investigate the extent to which commercial surveillance tools, such as spyware and extraction technology, have been used against Americans and ensure that appropriate safeguards are in place.

**Protect encryption.** Robust encryption is fundamental to cybersecurity, commerce, and the protection of human rights. Weakening encryption endangers the lives of activists, journalists, members of marginalized communities, and ordinary users around the world. Governments should refrain from mandating the introduction of "back doors," requiring traceability of messages, or reducing intermediary liability protections for providers of end-to-end encryption services. In the United States, any reforms to Section 230 of the Communications Decency Act should not undermine the ability of intermediaries and service providers to offer robust encryption.

**Strengthen data-privacy protections by promulgating stronger regulations and enacting comprehensive legislation.** Democracies should collaborate to create interoperable privacy regimes that comprehensively safeguard user information, while also allowing data to flow across borders to jurisdictions with similar levels of protection. Individuals should have control over their information, including the right to access it, delete it, and easily transfer it to the providers of their choosing. Companies should be required to limit the collection of consumer data, particularly intimate information such as health, biometric, and location data, disclose in plain language how they use data they do collect, and limit how third parties can access and use this data. Updated data-privacy protections should include provisions that provide independent regulators and oversight mechanisms with the ability, resources, and expertise needed to enforce and ensure foreign and domestic companies comply with privacy, nondiscrimination, and consumer-protection laws. In the United States, the Federal Trade Commission (FTC) has initiated important action to strengthen privacy enforcement under existing authorities by issuing an Advance Notice of Proposed Rulemaking to explore whether stronger protections are needed regarding commercial surveillance and data security. In the current absence of a federal data privacy law, the FTC should issue a final rule that provides robust protections and facilitates enforcement. Comprehensive data-privacy legislation is also needed in the United States. The proposed American Data Privacy and Protection Act (ADPPA), which would institute a comprehensive framework that limits what data can be collected by companies, would be a positive step. The ADPPA would be made stronger by making it clear that states are free to pass their own, more robust privacy protection laws.

**Restrict the export of censorship and surveillance technology.** A booming commercial market for surveillance and censorship technologies has given governments even greater capacity to flout the rule of law, monitor private communications, and restrict access to essential resources. Democracies should place strict limits on the sale of technologies that enable monitoring, surveillance, interception, or collection of information and communications—including technologies that collect and analyze biometric information (including gait, facial measurements, voice, and DNA, among others), spyware,

data-extraction technology, and general-purpose products that provide the advanced computing power, machine learning, natural-language processing, and artificial intelligence capabilities that can be used to enhance these technologies. In a first, the Costa Rican government called for a global moratorium on the use of spyware technology in 2022. The United States, Australia, Denmark, and Norway, supported by Canada, France, the Netherlands, and the United Kingdom, have recently announced the Export Controls and Human Rights Initiative, intended to "help stem the tide of authoritarian government misuse of technology and promote a positive vision for technologies anchored by democratic values." The United States additionally updated its licensing policy to restrict the export of items if there is "a risk that the items will be used to violate or abuse human rights," and the European Union (EU) tightened export controls for dual-use products and cybersurveillance technologies. When implementing such new policies, government officials should give extra scrutiny to the suitability of exports intended for countries rated as Not Free or Partly Free by Freedom House, where the most frequent censorship and surveillance abuses occur. Government export guidance should urge businesses to adhere to the UN Guiding Principles on Business and Human Rights. Businesses exporting surveillance and censorship technologies that could be used to commit human rights abuses should be required to report annually to the public on the impacts of their exports. Reports should include a list of countries to which they have exported such technologies, potential human rights concerns in each of those countries, a summary of preexport due diligence undertaken to ensure that their products are not misused, human rights violations that have occurred as a result of the use or potential use of their technologies, and efforts to mitigate the harm done and prevent future abuses. In the United States, Congress should pass the Foreign Advanced Technology Surveillance Accountability Act, which requires the Department of State to include information on the status of surveillance and use of advanced technology in its annual report on global human rights practices.

## *Safeguard free expression, access to information, and a diverse online environment*

**Maintain access to internet services, digital platforms, and circumvention technology, particularly during elections, protests, and periods of conflict.** Intentional disruptions to internet access and online services impact individuals' economic, social, political, and civil rights. Governments should avoid blocking or imposing onerous regulatory requirements on circumvention tools, and imposing outright or arbitrary bans on social media and messaging platforms. While some services may present genuine societal and national security concerns, bans unduly restrict user expression. Governments should instead address any legitimate risks posed by social media and messaging platforms through existing democratic mechanisms including regulatory action, security audits, parliamentary scrutiny, and legislation passed in consultation with civil society and affected stakeholders. Any restrictions to online content should adhere to international human rights standards of legality, necessity, and proportionality, and include robust oversight, transparency, and consultation with civil society and the private sector. When sanctions are imposed, it should be made clear that internet communications services are exempt so as not to limit essential online tools for users in authoritarian countries.

**Enshrine human rights principles, transparency, and democratic oversight in laws that regulate online content.** Legal frameworks addressing online content should establish special type- and size-oriented obligations on companies, incentivize platforms to improve their own standards, and require human rights due diligence and reporting. Such requirements should prioritize transparency across core products and practices, including content moderation, recommendation and algorithmic systems, collection and use of data, and political and targeted advertising practices. Laws should also provide opportunities for vetted researchers to access platform data—information that can provide insights for policy development and civil society's research and advocacy. Intermediaries should continue to benefit from safe-harbor protections for most user-generated and third-party content appearing on their platforms, so as not to encourage restrictions that could inhibit free expression. Laws should also protect "good Samaritan" rules and reserve decisions on the legality of content for the judiciary rather than companies or executive agencies. Internet users whose account or content is limited or removed should have access to systems for notice, explanation, redress, and appeal. Independent, multistakeholder bodies and independent regulators with sufficient resources and expertise should be empowered to oversee the implementation of laws, conduct audits, and ensure compliance. Provisions within the EU's Digital Services Act, notably its transparency provisions, data accessibility for researchers, and a coregulatory form of enforcement, offer a promising model for content-related laws.

**Support online media and foster a resilient information space.** Combating disinformation and propaganda begins with public access to reliable information and local, on-the-ground reporting. Democracies should scale up efforts to support independent online media in their own countries and abroad through financial assistance and innovative financing models, technical support, and professional development support. They should pair those efforts with broader civic education initiatives and digital literacy training that help people navigate complex media environments. They should also expand protections for journalists who face physical attacks, legal reprisals, and harassment for their work online, including by supporting the creation of emergency visas for those at risk. Laws should protect the free flow of information, grant journalists access to those in power, allow the public to place freedom of information requests, and guard against state monopolization of media outlets.

**Fully integrate human rights principles in competition policy enforcement.** Diversifying the market for online services—particularly through the creation of smaller platforms that can be tailored toward the needs of a particular community or audience—is a key step toward a more resilient information environment. Competition in the digital market can also encourage companies to create innovative products that protect fundamental rights and tackle online harms such as harassment. When enforcing competition policy, regulators should consider the implications of market dominance on free expression, privacy, nondiscrimination, and other rights. Governments should also ensure antitrust frameworks can effectively be applied in the digital age, and create legal regimes that incentivize such diversity, such as by introducing interoperability and data-portability provisions like those in the EU's Digital Markets Act.

**Address the digital divide.** Unequal access to the internet contributes to economic and social inequality and undermines the benefits of a free and open internet. In the short term, governments should work with service providers to lift data caps and waive late-payment fees; they should also support community-based initiatives to provide secure public-access points and lend electronic devices to individuals who need them. Longer-term efforts should include expanding access and building internet infrastructure for underserved areas and populations, ensuring that connectivity is affordable, and enacting strong legal protections for user privacy and net neutrality.

## *Strengthen global internet freedom*

**Ensure that cyber diplomacy is both coordinated among democracies and grounded in human rights.** Democracies should facilitate dialogue among national policymakers and regulators to coordinate on best practices for tech policy, and strengthen engagement at international standards–setting bodies. Diplomats should develop common approaches to countering authoritarian influence within the UN General Assembly, International Telecommunication Union (ITU), and other multilateral bodies. Multilateral decision-making should support and complement, not replace, specific internet-governance and standards-setting activities by multistakeholder bodies like the Internet Corporation for Assigned Names and Numbers (ICANN). In the United States, there is an opportunity to institutionalize and sustain new initiatives and funding streams focused on global technology policy and internet freedom, especially those announced at the inaugural Summit for Democracy. The State Department's new Bureau of Cyberspace and Digital Policy should make human rights a central component of its mandate, including by ensuring that staff have relevant expertise and coordinating closely with other internet-focused departments within and across agencies. These efforts should also formalize regular, ongoing engagement with civil society and the private sector.

**Strengthen the Freedom Online Coalition's capacity to protect internet freedom.** As the upcoming 2023 chair, the United States should focus on strengthening the FOC's name recognition and its ability to drive diplomatic coordination and global action. This includes by more proactively articulating the benefits of a free and open internet to governments, being more publicly and privately vocal on threats and opportunities for human rights online, mainstreaming FOC activity in other multilateral initiatives like the ITU and Group of 7 (G7), and creating more avenues to engage with civil society and the private sector, including through diversifying and expanding the coalition's advisory network. The FOC should consider increasing internal staffing to achieve these goals, and creating an internal mechanism by which member states' activities can be evaluated to ensure they align with FOC principles. A new funding mechanism, supported by member states, for programs and activities

led by nonstate stakeholders could also advance FOC priorities. Any expansion of the coalition's membership should be carried out in consultation with the advisory network, and new members should be selected based on their capacity to bolster the FOC's work and contribute to greater geographic diversity within the body.

**Defend and expand internet freedom programming as a vital component of democracy assistance.** Democracy assistance targeting internet freedom activities should prioritize digital security and digital activism trainings, as well as provision of software that can protect or assist users. Policymakers should support programs that seek to strengthen judicial independence, enhance technical literacy among judges and others within the legal system, and provide other financial and administrative resources for strategic litigation. Governments should increase support for technologies that help individuals in closed environments circumvent government censorship, protect themselves against surveillance, and overcome restrictions on connectivity. Such tools should be open-source, user-friendly, and locally responsive in order to ensure high levels of security and use. Finally, programming should support efforts aimed at strengthening the independence and expertise of regulators, which can serve as politically neutral bodies that protect internet freedom across changes in political leadership.

**Advocate for the immediate, unconditional release of those imprisoned for online expression protected under international standards.** Governments should incorporate these cases, in addition to broader internet-freedom concerns, into bilateral and multilateral engagement with perpetrator countries. It should be made standard practice to raise the names of those detained for their online content, to request information or specific action related to their treatment, and to call for their release and the repeal of laws that criminalize online expression.

## FOR COMPANIES

**Ensure fair and transparent content moderation.** To ensure content-moderation policies that are respectful of users, private companies should:

- Prioritize users' free expression and access to information, particularly for journalism; discussion of human rights; educational materials; and political, social, cultural, religious, and artistic expression.
- Clearly and completely explain in guidelines and terms of service what speech is not permissible, what aims restrictions serve, and how content is assessed for violations. An essential step is ensuring that terms of service, as well as mechanisms for reporting harmful content and appealing content decisions, are translated into all languages where the company's products are used.
- When appropriate, consider less-invasive alternatives to content removal, such as demotion of content, labeling, fact-checking, promoting more authoritative sources, and implementing design changes that improve civic discussions.
- Publish detailed transparency reports on content takedowns, both for those initiated by governments and for those undertaken by companies. Transparency reports should also address how machine learning is used to train automated systems that classify, recommend, and prioritize content for human review.
- Provide an efficient and timely avenue of appeal for users who believe that their rights were unduly restricted, including through censorship, banning, assignment of labels, or demonetization of posts.
- Refrain from relying on automated systems for removing content without opportunity for meaningful human review.
- Expand the capacity, geographic, and linguistic diversity of content moderation teams, and ensure they are sensitive to nuances in a language that is spoken across multiple countries or regions. Conduct human rights due diligence assessments to ensure that implementation of moderation does not lead to unintended consequences, such as disproportionately affecting marginalized communities.

**Resist government orders to shut down internet connectivity, ban digital services, and unduly turn over data or restrict user accounts and content.** Service providers should use all available legal channels to challenge such requests from state agencies, whether they are official or informal, especially those that relate to human rights defenders, activists, civil society, journalists, or other at-risk accounts. If companies cannot resist demands in full, they should ensure that any restrictions or disruptions are as limited as possible in duration, geographic scope, and type of content affected. Companies should thoroughly document government demands internally and notify users as to why connectivity or their content may be restricted, especially in countries where government actions lack transparency. When faced with a choice between a ban of their services and complying with undue data requests and censorship orders, companies should bring strategic legal cases that challenge government overreach, in consultation or partnership with civil society.

**Adhere to the UN Guiding Principles on Business and Human Rights, adopt the Global Network Initiative Principles on Freedom of Expression and Privacy, and conduct human rights impact assessments.** Companies should commit to respecting the rights of their users and addressing any adverse impact that their products might have on human rights. The Global Network Initiative's Principles provide concrete guidance on how to do so. Companies should invest in and expand programs and tools that allow users, especially human rights defenders, journalists, and those from at-risk populations, to easily protect themselves from online and offline harms, particularly during crisis events. Companies should also minimize the amount of data they collect, sell, and use, and clearly communicate to users what data are collected and for what purpose. Where companies do operate, they should conduct and publish periodic assessments to fully understand how their products and actions might affect rights including freedom of expression, nondiscrimination, and privacy.

**Enshrine human rights principles in product design and development.** Protecting rights online begins with responsible product design and development. Technologists and engineers should be trained on the human rights implications of the products they build and on international best practices for preventing their abuse. Companies should conduct research and consult with impacted communities to understand the ways their products can be used to perpetrate online and offline harms and respond with strong guardrails that prioritize safety. When a product is found to have been used for human rights violations, companies should suspend sales to the perpetrating party and develop an immediate action plan to mitigate harm and prevent further abuse. Companies should also support the accessibility of circumvention technology, mainstream end-to-end encryption in their products, and ensure other robust security protocols, including by resisting government requests to provide special decryption access.

**Engage in continuous dialogue with civil society to understand the effects of company policies and products.** Companies should seek out local expertise on the political and cultural context in markets where they have a presence or where their products are widely used, especially in repressive contexts due to unique sets of human rights challenges that require context-specific solutions. Consultations with civil society groups should inform whether companies choose to operate in a particular country, the companies' approach to content moderation, the development of products and policies, especially during elections or crisis events, when managing government requests, and when working to counter online harms.

# Methodology

## WHAT WE MEASURE

The *Freedom on the Net* index measures each country's level of internet freedom based on a set of methodology questions. The methodology is developed in consultation with international experts to capture the vast array of relevant issues to human rights online (see "Checklist of Questions").

*Freedom on the Net's* core values are grounded in international human rights standards, particularly Article 19 of the Universal Declaration of Human Rights. The project particularly focuses on the free flow of information, the protection of free expression, access to information, and privacy rights, and freedom from both legal and extralegal repercussions arising from online activities. The project also evaluates to what extent a rights-enabling online environment is fostered in a particular country.

The index acknowledges that certain rights may be legitimately restricted. The standard of such restrictions within the methodology and scoring aligns with international human rights principles of necessity and proportionality, the rule of law, and other democratic safeguards. Censorship and surveillance policies and procedures should be transparent, minimal, and include avenues for appeal available to those affected, among other safeguards.

**The project rates the real-world rights and freedoms enjoyed by individuals within each country.** While internet freedom may be primarily affected by state behavior, actions by nonstate actors, including technology companies, are also considered. Thus, the index ratings generally reflect the interplay of a variety of actors, both governmental and nongovernmental. Over the years, *Freedom on the Net* has been continuously adapted to capture technological advances, shifting tactics of repression, and emerging threats to internet freedom.

## THE RESEARCH AND SCORING PROCESS

The methodology includes 21 questions and nearly 100 subquestions, divided into three categories:

1. **Obstacles to Access** details infrastructural, economic, and political barriers to access; government decisions to shut off connectivity or block specific applications or technologies; legal, regulatory, and ownership control over internet service providers; and the independence of regulatory bodies;

2. **Limits on Content** analyzes legal regulations on content; technical filtering and blocking of websites; other forms of censorship and self-censorship; the vibrancy and diversity of online information space; and the use of digital tools for civic mobilization;

3. **Violations of User Rights** tackles legal protections and restrictions on free expression; surveillance and privacy; and legal and extralegal repercussions for online speech and activities, such as imprisonment, cyberattacks, or extralegal harassment and physical violence.

Each question is scored on a varying range of points. The subquestions guide researchers regarding factors they should consider while evaluating and assigning points, though not all apply to every country. Under each question, a higher number of points is allotted for a freer situation, while a lower number of points is allotted for a less free environment. Points add up to produce a score for each of the subcategories, and a country's total points for all three represent its final score (0-100). Based on the score, Freedom House assigns the following internet freedom ratings:

- **Scores 100-70 = Free**
- **Scores 69-40 = Partly Free**
- **Scores 39-0 = Not Free**

Freedom House staff invite at least one researcher or organization to serve as the report author for each country, training them to assess internet freedom developments according to the project's comprehensive research methodology. Researchers submit draft country reports and attend a ratings review meeting focused on their region. During the meetings, participants review, critique, and adjust the draft scores—based on set coding guidelines—through careful consideration of events, laws, and practices relevant to each item. After completing the regional and country consultations, Freedom House staff edit and fact-check all country reports and perform a final review of all scores to ensure their comparative reliability and integrity. Freedom House staff also conduct robust qualitative analysis on every country to determine each year's key global findings and emerging trends.

# Checklist of Questions

- Each country is rated on a scale of 100 to 0, with 100 representing the most free conditions and 0 the least free.
- A combined score of 100-70 = Free, 69-40 = Partly Free, and 39-0 = Not Free.

## A. OBSTACLES TO ACCESS

### (*0–25 POINTS*)

1. **Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?** (*0–6 points*)
   - Do individuals have access to high-speed internet services at their home, place of work, internet cafés, libraries, schools, and other venues, as well as on mobile devices?
   - Does poor infrastructure (including unreliable electricity) or catastrophic damage to infrastructure (caused by events such as natural disasters or armed conflicts) limit residents' ability to access the internet?

2. **Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?** (*0–3 points*)
   - Do financial constraints—such as high prices for internet services, excessive taxes imposed on such services, or state manipulation of the relevant markets—make internet access prohibitively expensive for large segments of the population?
   - Are there significant differences in internet penetration and access based on geographical area, or for certain ethnic, religious, gender, LGBT+, migrant, and other relevant groups?
   - Do pricing practices, such as zero-rating plans, by service providers and digital platforms contribute to a digital divide in terms of what types of content individuals with different financial means can access?

3. **Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?** (*0–6 points*)
   - Does the government restrict, or compel service providers to restrict, internet connectivity by slowing or shutting down internet connections during specific events (such as protests or elections), either locally or nationally?
   - Does the government centralize internet infrastructure in a manner that could facilitate restrictions on connectivity?
   - Does the government block, or compel service providers to block, social media platforms and communication apps that serve in practice as major conduits for online information?
   - Does the government block, or compel service providers to block, certain protocols, ports, and functionalities within such platforms and apps (e.g., Voice-over-Internet-Protocol or VoIP, video streaming, multimedia messaging, Secure Sockets Layer or SSL), either permanently or during specific events?
   - Do restrictions on connectivity disproportionately affect marginalized communities, such as inhabitants of certain regions or those belonging to different ethnic, religious, gender, LGBT+, migrant, and other relevant groups?

4. **Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?** (*0–6 points*)
   - Is there a legal or de facto monopoly on the provision of fixed-line, mobile, and public internet access?
   - Does the state place extensive legal, regulatory, or economic requirements on the establishment or operation of service providers?
   - Do licensing requirements, such as retaining customer data or preventing access to certain content, place an onerous financial burden on service providers?

5. **Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?** (*0–4 points*)
   - Are there explicit legal guarantees that protect the independence and autonomy of any regulatory body overseeing the internet (exclusively or as part of a broader mandate) from political or commercial interference?
   - Is the process for appointing members of regulatory bodies transparent and representative of different stakeholders' legitimate interests?
   - Are decisions taken by regulatory bodies seen to be fair and to take meaningful notice of comments from stakeholders in society?
   - Are decisions taken by regulatory bodies seen to be apolitical and independent from changes in government?
   - Are decisions taken by regulatory bodies seen to be protecting internet freedom, including by ensuring service providers, digital platforms, and other content hosts behave fairly?

# B. LIMITS ON CONTENT

## (*0–35 POINTS*)

1. **Does the state block or filter, or compel service providers to block or filter, internet content particularly material that is protected by international human rights standards?** (*0–6 points*)
   - Does the state use, or compel service providers to use, technical means to restrict freedom of opinion and expression, for example by blocking or filtering websites and online content featuring journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression?
   - Does the state use, or compel service providers to use, technical means to block or filter access to websites that may be socially or legally problematic (e.g., those related to gambling, pornography, copyright violations, illegal drugs) in lieu of more effective remedies, or in a manner that inflicts collateral damage on content and activities that are protected under international human rights standards?
   - Does the state block or order the blocking of entire social media platforms, communication apps, blog-hosting platforms, discussion forums, and other web domains for the purpose of censoring the content that appears on them?
   - Is there blocking of tools that enable users to bypass censorship?
   - Does the state procure, or compel services providers to procure, advanced technology to automate censorship or increase its scope?

2. **Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content particularly material that is protected by international human rights standards?** (*0–4 points*)
   - Are administrative, judicial, or extralegal measures used to order the deletion of content from the internet, particularly journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression, either prior to or after its publication?
   - Do digital platforms and content hosts arbitrarily remove such content due to informal or formal pressure from government officials or other powerful political actors?
   - Are access providers, content hosts, and third parties free from excessive or improper legal responsibility for opinions expressed by third parties transmitted via the technology they supply?

3. **Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?** (*0–4 points*)
   - Are there national laws, independent oversight bodies, and other democratically accountable procedures in place to ensure that decisions to restrict access to certain content are proportional to their stated aim?
   - Are those that restrict content—including state authorities, ISPs, content hosts, digital platforms, and other intermediaries—transparent about what content is blocked or deleted, including to the public and directly to the impacted user?
   - Do efficient and timely avenues of appeal exist for those who find content they produced to have been subjected to censorship?
   - Are self-regulatory mechanisms and oversight bodies effective at ensuring content protected under international human rights standards is not removed?

4. **Do online journalists, commentators, and ordinary users practice self-censorship?** (*0–4 points*)
   - Do internet users in the country engage in self-censorship on important political, social, or religious issues, including on public forums and in private communications?
   - Does fear of retribution, censorship, state surveillance, or data collection practices have a chilling effect on online speech or cause users to avoid certain online activities of a civic nature?
   - Where widespread self-censorship exists, do some journalists, commentators, or ordinary users continue to test the boundaries, despite the potential repercussions?

5. **Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?** (*0–4 points*)
   - Do political leaders, government agencies, political parties, or other powerful actors directly manipulate information via state-owned news outlets, official social media accounts/groups, or other formal channels?
   - Do government officials or other actors surreptitiously employ or encourage individuals or automated systems to artificially amplify political narratives or smear campaigns on social media?
   - Do government officials or other powerful actors pressure or coerce online news outlets, journalists, or bloggers to follow a particular editorial direction in their reporting and commentary?
   - Do authorities issue official guidelines or directives on coverage to online media outlets, including instructions to downplay or amplify certain comments or topics for discussion?
   - Do government officials or other actors bribe or use close economic ties with online journalists, bloggers, or website owners in order to influence the content they produce or host?
   - Does disinformation, coordinated by foreign or domestic actors for political purposes, have a significant impact on public debate?

6. **Are there economic, regulatory, or other constraints that negatively affect users' ability to publish content online?** (*0–3 points*)
   - Are favorable informal connections with government officials necessary for online media outlets, content hosts, or digital platforms (e.g., search engines, email applications, blog-hosting platforms) to be economically viable?
   - Does the state limit the ability of online media to accept advertising or investment, particularly from foreign sources, or does it discourage advertisers from conducting business with disfavored online media or service providers?
   - Do onerous taxes, regulations, or licensing fees present an obstacle to participation in, establishment of, or management of digital platforms, news outlets, blogs, or social media groups/channels?
   - Do ISPs manage network traffic and bandwidth availability in a manner that is transparent, is evenly applied, and does not discriminate against users or producers of content based on the nature or source of the content itself (i.e., do they respect "net neutrality" with regard to content)?

7. **Does the online information landscape lack diversity and reliability?** (*0–4 points*)
   - Are people able to access a range of local, regional, and international news sources that convey independent, balanced views in the main languages spoken in the country?
   - Do online media outlets, social media pages, blogs, and websites represent diverse interests, experiences, and languages within society, for example by providing content produced by different ethnic, religious, gender, LGBT+, migrant, and other relevant groups?
   - Does a lack of competition among content hosts and digital platforms limit users' ability to publish content online?
   - Does the presence of misinformation undermine users' ability to access independent, credible, and diverse sources of information?
   - Does false or misleading content online significantly contribute to offline harms, such as harassment, property destruction, physical violence, or death?
   - If there is extensive censorship, do users employ virtual private networks (VPNs) and other circumvention tools to access a broader array of information sources?

8. **Do conditions impede users' ability to form communities, mobilize, and campaign, particularly on political and social issues?** (*0–6 points*)
   - Can people freely join online communities based around their political, social, or cultural identities, including without fear of retribution?
   - Do civil society organizations, activists, and online communities organize online on political, social, cultural, and economic issues, including during electoral campaigns and nonviolent protests, including without fear of retribution?
   - Do state or other actors limit access to online tools and websites (e.g., social media platforms, messaging groups, petition websites) for the purpose of restricting free assembly and association online?
   - Does the state place legal or other restrictions (e.g. criminal provisions, detentions, surveillance) for the purpose of restricting free assembly and association online?

# C. VIOLATIONS OF USER RIGHTS

## (*0–40 POINTS*)

1. **Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?** (*0–6 points*)
   - Does the constitution contain language that provides for freedom of expression, access to information, and press freedom generally?
   - Are there laws or binding legal decisions that specifically protect online modes of expression?
   - Do executive, legislative, and other governmental authorities comply with these legal decisions, and are these decisions effectively enforced?
   - Are online journalists and bloggers accorded strong rights and protections to perform their work?
   - Is the judiciary independent, and do senior judicial bodies and officials support free expression, access to information, and press freedom online?

2. **Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?** (*0–4 points*)
   - Do specific laws—including penal codes and those related to the media, defamation, cybercrime, cybersecurity, and terrorism—criminalize online expression and activities that are protected under international human rights standards (e.g., journalism, discussion of human rights, educational materials, or political, social, cultural, religious, and artistic expression)?
   - Are restrictions on internet freedom defined by law, narrowly circumscribed, and both necessary and proportionate to address a legitimate aim?

3. **Are individuals penalized for online activities, particularly those that are protected under international human rights standards?** (*0–6 points*)
   - Are writers, commentators, bloggers, or social media users subject to civil liability, imprisonment, arbitrary detention, police raids, or other legal sanction for publishing, sharing, or accessing material on the internet in contravention of international human rights standards?
   - Are penalties for defamation; spreading false information or "fake news"; cybersecurity, national security, terrorism, and extremism; blasphemy; insulting state institutions and officials; or harming foreign relations applied unnecessarily and disproportionately?

4. **Does the government place restrictions on anonymous communication or encryption?** (*0–4 points*)
   - Are website owners, bloggers, or users in general required to register with the government?
   - Does the government require that individuals use their real names or register with the authorities when posting comments or purchasing electronic devices, such as mobile phones?
   - Are users prohibited from using encryption services to protect their communications?
   - Are there laws requiring that users or providers of encryption services turn over decryption keys to the government?

5. **Does state surveillance of internet activities infringe on users' right to privacy?** (*0–6 points*)
   - Does the constitution, specific laws, or binding legal decisions protect against government intrusion into private lives?
   - Do state authorities engage in the blanket collection of communications metadata and/or content transmitted within the country?
   - Are there legal guidelines and independent oversight on the collection, retention, and inspection of surveillance data by state security agencies, and if so, do those guidelines adhere to international human rights standards regarding transparency, necessity, and proportionality?
   - Do state authorities monitor publicly available information posted online (including on websites, blogs, social media, and other digital platforms), particularly for the purpose of deterring independent journalism or political, social, cultural, religious, and artistic expression?
   - Do authorities have the technical capacity to regularly monitor or intercept the content of private communications, such as email and other private messages, including through spyware and extraction technology?
   - Do local authorities such as police departments surveil residents (including through International Mobile Subscriber Identity-Catchers or IMSI catcher technology), and if so, are such practices subject to rigorous guidelines and judicial oversight?
   - Do state actors use artificial intelligence and other advanced technology for the purposes of online surveillance without appropriate oversight?
   - Do government surveillance measures target or disproportionately affect dissidents, human rights defenders, journalists, or certain ethnic, religious, gender, LGBT+, migrant, and other relevant groups?

6. **Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?** (*0–6 points*)
   - Do specific laws or binding legal decisions enshrine the rights of users over personal data, including biometric information, generated, collected, or processed by public or private entities?
   - Do regulatory bodies, such as a data protection agency, effectively protect user privacy, including through investigating companies' mismanagement of data and enforcing relevant laws or legal decisions?
   - Can the government obtain user information from companies (e.g., service providers, providers of public access, internet cafés, social media platforms, email providers, device manufacturers) without a legal process?
   - Are these companies required to collect and retain data about their users?
   - Are these companies required to store users' data on servers located in the country, particularly data related to online activities and expression that are protected under international human rights standards (i.e., are there "data localization" requirements)?
   - Do these companies monitor users and supply information about their digital activities to the government or other powerful actors (either through technical interception, data sharing, or other means)?
   - Does the state attempt to impose similar requirements on these companies through less formal methods, such as codes of conduct, threats of censorship, or other economic or political consequences?
   - Are government requests for user data from these companies transparent, and do companies have a realistic avenue for appeal, for example via independent courts?

7. **Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?** (*0–5 points*)
   - Are individuals subject to physical violence—such as murder, assault, torture, sexual violence, or enforced disappearance—in relation to their online activities, including membership in certain online communities?
   - Are individuals subject to other intimidation and harassment—such as verbal threats, travel restrictions, nonconsensual sharing of intimate images, doxing, or property destruction or confiscation—in relation to their online activities?
   - Are individuals subject to online intimidation and harassment specifically because they belong to a certain ethnic, religious, gender, LGBT+, migrant or other relevant group?
   - Have online journalists, bloggers, or others fled the country or gone into hiding to avoid such consequences?
   - Have the online activities of dissidents, journalists, bloggers, human rights defenders, or other users based outside the country led to repercussions for their family members or associates based in the country?

8. **Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?** (*0–3 points*)
   - Have websites belonging to opposition, news outlets, or civil society groups in the country been temporarily or permanently disabled due to cyberattacks, particularly at politically sensitive times?
   - Are websites or blogs subject to targeted technical attacks as retribution for posting certain content, for example on political and social topics?
   - Are financial, commercial, and governmental entities subject to significant and targeted cyberattacks meant to steal data or disable normal operations, including attacks that originate outside the country?
   - Are laws and policies in place to prevent and protect against cyberattacks (including systematic attacks by domestic nonstate actors), and are they enforced?

# Acknowledgements

*Freedom on the Net* is a collaborative effort between Freedom House staff and a network of more than 80 researchers, who come from civil society organizations, academia, journalism, and other backgrounds, covering 70 countries. In repressive environments, Freedom House takes care to ensure researchers' anonymity and/or works with experts living abroad.

This report was made possible by the generous support of Amazon, the Dutch Ministry of Foreign Affairs, Google, the Hurford Foundation, Internet Society, Lilly Endowment Inc., The New York Community Trust, and the U.S. State Department's Bureau of Democracy, Human Rights, and Labor (DRL). Freedom House is committed to editorial independence. Our donors do not influence the organization's research priorities, report findings, or policy recommendations.

The *Freedom on the Net* team expresses their gratitude to the global internet freedom community, including the many individuals and organizations whose tireless and courageous work informs this report.

Elisha Aaron, David Meijer, Shannon O'Toole, Tyler Roylance, and Lora Uhlig edited *Freedom on the Net*. Michael Abramowitz, Gerardo Berthin, Nicole Bibbins Sedaca, Annie Boyajian, Nate Schenkkan, and Lara Shane provided valuable feedback on the summary of findings. Sarah Cook and Angeli Datt served as advisers for China. Mike Smeltzer and Noah Buyon advised on the Europe and Eurasia regions. Danielle Dougall, Dasha M, and Eilidh Stalker provided research assistance.

## CONTRIBUTORS

### Freedom House staff

- **Adrian Shahbaz**, Vice President of Research and Analysis
- **Allie Funk**, Research Director for Technology and Democracy
- **Philip Friedrich**, Senior Research Analyst for Technology and Elections
- **Kian Vesteinsson**, Senior Research Analyst for Technology and Democracy
- **Grant Baker**, Research Analyst for Technology and Democracy
- **Cathryn Grothe**, Research Analyst for Middle East & North Africa
- **Maddie Masinsin**, Community Engagement Specialist for Technology and Democracy
- **Manisha Vepa**, former Research Associate
- **Tessa Weal**, Research Associate for Technology and Democracy

### Report authors

- **Argentina:** Eduardo Ferreyra, independent researcher
- **Armenia:** Samvel Martirosyan, Co-Founder of CyberHUB-AM
- **Australia:** Elizabeth O'Shea and Lucie Krahulcova, Digital Rights Watch
- **Azerbaijan:** Arzu Geybulla, journalist
- **Brazil:** Bruna Martins dos Santos, German Chancellor Fellow at Alexander von Humboldt Foundation and Visiting Researcher at Berlin Social Science Center
- **Cambodia:** Sopheap Chak, Executive Director of Cambodian Center for Human Rights
- **Canada:** Allen Mendelsohn, McGill University
- **Colombia:** Emmanuel Vargas and Susana Echaverría, El Veinte
- **Costa Rica:** Oscar Mario Jiménez Alvarado, Fernando Martínez de Lemos, Johanna Rodríguez López, Programa de Libertad de Expresión, Derecho a la Información y Opinión Pública (PROLEDI), Universidad de Costa Rica (UCR)
- **Cuba:** Ted Henken, Baruch College, City University of New York
- **Estonia:** Hille Hinsberg and Florian Marcus, Proud Engineers
- **Ethiopia:** Atnafu Brhane, Center for Advancement of Rights and Democracy
- **France:** Dr. Suzanne Vergnolle, Associate Professor at Cnam Institute
- **Georgia:** Teona Turashvili, Institute for Development of Freedom of Information
- **Germany:** Paul Ritzka and Lisa Schmechel, iRights.Lab
- **Hungary:** Dalma Dojcsák, Hungarian Civil Liberties Union
- **Iceland:** Arnaldur Sigurðarson, independent researcher

- **Indonesia:** Southeast Asia Freedom of Expression Network (SAFEnet)
- **Iraq:** Hayder Hamzoz and Assia Abdulkareem, Iraqi Network for Social Media
- **Italy:** Philip Di Salvo, Visiting Fellow at the London School of Economics; Antonella Napolitano, Privacy International
- **Japan:** Hamada Tadahisa, Japan Computer Access for Empowerment
- **Lebanon:** Marianne Rahme, SMEX
- **Libya:** Jabir Zain, Libyan Center for Freedom of the Press
- **Malawi:** Jimmy Kainja, University of Malawi
- **Malaysia:** Kelly Koh, Sinar Project
- **Mexico:** Mariel García-Montes, Massachusetts Institute of Technology
- **Myanmar:** Free Expression Myanmar
- **Nicaragua:** Abdías Zambrano, IPANDETEC
- **Nigeria:** Adeboro Odunlami, independent researcher
- **Serbia:** Mila Bajic, Asja Lazarević, Bojan Perkov, SHARE Foundation
- **Singapore:** Kirsten Han, independent researcher
- **South Africa:** Tshepiso Hadebe, PPM Attorneys
- **South Korea:** Yenn Lee, SOAS University of London
- **Sri Lanka:** Raisa Wickrematunge, independent researcher
- **Taiwan:** Ming-Syuan Ho, independent researcher
- **Thailand:** Emilie Pradichit and Letitia Visan, Manushya Foundation
- **The Gambia:** Nasiru Deen, Gambia Press Union
- **Tunisia:** Yosr Jouini, independent researcher
- **Turkey:** Gürkan Özturan, Media Freedom Rapid Response Coordinator at the European Centre for Press and Media Freedom
- **United Kingdom:** Edina Harbinja, Aston University
- **United States:** Claire Park, independent researcher
- **Uzbekistan:** Ernest Zhanaev, independent researcher
- **Venezuela:** Raisa Urribarri, Universidad de Los Andes (Emeritus)
- **Vietnam:** Trinh Huu Long, Legal Initiatives for Vietnam
- **Zambia:** Bulanda T. Nkhowani, Paradigm Initiative
- **Zimbabwe:** Nompilo Simanje, Legal and ICT Policy Officer, Media Institute of Southern Africa

*Researchers for Angola, Bahrain, Bangladesh, Belarus, China, Ecuador, Egypt, Ghana, India, Iran, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Morocco, Pakistan, Philippines, Russia, Rwanda, Saudi Arabia, Sudan, Uganda, the United Arab Emirates, and Ukraine wished to remain anonymous.*

## Advisers

- Abrar Mohamed Ali, Researcher, African Digital Rights Network
- Eto Buziashvili, Atlantic Council's Digital Forensic Research Lab
- Jonathan Corpus Ong, Associate Professor at the University of Massachusetts Amherst and Research Fellow at the Shorenstein Center at Harvard University
- Angel Diaz, Visiting Assistant Professor of Law at USC Gould School of Law
- Alena Epifanova, Research Fellow at International Order and Democracy Program, German Council on Foreign Relations
- Alyssa Kann, Research Associate at Atlantic Council's Digital Forensic Research Lab
- Jeff Kosseff, Associate Professor, Cyber Science Department, United States Naval Academy
- Artur Pericles Lima Monteiro, Wikimedia Fellow, Information Society Project, Yale Law School, and member, Constitution, Politics, and Institutions research cluster, University of São Paulo
- Iria Puyosa, Senior Research Fellow at Atlantic Council's Digital Forensic Research Lab
- Hakeem Dawd Qaradaghi, independent researcher
- Xiao Qiang, Founder and Editor-in-Chief of China Digital Times and research scientist at the School of Information, University of California Berkeley

# HOW TO CITE THIS REPORT

Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. *Freedom on the Net 2022*, Freedom House, 2022, freedomonthenet.org.

Shahbaz, Funk, and Vesteinsson, "Countering the Authoritarian Overhaul of the Internet," in Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. *Freedom on the Net 2022*, Freedom House, 2022, freedomonthenet.org.

"Angola," in Shahbaz, Funk, Friedrich, Vesteinsson, Baker, Grothe, Masinsin, Vepa, Weal eds. *Freedom on the Net 2022*, Freedom House, 2022, freedomonthenet.org.

# EXHIBIT 38

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# CROSS-BORDER DATA TRANSFERS & INNOVATION

In today's rapidly changing world, the future depends on technological and scientific progress: Governments and industries must continually innovate to address emergent health, development, and sustainability challenges. Countries can foster innovation with the right mix of policy tools.[1] Those tools include cross-border access to technology; the ability to share knowledge, ideas, and information across international IT networks; and improved digital connectivity and inclusiveness. Applying these tools can also help ensure that innovations are widely disseminated–spreading their societal benefits for all, including safer and more rewarding work, improved health, and a cleaner environment.

**Today's challenges call for creative and inventive endeavors on a collaborative, coordinated, and cross-border scale.**

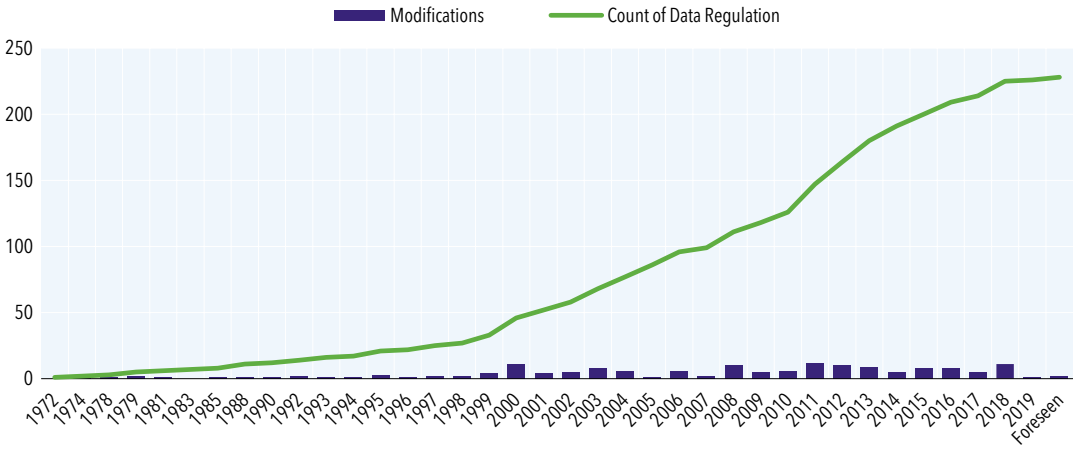
## CROSS-BORDER DATA TRANSFERS ARE IMPORTANT TO INNOVATION

Technological and scientific endeavors are inherently cross-border in a connected global economy. For example, multinational teams of biopharmaceutical researchers engage in cross-border collaboration in many ways, including by leveraging artificial intelligence (AI) to identify potential drug candidates within large drug discovery data sets consolidated from around the world.[2] Similarly, cross-border access to remote work and remote learning technologies is necessary for workers, engineers, technicians, and students to collaborate across vast distances in an era of social distancing.[3] Scientific progress and technological competitiveness require the exchange of information and ideas across borders. Rising digital trade restrictiveness threatens this exchange.

> **"[F]or data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies. This may, at least in part, explain why binding rules on cross-border data transfers and localization restrictions have been introduced in a number of RTAs and have been discussed [at the WTO]."**
>
> WTO, *Government Policies to Promote Innovation in the Digital Age*, 2020 World Trade Report (2020)

Data policy measures, which may seek to achieve a range of policy objectives, are growing rapidly, increasing by at least 800% between 1995 and 2015.[4] How can governments ensure that such data-related policy measures facilitate–rather than impede–innovation? A growing consensus of authorities looks to whether measures are (1) transparent; (2) interoperable; (3) non-discriminatory; and (4) no more trade restrictive than necessary.[5] Human creativity and ingenuity depend heavily on access to, and exchange of, information, ideas, and knowledge. **For this reason, unnecessary or discriminatory data localization mandates and cross-border data transfer restrictions–which impede that access and exchange–are particularly detrimental to innovation.**

**Figure 1. OECD Statistics on Data Regulation Growth, 1972–2019**
Cumulative number of data regulations




**Source:** OECD, *Trade and Cross-Border Data Flows* (2019), https://doi.org/10.1787/b2023a47-en

**Data policy measures tend to deter investment in R&D and innovation when they are opaque, discriminatory, more restrictive than necessary, or incompatible with other legal regimes.**

## CROSS-BORDER DATA TRANSFERS ARE IMPORTANT AT EVERY STAGE OF THE INNOVATION LIFE CYCLE

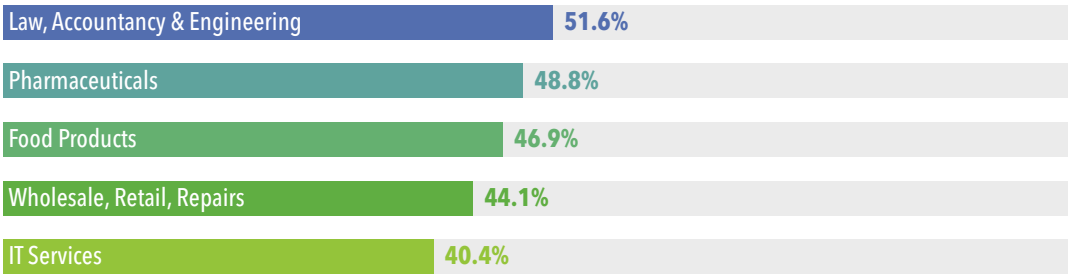
Cross-border data transfers support many aspects of innovation.

### Data Transfers and Core Innovative Processes

In every sector, cross-border data transfers play an integral role in R&D, and other core innovative and creative functions. For example, in both semiconductor design and biopharmaceutical research, R&D depends on access to research data from laboratories and research institutions from sources across the world, as well as collaboration, joint research, and the exchange of ideas and knowledge among teams of inventors, designers, authors, and other creators and innovators in different countries. All these activities also rely on cloud computing and data storage to facilitate cost-effective analysis and storage of R&D data.[6]

This trend is also reflected in the growing percentage of scientific and research publications with co-authors from multiple countries. Figure 2 identifies the top five categories for such.

**Figure 2. Top Five Sectors of Scientific Publications With International Co-authorship**




**Source:** H. Dernis, P. Gkotsis, N. Grassano, S. Nakazato, M. Squicciarini, B. van Beuzekom, A. Vezzani, *World Corporate Top R&D Investors: Shaping the Future of Technologies and of AI*, A joint JRC and OECD Report (2019), http://www.oecd.org/sti/world-corporate-top-rd-investors-shaping-future-of-technology-and-of-ai.pdf.

## Data Transfers and Artificial Intelligence

Businesses of all sizes in every sector of the economy can benefit from smart and responsible AI. Increasingly, R&D is conducted across cloud-enabled and networked environments that apply AI-based analytical software tools to research, statistical, and other data transferred around the world.[7] As explained by international science- and innovation-oriented organizations[8] and by national authorities,[9] such R&D depends on applying AI-related tools to globally sourced data sets. Data sets consolidated across IT networks and borders can be analyzed (e.g., through machine learning or data analytical techniques) to identify meaningful insights, patterns, and connections that can aid R&D teams in discovering and developing novel solutions to scientific and technical challenges.

## Data Transfers and Regulatory Approval and Licensing Processes

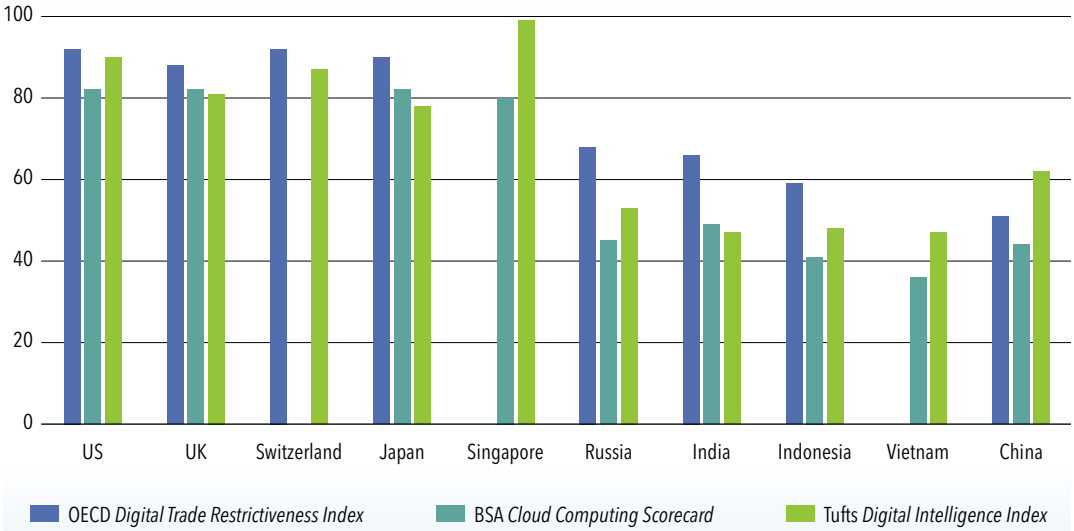
Transferring data across borders is also critical to advancing governmental approvals and licensures for innovative connected devices–from aircraft and vehicles, to medical devices and machine tools. Data transfers are not merely important to the functioning of these connected devices, but also to their regulatory testing and approval.

For example, doctors rely on life-enhancing connected medical devices that diagnose or treat endocrine, cardiovascular, oncological, or neurological conditions, which in turn depend on device producers' ability to share comprehensive safety and operational data with regulators such as the US Food & Drug Administration (FDA), the European Medicines Agency (EMA), and other members of the International Medical Device Regulators Forum (IMDRF). Restrictions on cross-border data transfers hinder the ability to share innovative device prototypes, scientific evidence necessary for premarket approval, and post-market surveillance data.

## Data Transfers and Intellectual Property Application Processes

Innovators must transfer information across borders to apply for intellectual property (IP) rights with authorities in different countries. Access to data from multiple countries–such as prior art references–is an integral part of the patent application examination process. Likewise, transferring data (including inventor files, etc.) across borders is critical to advancing local innovation in developing countries through the international Inventor Assistance Program (IAP), which provides under-resourced developing country inventors with *gratis* legal representation from around the world.[10]

**Measures of Digital Trade Openness, Cloud Readiness, and Digital Evolution[11]**




**Data localization mandates and data transfer restrictions are particularly detrimental to innovation because they impede information access and exchange. Trade barriers that impede data transfers undermine basic research and scientific activity, as well as the development of new treatments and inventions to protect human health and welfare.**

## Data Transfers and Market Access for Innovative Products

Cross-border data transfers are also necessary for servicing and supporting many exported products. Data localization mandates and data transfer restrictions can directly impede the ability to provide service or support, impairing foreign market access. With so many innovative exported products functionally depending on satellite or other cross-border data communications (e.g., IoT software applications in the aerospace, automotive, and agricultural machinery sectors; legitimate music and video streaming services; scientific publication databases), cross-border data transfer restrictions make it much more difficult for innovators and creators to sell or provide support to their products abroad.

## Data Transfers and the Dissemination of the Benefits of Innovation

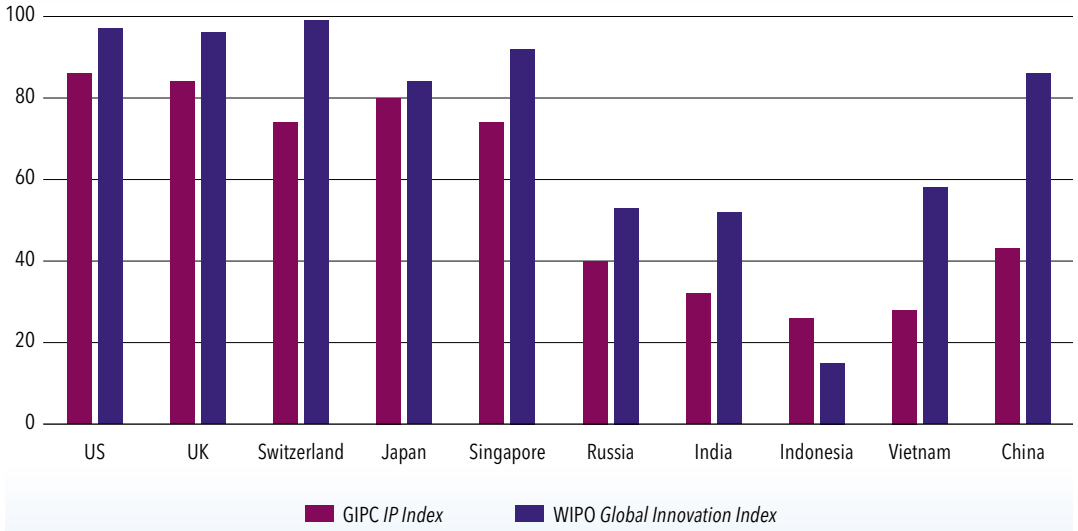
Cross-border data transfers are necessary to bring the benefits of innovations to populations at large. For example, in a recent WTO report describing data-related tools to facilitate an innovation-centric response to COVID-19, almost all (if not all) the tools described depended on the ability to transfer data across borders.[12]

In concrete terms, a country that unnecessarily limits cross-border data transfers limits its own workers' and citizens' access to technologies and data sources that are critical to development, innovation, and the transfer of technology. These include (1) software and ICT solutions that offer local Micro, Small, and Medium-Sized Enterprises (MSMEs) access to foreign buyers and financing; (2) scientific, research, and other publications that allow local inventors, designers, researchers to access knowledge from abroad; and (3) manufacturing data, blueprints, and other operational information necessary to support local construction, manufacturing, and service-related jobs.

> **"Technological advancement goes hand in hand with increased global data flows. Data are more valuable (and 'big data' especially so), thus increasing incentives to share them, including across borders."**
>
> OECD, *Digital Economy Outlook* (2020)

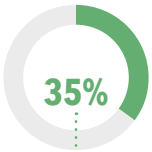
Innovation- and data-restrictive trade barriers undermine the core TRIPS Agreement objective of promoting, "technological innovation and…the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations."

### Measures of Innovation-Related Performance[13]




## DATA SNAPSHOT ON CROSS-BORDER INNOVATION

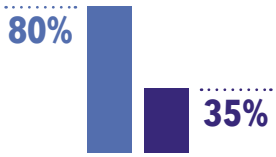
### Research Collaboration Across Borders and Nationalities[14]



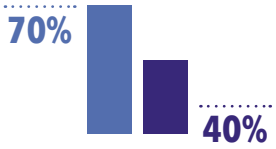

of scientific publications have multiple country co-authors


of certain AI-related publications (e.g., in the electrical and chemical arts) are more likely to have multiple country co-authors than single country authors

### Inter- and Intra-Company Innovation, Including Across Borders[15]




**80%** of respondents from digitally advanced companies say their **organizations foster innovation through partnerships** with other organizations, as compared with **35%** of respondents at less digitally advanced companies




**70%** of respondents from digitally advanced companies say that **cross-functional teams are supported and given freedom to innovate**, as compared with less than **40%** of respondents at less digitally advanced companies

## CONCLUSION

Data localization mandates and cross-border data transfer restrictions threaten the very innovation that is necessary to solve emergent health, climate, and economic challenges across the globe. Countries should refrain from imposing such restrictions, and should ensure any rules impacting cross-border data transfers (1) adhere to good regulatory practices, including transparency, (2) are non-discriminatory, (3) are necessary to achieve a legitimate objective and do not impose greater restrictions than necessary, (4) respect accountability models aligned with international best practices, and (5) are interoperable with other countries' legal frameworks.

### Endnotes

1 *See e.g.*, Arthur D. Little, *The National Innovation Ecosystem: A Holistic Approach to Designing an Effective National Innovation Ecosystem* (2020), https://www.adlittle.com/sites/default/files/viewpoints/adl_national_innovation_0.pdf.

2 *See e.g.*, Ganes Kesari, "Why Covid Will Make AI Go Mainstream in 2021," *Forbes* (December 2020), https://www.forbes.com/sites/ganeskesari/2020/12/21/why-covid-will-make-ai-go-mainstream-in-2021-top-3-trends-for-enterprises/?sh=1d83a3f6797a; Arshadi et al., "Artificial Intelligence for COVID-19 Drug Discovery and Vaccine Development," *Frontiers in Artificial Intelligence* (August 2020), https://www.frontiersin.org/articles/10.3389/frai.2020.00065/full; Ungaro, et al., "Accelerating Vaccine Research for COVID-19 with High-Performance Computing and Artificial Intelligence," *HP Enterprise* (2020), https://www.hpe.com/us/en/newsroom/blog-post/2020/04/accelerating-vaccine-research-for-covid-19-with-high-performance-computing-and-artificial-intelligence.html; IEEE, "Can AI and Automation Deliver a COVID-19 Antiviral While It Still Matters?" *IEEE Spectrum* (2020), https://spectrum.ieee.org/artificial-intelligence/medical-ai/can-ai-and-automation-deliver-a-covid19-antiviral-while-it-still-matters.

3 *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (October 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf; *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (September 2020), https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf.

4 Martina Ferracane, *Restrictions on Cross-Border Data flows: A Taxonomy*, ECIPE Working Paper (2017), https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf. *See* OECD, *Trade and Cross-Border Data Flows* (2019), https://doi.org/10.1787/b2023a47-en.

5 *See e.g.*, OECD, *Principles for Market Openness in the Digital Age*, Working Party Report, TAD/TC/WP(2018)17/FINAL (2018) ("[A]pproaches to digital trade [should] be: *Transparent*: helping reduce the costs of operating across different markets and clarifying the rules that apply to different products by providing up-to-date information and enabling access for different stakeholders to the policy-making process. *Non-discriminatory*: ensuring that domestic incumbents are not favoured over foreign firms, or certain foreign firms over others, when operating in the digital space and selling like products in view of levelling the playing field. *Not unnecessarily trade restrictive to meet desired policy-objectives*: ensuring that the least trade restrictive tool is being used to meet desired objectives. This might involve drawing on the expertise of different policy communities and business. For instance, where digital trade might raise technical problems which might best be tackled through technical solutions. *Interoperable*: helping devices better speak to each other through more private sector discussion on technical specifications and allowing flexibility so that rules or standards are also based on common understandings, or at least offer possibilities of not mutually exclusive coexistence. Interoperability need not be forced, it might come naturally as a result of the processes that the above stated principles support.") http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)17/FINAL&docLanguage=En.

*Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in the WTO Negotiations on E-Commerce* (January 26, 2021) (stating that, "Any [JSI] agreement should discipline unnecessary or discriminatory data localization mandates and data transfer restrictions. Any agreement should also be guided by principles of transparency and interoperability among legal frameworks; should apply across all economic sectors; and should require all countries to adopt or maintain legal frameworks to protect personal information.") https://iccwbo.org/content/uploads/sites/3/2021/01/multi-industry-statement-on-crossborder-data-transfers-and-data-localization.pdf.

Global Data Alliance, *Cross-Border Data Policy Principles* (2021) (outlining six policy principles, including that any rules impacting cross-border data transfers should be (1) developed and maintained in accordance with good regulatory practices; (2) non-discriminatory; (3) necessary to achieve a legitimate objective and not impose greater restrictions than necessary; and (4) interoperable), at _____ [au: complete cite?]

6 *See generally* Arthur D. Little, *Innovation Management* (2021) (identifying a range of innovation-enhancing digital tools and processes), https://www.adlittle.com/en/RightInnovationTools.

*OECD Science, Technology and Industry Scoreboard 2017: The Digital Transformation* (Paris: OECD Publishing, 2017), https://doi.org/10.1787/9789264268821-en. (Collaborations may take a variety of forms including international co-inventions involving several firms, both small and large, joint research ventures by private and public entities (e.g. firms and universities or public research organisations), and formal and informal networks of scientists. In the case of multinational corporations, international collaboration often reflects a process whereby companies rely on research and innovation facilities located in several economies to draw upon geographically dispersed knowledge and/or develop complementarities with foreign inventors.)

7 *See* Joshua Meltzer, *The Impact of Artificial Intelligence on International Trade* (Washington, DC: Brookings Institution, 2018), https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/.

[8] *See e.g.*, WIPO, *WIPO Technology Trends 2019, Artificial Intelligence* (2019), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf; WIPO, *Frequently Asked Questions: AI and IP Policy* (2021), https://www.wipo.int/about-ip/en/artificial_intelligence/faq.html; WIPO, *Artificial Intelligence and Intellectual Property Policy* (2020), https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html.

[9] *See e.g.*, Canadian Intellectual Property Office, *Processing Artificial Intelligence: Highlighting the Canadian Patent Landscape* (2020), https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/vwapj/AI_Report_ENG.pdf/$FILE/AI_Report_ENG.pdf; Japan Patent Office, *Recent Trends in AI-Related Inventions* (2019), https://www.jpo.go.jp/e/system/patent/gaiyo/ai/document/ai_shutsugan_chosa/report-2019.pdf; IP Australia, *Machine Learning Innovation: A Patent Analytics Report* (2019), https://www.ipaustralia.gov.au/sites/default/files/reports_publications/patent_analytics_report_on_machine_learning_innovation.pdf; UKIPO, Artificial Intelligence: A Worldwide Overview of AI Patents and Patenting by the UK AI Sector (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf; European Patent Office, *Patents and the Fourth Industrial Revolution* (2017), documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/%24File/fourth_industrial_revolution_2017__en.pdf; USPTO, *Artificial Intelligence Webpage* (2021), https://www.uspto.gov/initiatives/artificial-intelligence; USPTO, *Public Views on Artificial Intelligence and Intellectual Property Policy* (2020), https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf; USPTO, *Inventing AI: Tracing the Diffusion of Artificial Intelligence with US Patents* (October 2020), https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf.

[10] WIPO, *Inventor Assistance Program Webpage* (2021) ("The Inventor Assistance Program—a WIPO initiative in cooperation with the World Economic Forum—is the first global program to match developing country inventors and small businesses with limited financial means with…experts [who] provide *pro bono* legal assistance to help inventors secure patent protection."), https://www.wipo.int/iap/en/; David Kappos, *3 Ways to Improve the Patent System and Protect Inventors*, World Economic Forum (2019), https://www.weforum.org/agenda/2019/06/ways-to-improve-the-patent-system-and-protect-inventors/.

[11] This chart comprises data from the 2019 OECD *Digital Trade Restrictiveness Index*, the 2018 BSA *Cloud Computing Scorecard*, and the 2020 Tufts University *Digital Intelligence Index* (specifically, its scoring of the state of "digital evolution" in the listed countries).

- The 2018 BSA *Cloud Computing Scorecard* highlights data localization measures and/or other digital trade restrictions in China, India, Indonesia, Russia, and Vietnam, while noting the absence of such restrictions in Australia, Canada, Japan, Singapore, the UK, and the US. https://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf.
- The 2019 OECD *Digital Trade Restrictiveness Index* ranks China, India, Indonesia, and Russia among the most digitally trade restrictive major economies, and ranks Australia, Canada, Japan, Switzerland, the UK, and the US among the least trade restrictive major economies. https://stats.oecd.org/Index.aspx?DataSetCode=STRI_DIGITAL.
- The 2020 Tufts University *Digital Intelligence Index* observes that, "[l]ess data protectionism coupled with stronger data privacy protections will improve competitiveness and innovation…Singapore, Japan, Canada, and the Netherlands, illustrate this approach well, with greater openness to data flows and strong privacy protections. Economies…such as China, Russia, Turkey, and Saudi Arabia score poorly on both these measures." https://sites.tufts.edu/digitalplanet/files/2020/12/digital-intelligence-index.pdf.

For comparability purposes, we recalculated each of the foregoing report rankings (where necessary) as a percentage (out of 100 points). EU member states are omitted from this analysis because of comparability challenges in separating EU-wide policies from specific member state policies.

[12] *See generally*, World Trade Organization, The TRIPS Agreement and COVID-19 (2020), https://www.wto.org/english/tratop_e/covid19_e/trips_report_e.pdf.

[13] This chart comprises data from the 2019 WIPO *Global Innovation Index* and the Global Innovation Policy Center's 2019 *IP Index*.

- The Global Innovation Policy Center's 2019 *IP Index* ranks Japan, Singapore, Switzerland, the UK, and the US among the top major innovation economies, while placing China, India, Indonesia, and Russia in the lower half of its rankings. https://www.theglobalipcenter.com/ipindex2019-chart/.
- The 2020 *Global Innovation Index* ranks Singapore, Switzerland, the UK, the US, and several other European countries among the top major innovation economies, while placing China, India, Russia, and Indonesia in the 14th, 47th, 48th and 85th positions respectively. It bears noting that China is ranked in the 14th position, although there is an ongoing public debate regarding the role of non-commercial considerations (e.g., subsidies for patent and trademark filings, incidence of bad faith trademark applications, etc.) in driving high rates of trademark and patent filings in China. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf.

For comparability purposes, we recalculated each of the foregoing report rankings (where necessary) as a percentage (out of 100 points). EU member states are omitted from this analysis, because of comparability challenges in separating EU-wide policies from specific member state policies.

[14] H. Dernis, P. Gkotsis, N. Grassano, S. Nakazato, M. Squicciarini, B. van Beuzekom, A. Vezzani, *World Corporate Top R&D Investors: Shaping the Future of Technologies and of AI*, A joint JRC and OECD Report (2019), http://www.oecd.org/sti/world-corporate-top-rd-investors-shaping-future-of-technology-and-of-ai.pdf.

[15] MIT Sloan Business Management Review, *Accelerating Digital Innovation Inside and Out: Findings from the 2019 Digital Business Global Executive Study and Research Project* (2020), https://sloanreview.mit.edu/projects/accelerating-digital-innovation-inside-and-out/.

# EXHIBIT 39

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

January 30, 2024

Docket No. USTR-2023-0014 (88 Fed. Reg. 84869)

Claire Avery-Page
Director for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508
Attn: Special301@ustr.eop.gov

Dear Ms. Avery-Page,

The Global Data Alliance (GDA)[1] provides the following information in response to the notice published by the Office of the US Trade Representative (USTR) seeking comments on the 2023-2024 Special 301 review under Section 182 of the Trade Act of 1974 (Special 301). The GDA also hereby requests the opportunity to testify at the Special 301 hearing.

GDA members rely on intellectual property (IP) – including copyrights and related rights, patents, trademarks, and trade secrets – and on the ability to transfer data across borders in many aspects of their international operations. However, GDA members increasingly face market access barriers in the form of unnecessary and discriminatory data localization mandates and data transfer restrictions that have a direct impact on their ability to acquire, protect, enforce, and enjoy the benefits of, IP rights. Between 1995 and 2015, such data-related trade barriers have increased by over 800%, and the rate of increase has further accelerated in recent years.[2]

Section 182 of the Trade Act of 1974, as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act of 1994 (19 USC § 2242), requires USTR to identify countries based on *inter alia,* policies that deny "fair and equitable market access to United States persons that rely upon intellectual property protection." In this submission, we focus on market access barriers that impact IP-intensive industries by mandating data localization or restricting legitimate data transfers.[3]

National policies on cross-border data transfers are – alongside standards of IP protection and enforcement – important determinants of the ability of economies to create, innovate, and generate new IP. They also are important measures of the openness and fairness of those markets to non-nationals who rely on IP in their commercial operations.

Innovation and market access-limiting data localization mandates and data transfer restrictions cite "indigenous innovation" or other priorities, yet they often undermine the very priorities that they purport to support. These restrictions take many forms: Sometimes the policies expressly require data to stay in-country. Sometimes, these policies impose unreasonable conditions on sending data abroad or prohibit such transfers outright. In other cases, the policies require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors. For example, these measures may:

- Reflect a choice of policy tools that are significantly more trade-restrictive than necessary to achieve the stated public policy goal;
- Constitute unnecessary, unjustified and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or
- Treat cross-border data transfers less favorably than domestic data transfers.

Sustained attention to these issues is critical, because in today's digitized economy, research and development (R&D), IP generation, and other creative and scientific endeavors are increasingly cross-border in nature.

For example, artificial intelligence (AI) involves the application of analytical techniques to data generated in various countries, transferred across borders, and consolidated into larger data sets. AI helped fast-track the COVID-19 vaccine, cutting timelines from years to months, as researchers analyzed data transferred from around the world to quickly identify potential vaccine treatments.[4] Trade barriers that impede data transfers undermine the potential of AI, as they prevent the consolidation of representative data sets necessary to conduct AI analysis. In this way, these trade barriers directly impede new innovations and creations that could advance human health and welfare.

Failing to attend to data-related trade barriers also threatens other IP priorities – from engaging in cross-border R&D, to protecting brands, to investigating IP infringement, to conducting comprehensive prior art searches. Likewise, with so many patented or copyrighted innovations functionally dependent upon satellite or other cross-border data communications (e.g., IoT software applications in the aerospace, automotive, and agricultural machinery sectors; music and video streaming services that disseminate licensed film or music content), cross-border data transfer restrictions make it difficult, if not impossible, for innovators and creators to sell or provide support to their IP-protected products abroad – interfering with their ability to enjoy the benefits of their IP rights abroad. In each of the foregoing examples (and many others), innovation and market access-limiting data localization mandates and data transfer restrictions impact IPR holders in respect of the availability, acquisition, scope, maintenance, enforcement, and enjoyment of IP rights.

The Global Data Alliance urges USTR to attend to the growing threat to global innovation and IP protection presented by unfair market access barriers in form of cross-border data transfer restrictions and data localization mandates. We look forward to your questions and comments.

**Submission of Global Data Alliance for**
**Special 301 Annual Review**

This submission responds to USTR's solicitation of information relevant to the Special 301 Annual Review, and contains the following major sections:

A. Cross-Border Data Transfers, Innovation, and Intellectual Property — Overview ....4
B. Cross-Border Data Transfers and the Innovation Lifecycle ....4
1. Data Transfers and Core Innovation ....5
2. IP Acquisition, Registration, and Maintenance ....5
3. IP Enforcement and Brand Protection ....5
4. IP Commercialization ....6
C. Data-Related Market Access Barriers that Impact Innovation and IP ....6
D. Conclusion ....6

### A. Cross-Border Data Transfers, Innovation, and Intellectual Property — Overview

Many international organizations recognize the close nexus between cross-border data transfers and innovation. The G20 has underscored that the "[c]ross-border flow of data, information, ideas and knowledge generates … greater innovation,"[5] and the WTO has similarly emphasized that, "for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies."[6] Likewise, UNCTAD has warned that barriers driven by "data nationalism" reduce "opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation."[7]

By their nature, data localization mandates and data transfer restrictions tend to impede the cross-border exchange of knowledge, technical know-how, laboratory analysis, scientific research, and other information. Data localization mandates and unnecessary data transfer restrictions hurt local innovation because a country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are integral to innovation and the dissemination of technology. These include: (a) scientific, research, and other publications; (b) manufacturing data, blueprints, and other operational information; and (c) digital tools for remote work, laboratory research, and other innovation-related applications.[8] Faced with higher costs to access or exchange information and an unpredictable environment for R&D investments, local industries face increasing innovation challenges. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for R&D.

### B. Cross-Border Data Transfers and the Innovation Lifecycle

Cross border data transfers are critical at every stage of the innovation life cycle, and in all facets of IP legal frameworks. This includes: (1) early stages of innovative and creative processes, including basic R&D, initial conception, and design; (2) the acquisition and maintenance of IP rights; (3) the enforcement of IP rights and brand protection activities; and (4) the ongoing enjoyment and commercialization of those IP rights.

The WIPO Global Innovation Index (GII), which ranks 132 countries against 81 innovation and IP-related indicators and which aims to help policymakers "discover what works best in producing an ecosystem where people can achieve their highest potential, innovating and creating to improve lives everywhere," highlights these risks.[9] The GII does not directly account for countries' cross-border data restrictions, despite the fact that several countries that impose such barriers have stated their belief that such barriers advance "indigenous innovation" goals and despite the close nexus between the cross-border exchange of knowledge, ideas, and information and cross-border access to technology (on the one hand) and R&D, scientific endeavor, innovation, creativity, and intellectual property generation (IP) (on the other). Many of the GII's metrics would likely be directly impacted by new cross-border data restrictive measures in China, India, and Vietnam, etc., including strict data localization mandates and prohibitions on transfers of "important," "sensitive," or "critical" information (whether "personal" or "non-personal"). These measures – often implemented quickly and with minimal input from the public – directly impact GII metrics in the cross-border context, including: (1) legal and operational stability; (2) regulatory quality; (3) ICT access and use; (4) gross expenditures on R&D; (5) university-industry R&D collaboration; (6) cross-border knowledge absorption and output; (7) research talent; and (8) High-tech and ICT services imports.[10]

### 1. Data Transfers and Core Innovation

In every sector, cross border data transfers play an integral role in basic research and development (R&D), and other core innovative and creative functions. For example, in semiconductor design as well as biopharmaceutical research, basic R&D depends upon access to globally sourced research materials from laboratories and research institutions from across the world, as well as collaboration, joint research, and the exchange of ideas and knowledge among teams of inventors, designers, authors, and other creators and innovators in different countries.

*Trade barriers that impede data transfers undermine basic research and scientific activity, as well as the development of new treatments and inventions to protect human health and welfare.*

This collaborative, multinational approach to technological and creative endeavor integrates and binds together the international IP legal framework as well as scientific and artistic communities. R&D teams across universities, commercial labs, and enterprises in different countries collaborate across borders to develop new products, cures, and other advances protected by patents, trade secrets, copyrights and trademarks. Typically, such R&D also often requires the use of copyrighted software solutions and research data accessible across cloud-enabled and networked environments, as well as the application of artificial intelligence (AI)-based analytical techniques to data transferred across borders and consolidated into larger data sets.[11]

As explained by the World Intellectual Property Organization (WIPO),[12] the US Patent & Trademark Office (USPTO),[13] and other IP authorities,[14] such R&D depends upon the application of AI-related tools to globally sourced data sets. Data sets consolidated across IT networks and borders can be analyzed (e.g., through machine learning or data analytical techniques) to identify to meaningful insights, patterns, and connections that can aid R&D teams in the discovery and development of novel solutions to scientific and technical challenges.

### 2. IP Acquisition, Registration, and Maintenance

The ability to transfer data across borders is also critical to the acquisition of IP rights. Applicants must be able to transfer information across borders in order to apply for patent, copyright, trademark or other rights in a coordinated manner with IP office authorities in different countries. Access to data from multiple countries – such as prior art references – is also an integral part of the patent application examination process. They must also be able to transfer data across borders in order to avail themselves of WIPO-administered international registration and examination frameworks for IP rights, such as the Patent Cooperation Treaty, the Madrid Registry for trademarks, or the Hague System for the International Registration of Industrial Designs.

Data localization mandates and data transfer restrictions that prohibit the transfer of “important,” “critical,” or “sensitive” data (e.g., under Chinese measures discussed below) create uncertainty regarding the future ability to transfer information and data necessary to these procedures for the acquisition, registration, and maintenance of IP rights.

### 3. IP Enforcement and Brand Protection

In today's global marketplace, IP infringement is increasingly complex and globalized, requiring sophisticated investigatory tools. No IP enforcement program can be effective without the ability to trace – on a cross-border basis – counterfeiting, commercial scale piracy, and other illicit activities with insights and information derived from foreign source countries, distribution hubs and networks, and end-user markets. Data localization measures and unnecessary data transfer restrictions directly interfere with the ability to investigate and counteract transnational IP infringing activities.

Cross-border data transfers are critical to many aspects of IP enforcement - from monitoring marketplaces, to gathering evidence of infringement in multiple locations, to researching details of illicit networks, to using administrative or judicial tools in multiple jurisdictions to preserve evidence and secure recourse. The ability to track and trace infringing activities across IT networks and borders is particularly important as many infringing acts involve an online element, whether via the offer and sale of infringing articles online; the cross-border

exfiltration of source code, trade secrets or other proprietary data; the circumvention of technological protection measures; or the unauthorized and unlicensed use of copyrighted software or trademarks in an online environment.

> *Cross border access to information is frequently necessary for IP infringement investigations (e.g., obscuring patterns and trends in counterfeiting and piracy and making it more difficult for investigators to obtain forensic data to identify criminal enterprises engaged in counterfeiting, piracy, and other IP infringement)*

#### 4. IP Commercialization

Cross-border data transfers are also critical to the ability of enterprises to commercialize and enjoy the benefits of their IP rights. When a country mandates data localization or restricts data transfers, it can easily frustrate the ability to enjoy the benefits of any IP right granted. With so many patented or copyrighted innovations functionally dependent upon satellite or other cross-border data communications (e.g., IoT software applications in the aerospace, automotive, and agricultural machinery sectors; music and video streaming services that disseminate licensed film or music content), cross-border data transfer restrictions make it difficult, if not impossible, for innovators and creators to sell or provide support to their IP-protected products or in foreign markets – interfering with their ability to secure a commercial return on, or otherwise enjoy the benefits of, their IP rights abroad.

### C. Data-Related Market Access Barriers that Impact Innovation and IP

As further detailed in the GDA's National Trade Estimate submission, some trading partners are erecting **unfair market access barriers** that affect GDA members who rely on IP in their commercial operations. The GDA does not provide specific country listing recommendations (as between Priority Watch List or Watch List) for these trading partners, but requests that the US government include the information submitted in its qualitative overall review of the referenced countries. Below is a brief preview of several measures described in greater detail in the Appendix.

### D. Conclusion

The Global Data Alliance welcomes the opportunity to provide this submission and looks forward to working with USTR to achieve meaningful progress in addressing the cross-border data policy concerns identified in this submission.

---

[1] The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. *See* Global Data Alliance, *About the Global Data Alliance* (2020), at: https://www.globaldataalliance.org/downloads/aboutgda.pdf

[2] https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf

[3] We do not address the first statutory element under section 182 of the Trade Act of 1974 relating to the adequacy and effectiveness of IP protections because the GDA is organizationally focused on issues relating directly to cross-border data policies. However, GDA members own extensive portfolios of trademarks, copyrights, patents, trade secrets, and other IP rights, and rely on other trade associations to represent their specific perspectives on substantive matters of IP protection and enforcement.

[4] *See e.g.,* Ganes Kesari, *Why Covid Will Make AI Go Mainstream In 2021*, Forbes (Dec. 2020), https://www.forbes.com/sites/ganeskesari/2020/12/21/why-covid-will-make-ai-go-mainstream-in-2021-top-3-trends-for-enterprises/?sh=1d83a3f6797a; Arshadi et al., *Artificial Intelligence for COVID-19 Drug Discovery and Vaccine Development*, Front. Artif. Intell. (Aug. 2020), https://www.frontiersin.org/articles/10.3389/frai.2020.00065/full ; Ungaro, et al., *Accelerating vaccine research for COVID-19 with high-performance computing and artificial intelligence*, HP Enterprise (2020), https://www.hpe.com/us/en/newsroom/blog-post/2020/04/accelerating-vaccine-research-for-covid-19-with-high-performance-computing-and-artificial-intelligence.html; IEEE, *Can AI and Automation Deliver a COVID-19 Antiviral While It Still Matters?* IEEE Spectrum (2020), https://spectrum.ieee.org/artificial-intelligence/medical-ai/can-ai-and-automation-deliver-a-covid19-antiviral-while-it-still-matters

[5] G20, *Ministerial Statement on Trade and Digital Economy* (2019), http://www.g20.utoronto.ca/2019/2019-g20-trade.html

[6] *See Trade Policy Review of India*, Secretariat Report, *supra* note 5.

[7] UNCTAD Digital Economy Report 2021, *supra* note 2.

[8] See Global Data Alliance, Cross-Border Data Transfers and Remote Work (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf; See Global Data Alliance, Cross-Border Data Transfers and Remote Health Services (Sept. 2020) https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf

[9] World Intellectual Property Organization, WIPO Global Innovation Index (Sept. 2021), at: https://www.wipo.int/global_innovation_index/en/2021/index.html

[10] Global Data Alliance, Cross-Border Data Transfers & Innovation (2021), at: https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf; Global Data Alliance, Cross-Border Data Transfers & Biopharmaceutical R&D (2021), at: https://globaldataalliance.org/wp-content/uploads/2021/09/09092021cbdtbiopharma.pdf; Global Data Alliance, Cross-Border Data Transfers & Economic Development (2021), at: https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf

[11] *See* Joshua Meltzer, *The impact of artificial intelligence on international trade*, Brookings Institution (2018), at: https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/

[12] *See e.g.,* WIPO, *WIPO Technology Trends 2019, Artificial Intelligence* (2019), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf; WIPO, *Frequently Asked Questions: AI and IP Policy (2021)*, https://www.wipo.int/about-ip/en/artificial_intelligence/faq.html; WIPO, *Artificial Intelligence and Intellectual Property Policy* (2020), https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html

[13] USPTO, *Artificial Intelligence Webpage* (2021), https://www.uspto.gov/initiatives/artificial-intelligence; USPTO, *Public Views on Artificial Intelligence and Intellectual Property Policy* (2020), https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf; USPTO, *Inventing AI - Tracing the Diffusion of Artificial Intelligence with US Patents* (Oct. 2020), https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf.

[14] *See e.g.,* Canadian Intellectual Property Office, *Processing Artificial Intelligence: Highlighting the Canadian Patent Landscape* (2020), https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/vwapj/AI_Report_ENG.pdf/$FILE/AI_Report_ENG.pdf; Japan Patent Office, *Recent Trends in AI-Related Inventions* (2019), https://www.jpo.go.jp/e/system/patent/gaiyo/ai/document/ai_shutsugan_chosa/report-2019.pdf; IP Australia, *Machine Learning Innovation – A Patent Analytics Report* (2019), https://www.ipaustralia.gov.au/sites/default/files/reports_publications/patent_analytics_report_on_machine_learning_innovation.pdf; UKIPO, Artificial Intelligence - A worldwide overview of AI patents and patenting by the UK AI sector (2019), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf ; European Patent Office, *Patents and the Fourth Industrial Revolution* (2017), documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/%24File/fourth_industrial_revolution_2017__en.pdf.

# EXHIBIT 40

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# SUPPLY CHAIN RESILIENCE SECTOR BRIEF

## CROSS-BORDER ACCESS TO DATA & MEDICAL TECHNOLOGY

Cross-border data transfers are essential for medical technology companies to detect, monitor, and treat medical conditions in a safe, effective, precise, and timely manner. Such data transfers help support the real-time monitoring of patient health conditions at the request of patients and their clinicians, offering benefits from the perspectives of patient comfort and care, remote analysis and treatment, monitoring for safety and efficacy of deployed technologies, refinements to treatment pathways and clinician education, and researching and engineering therapy improvements and innovations.

### Disseminating the Benefits of Medical Technologies Across Borders

Cross-border access to healthcare data improves access to medical technology solutions that can improve patient outcomes and medical treatments. Expanding cross-border access to such technologies and allowing for the secure and protected transmission of data across transnational digital networks can increase patient access, reduce health disparities, and support innovation in safe and cost-effective technologies that can enhance health outcomes and quality of life. This may include data collected in the normal use of the medical devices, in hospital and other medical records, and from other devices and consumer technologies. Such data is also typically aggregated, anonymized, pseudonymized, encrypted, and/or subject to other data security mechanisms, including privacy-enhancing technologies in the course of such transfers. Ultimately, the ability to realize the benefits of digitally connected medical technologies for patients around the world depends greatly on the medical technology industry's ability to successfully and securely access, aggregate, and use health data across transnational digital networks.

### Realizing the Cross-Border Potential of Data Analytics in Medical Technologies

Cross-border data analytics in medical technologies can help medical researchers and clinicians better understand and predict patterns and responses, including in longitudinal clinical studies, to improve patient treatments and outcomes. The data used in such analytical processes—aggregated, anonymized, pseudonymized, encrypted, and/or subject to other data security measures—may derive from clinical trials, collaborative research arrangements with hospitals and health systems, as well as the "real world" data generated by medical devices from their ongoing clinical use. For example, cross-border access to banks of surgical image data in actual clinical use or from videos recorded of surgeries anywhere in the world can help in training and developing data analytical models for safer, less costly, and more effective medical technology applications.

### Improving Real-Time Patient Diagnosis and Therapy

In many cases, medical technologies function optimally through real-time measurement, display, transmittal, and interpretation of cross-border data. When this functionality is compromised, such as through data transfer restrictions, these technologies do not achieve their full diagnostic and therapeutic potential.

- Diagnostic technologies include diagnostic electrocardiograms, magnetic resonance imaging (MRI) devices, and implantable or disposable equipment including portable testing kits. This includes insertable cardiac monitoring systems that provide long-term monitoring of the heart for suspected arrhythmias and atrial fibrillation. By leveraging predictive analytics through cross-border data, such systems have the potential to save lives by distinguishing different arrhythmia types and by providing the patient's clinicians with actionable information to inform their diagnostic and treatment decisions.
- Therapeutic technologies include radiotherapy equipment for oncology treatments, insertable cardiac monitors, implantable cardioverter-defibrillators, and grid mapping catheters. These technologies include

robotic assisted surgery systems, which are developed based on artificial intelligence (AI)-enabled digital models and which can improve surgical precision, consistency, technical capability, and speed in the operating room. These AI-enabled models can help identify procedural steps during an operation and learn based on the outcome. They can also monitor vital signs during surgery to flag possible issues, such as blood loss, and can detect when a surgical instrument has moved outside the area of interest and cut power as a safety precaution. In the intra-operative stage, the captured video can enhance displays (providing more relevant information); in the post-operative stage it can provide useful analytics.

### Ensuring Cross-Population Representation in Medical Technology Development

Cross-border data is critical to ensuring that new medical technologies are safe and effective across different demographics, populations, and regions. Diverse and representative data is critical to identify clinically relevant differences among patient cohorts to detect and eliminate potential distortion in treatment protocols and access, and other sources of bias and disparity. To avoid distortion or bias in the data sets used to develop new medical technologies, the underlying data sets should be drawn from a sufficiently large and diverse population of participants and should contain sufficient data to create and train relevant analytical models. Constraining such data sets within national borders would make the data less robust and could risk introducing unnecessary distortion or bias. Ultimately, the more data from diverse sources, the more accurate, safe, and unbiased patient outcomes will be.

# EXHIBIT 41

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# CROSS-BORDER DATA TRANSFERS & REMOTE HEALTH SERVICES

**Cross-border access to remote health technologies often allows access to state-of-the-art cybersecurity and privacy protections, along with advantages from a health care cost, timeliness, and patient access perspective.**

Few economic sectors have been more impacted by the recent shift to an international remote economy than the health care sector, as evidenced by the rise of telehealth and telemedicine (collectively referred to as "remote health services"), which are often delivered via cloud-enabled remote health technologies and software solutions. Remote health services can take many forms. In many countries, telemedicine services often involve a health care provider and a patient in the same region or locality engaging in medical consultation, yet that consultation frequently requires cross-border access to remote health care technologies that offer security and privacy features needed in the telemedicine context.

International organizations and national governments have highlighted the importance of access to these technologies during the COVID-19 crisis, underscoring the "urgency to expand the use of [remote] technology to help people who need routine care, and keep vulnerable [patients and those]…with mild symptoms in their homes while maintaining access to the care they need."[1] The scale and pace of the shift to remote health services are unprecedented: One recent study in a large municipal hospital system shows non-urgent telemedicine visits increasing by more than 4,000 percent in a short period–jumping from 95 daily telemedicine visits in early March 2020 to 4,209 daily telemedicine visits by mid-April 2020.[2] More broadly, telehealth services are expected to grow seven-fold growth by 2025.[3]

## WHAT ARE REMOTE HEALTH SERVICES?

Remote health services comprise both telemedicine and telehealth–terms with different meanings. Broadly understood to involve the provision of remote clinical services to support patients, "telemedicine" includes "the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, and patient and professional health-related education."[4] "Telehealth" has been defined to cover a broader scope of remote health care services, including remote non-clinical services, such as provider training, administrative meetings, and

continuing medical education.[5] An example of a telemedicine service is an online consultation with a local doctor who makes a diagnosis and treatment recommendations after (often AI-enhanced) analysis of images of suspicious skin tissue.[6] An example of a remote telehealth service is the WHO's efforts to make available remotely to health care providers worldwide information relating to the classification of illnesses, their causes, and symptoms.[7]

Effectively providing remote health services depends on cloud-enabled connected devices, which can include:

> real-time, audio-video communication tools [to]…connect physicians and patients in different locations; store-and-forward technologies that collect images and data to be transmitted and interpreted later; remote patient-monitoring tools such as blood pressure monitors, Bluetooth-enabled digital scales and other wearable devices that can communicate biometric data for review; verbal/audio-only and virtual check-ins patient portals, messaging technologies, etc.[8]

Thus, even in a private, online consultation between a primary care physician and his/her patient, the underlying technology often requires the cloud-based integration of provider-side technologies (such as clinical telemedicine hubs and laboratory testing equipment), and patient-side technologies (such as health-related Internet of Things (IoT) devices integrated with personal computers or smartphones). Even in the case of providers and patients located in the same country, both provider and patient often require cross-border access to overseas-based remote health platforms, portals, or other technologies that can offer the highest levels of security, privacy, and functionality.

## CROSS-BORDER DATA TRANSFERS ARE CRITICAL TO REMOTE HEALTH SERVICES

In many countries, cross-border access to cloud-based solutions undergirds remote health services. These cloud-based solutions allow doctors, nurses, researchers, laboratory specialists, pharmacists, and other health care providers to seamlessly support human health at the highest possible levels of security and functionality. We outline several relevant contexts below.

First, in many countries, telemedicine services offered by a provider to a patient within the same country may nevertheless involve **cross-border** access to a secure remote health technology hosted in another country. Such cross-border technology access may be necessary to offer a secure provider-patient interaction, to comply with legal requirements regarding the custody, storage, and disclosure of patient data, and to add new insights and functionality to diagnoses and treatment recommendations via AI-enhanced data analytics.[9] This includes:

- **Cross-border** access to state-of-the-art cyber, encryption, authentication, and blockchain technologies provided from cloud-based servers in another jurisdiction—protecting the privacy of patient data and guarding against unauthorized monitoring, intrusion, or data exfiltration; and
- **Cross-border** access to health care data analytics solutions that can analyze local data samples against databases of relevant information gathered from all over the world—enhancing the reliability and accuracy of diagnoses and treatment recommendations.[10]

Second, telehealth collaboration and research may be conducted among medical researchers and other professionals through:

- **Cross-border** collaboration, research, or expert consultations among providers or other specialists located in different countries;
- **Cross-border** exchange of data with laboratories or advanced research facilities with particular expertise in different types of analysis or testing; and
- **Cross-border** consolidation of anonymized data sets from around the world for purposes of real-time statistical tracking, analytics, and monitoring of aggregated anonymized data–e.g., to identify health trends, epidemiological patterns, or localized disease outbreaks.

**Telehealth services are expected to grow seven-fold by 2025 in the US. One major US regional health system has seen a 4,000 percent increase in demand for such services, from 95 daily telemedicine visits in early March 2020 to 4,209 daily telemedicine visits by mid-April 2020.**

Finally, in some jurisdictions, depending upon medical licensure and other legal requirements, telemedicine services may be provided directly to patients and health care information consumers through:

- **Cross-border** provision to patients of consultations, remote second opinions, or other information from a provider in one country to a patient in another; and
- **Cross-border** humanitarian assistance to underserved populations. According to the WHO, "telemedicine networks around the world deliver humanitarian services on a routine basis, many to low-income countries. These networks provide tele-consultations for physicians and other health professionals needing advice about the clinical management of difficult cases, and some also provide education."[11]

Please note that the cross-border provision of provider-to-patient telemedicine services is by no means universally accepted, as the rules governing telemedicine differ by jurisdiction–with varying approaches to regulatory oversight, licensing board requirements, reporting mandates, equipment specifications and other technical regulations, and so forth.

## BENEFITS AND LIMITATIONS OF REMOTE HEALTH SERVICE

Telemedicine services, secured and enabled through cross-border access to best-in-class technologies, come with both limitations and benefits. On the one hand, there are inherent limitations to the remote clinical environment: Many conditions cannot be diagnosed or treated by telemedicine services, nor can those services fully substitute for in-person medical treatment. However, telemedicine can help to relieve capacity constraints at hospitals, while reducing the spread of disease. It may be deployed more effectively where, for example, the patient is capable of responding to provider questions in detail and with accuracy; the patient exhibits symptoms that are identifiable through visual inspection (e.g., dermatological conditions); the patient and his/her medical history are already known to the provider; and/or the patient would benefit from treatment options that are standardized and well-established. Within these or other appropriate parameters, telemedicine can offer significant benefits, including:

- Lower costs to provide medical services;
- More coordinated health care workflow, e.g., through fewer unnecessary emergency room visits;
- Improved timelines and speed in responding to patient needs;
- Better safety and quality, particularly for patients in remote areas that may have reliable broadband internet access, yet lack sufficient local health care capacity;

- Access to more specialized types of procedures that might not otherwise be available in a particular locality, including through robotic surgery or remote VR/AR enhanced procedures, where specialists in a central location guide or assist providers to conduct services that might otherwise not be available;
- Real-time monitoring of aggregated anonymized data to monitor for health trends, epidemiological patterns, or localized disease outbreaks;
- Reduced spread of disease (e.g., where possible, by treating some patients with communicable diseases remotely without exposing others, or conversely, by treating patients remotely without exposing those patients to communicable diseases prevalent in hospital settings);
- The ability to address emergency surges in demand for medical services and/or shortages of medical professionals;
- The ability to offer home-based patient treatment, recuperation, and monitoring–improving patient comfort and recovery times, and freeing up space and capacity in clinics and hospitals;
- Added insights and functionality (e.g., by leveraging diagnostics and analysis of patient data submitted to a provider). Such data may include trends in blood sugar, blood pressure, oxygen levels, temperature, heart rate, weight, height, etc. collected and shared with patient consent via sensors in wearables or other health tracking devices.

**Real-time aggregation and analytics of anonymized data from around the world is critical to global health–allowing for the rapid detection and response to emergent health trends, epidemiological patterns, and localized disease outbreaks.**

These benefits depend, in part, on ensuring that providers and patients within a country have cross-border access to the remote health technologies that enable these important services.

## CONCLUSION

Alongside a country's levels of internet access and computer literacy, cross-border connectivity is a critical factor in enabling the benefits of remote health services. Countries can promote diverse health care delivery options for their citizens by ensuring that data transfer restrictions do not unduly interfere with the ability to offer secure and private remote health care services.

## Endnotes

[1] See e.g., Center for Medicare and Medicaid Services, Medicare Telemedicine Health Care Provider Fact Sheet (March 2020), https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet; and World Health Organization, Rational Use of Personal Protective Equipment for Coronavirus Disease 2019 (COVID-19) (February 2020), https://apps.who.int/iris/bitstream/handle/10665/331215/WHO-2019-nCov-IPCPPE_use-2020.1-eng.pdf (encouraging patients to "consider using telemedicine to evaluate suspected cases of COVID-19 disease, thus minimizing the need for these individuals to go to healthcare facilities for evaluation.").

[2] Mann et al., COVID-19 Transforms Health Care through Telemedicine: Evidence from the Field (April 2020), https://academic.oup.com/jamia/advance-article-pdf/doi/10.1093/jamia/ocaa072/33120297/ocaa072.pdf (showing increases in daily telemedicine visits from March 2, 2020, to April 14, 2020, of 4,345 percent for non-urgent telemedicine visits and 135 percent for urgent telemedicine visits).

[3] See Mariana Fernandez, Telehealth to Experience Massive Growth with COVID-19 Pandemic, Says Frost & Sullivan (May 2020), https://ww2.frost.com/news/press-releases/telehealth-to-experience-massive-growth-with-covid-19-pandemic-says-frost-sullivan/.

[4] See US Department of Health and Human Services, HIPAA FAQ–What Is Telehealth? (2020), https://www.hhs.gov/hipaa/for-professionals/faq/3015/what-is-telehealth/index.html.

[5] See US Department of Health and Human Services, What Is Telehealth? How Is Telehealth Different from Telemedicine?, HeathIT.gov website (2020), https://www.healthit.gov/faq/what-telehealth-how-telehealth-different-telemedicine; and World Health Organization, Telemedicine–Opportunities and Developments, Report on the Second Global Survey on eHealth (2010), https://www.who.int/goe/publications/goe_telemedicine_2010.pdf.

[6] Michael Rucker, Health Tech Is Successful in Developing Countries, VeryWell Health (March 2020), https://www.verywellhealth.com/digital-health-developing-countries-1739155.

[7] World Health Organization, WHO Releases New International Classification of Diseases (ICD 11) (2018), https://www.who.int/news-room/detail/18-06-2018-who-releases-new-international-classification-of-diseases-(icd-11).

[8] American Medical Association, AMA Quick Guide to Telemedicine in Practice (April 2020), https://www.ama-assn.org/practice-management/digital/ama-quick-guide-telemedicine-practice; Centers for Medicare and Medicaid Services, General Medicine Toolkit (March 2020), https://www.cms.gov/files/document/general-telemedicine-toolkit.pdf (providing links and identifying technical ICT requirements for telemedicine and telehealth service providers); and American Medical Association, Telehealth Implementation Playbook (2020), https://www.ama-assn.org/system/files/2020-04/ama-telehealth-playbook.pdf (identifying relevant ICT equipment needed for providing telemedicine services).

[9] Relatedly, because internet traffic between providers and patients often transits among computing equipment and servers across borders, cross-border data transfers may be relevant to remote health services even in cases in which the remote health technologies are stored on servers in-country. See e.g., Casalini and Lopez González, Trade and Cross-Border Data Flows, OECD Trade Policy Papers (2019), http://dx.doi.org/10.1787/b2023a47-en (explaining that, "[t]he internet is a global network of computers, each with its own Internet Protocol (IP) address. When a file is sent from a computer in Country A to a recipient in Country B it is first broken down into different 'packets' …marked with the IP address of the sender, that of the recipient and a code identifying the sequence in which the packets are to be reassembled at destination. Once the packets are ready, they leave the origin computer, crossing different networks and taking different routes to destination.…In some instances, what might seem to be a domestic transfer involves a cross-border flow.")

[10] For example, algorithms can be trained to distinguish benign and malignant cancers based on a referential analysis of thousands of images of benign and malignant tissue samples, resulting in more accurate detection rates than a dermatological oncologist. See e.g., Computer Learns to Detect Skin Cancer More Accurately Than Doctors, Agence France Presse (May 2018), https://www.theguardian.com/society/2018/may/29/skin-cancer-computer-learns-to-detect-skin-cancer-more-accurately-than-a-doctor; Charles Towers-Clark, The Cutting-Edge of AI Cancer Detection, Forbes (April 2019), https://www.forbes.com/sites/charlestowersclark/2019/04/30/the-cutting-edge-of-ai-cancer-detection/#43acb1b67336; Taylor Kubota, Deep Learning Algorithm Does as Well as Dermatologists in Identifying Skin Cancer, Stanford News (January 2017), https://news.stanford.edu/2017/01/25/artificial-intelligence-used-identify-skin-cancer/.

[11] World Health Organization, Long-Running Telemedicine Networks Delivering Humanitarian Services, Bulletin of the World Health Organization (2012), https://www.who.int/bulletin/volumes/90/5/11-099143.pdf.

# EXHIBIT 42

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# CROSS-BORDER DATA TRANSFERS & BIOPHARMACEUTICAL RESEARCH AND DEVELOPMENT

Biopharmaceuticals are increasingly developed, tested, and analyzed for safety and efficacy in different countries. To perform this research and development (R&D), scientists, regulators, and others depend on the capability to transfer data securely across international IT networks.

## CROSS-BORDER DATA TRANSFERS ACCELERATE PHARMACEUTICAL CANDIDATE IDENTIFICATION

Cross-border data transfers can accelerate early-stage biopharmaceutical R&D, as researchers search for the best drug candidates.

### Artificial Intelligence (AI) and Target-Based Drug Discovery

As health-related data grows rapidly (increasing nearly 900 percent from 2016–2018),[1] cross-border data analytics can help speed the early identification of potentially useful drug candidates, shortening pharmaceutical discovery timelines from years to months.[2] This analysis depends upon data transferred from across the world containing information on "chemical properties [and] genetic information…to improve target-based discovery."[3]

Data analytics applied to data sets consolidated across borders is fast-tracking target discovery. As compared with traditional methods, this includes savings of up to:

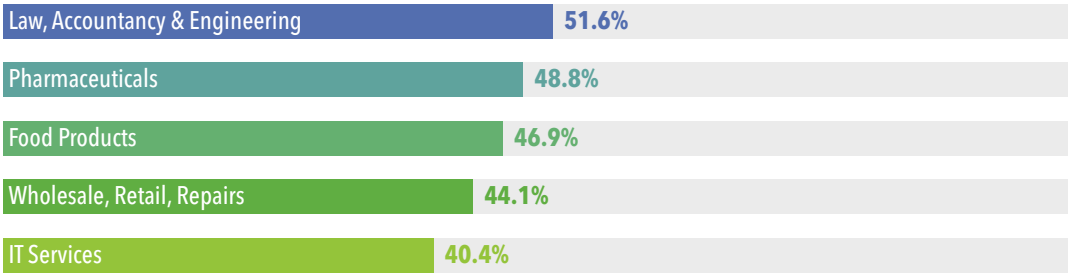
- 40–50 percent of the time required, and
- $26 billion in costs.

Pharmiweb, *How Can Artificial Intelligence Facilitate New Drug Research and Development* (2020), https://www.pharmiweb.com/article/how-can-artificial-intelligence-facilitate-new-drug-research-and-development.

## Cross-Border R&D Collaboration

Even before the launch of preclinical studies and clinical trials, the global R&D ecosystem depends on cross-border access to medical journals and scientific collaboration, reflected in a high proportion of relevant publications having international co-authors.[4] Cross-border R&D collaboration has also increased in response to the COVID-19 crisis, with the World Health Organization (WHO),[5] public-private research consortia,[6] and national governments establishing new platforms and methods of sharing research[7] and resources[8] across borders. The US-Canada Cascadia Data Discovery Initiative (CCD) is another model for cross-border R&D collaboration.[9]

### Top Five Sectors of Scientific Publications With International Co-authorship




**Source:** H. Dernis, P. Gkotsis, N. Grassano, S. Nakazato, M. Squicciarini, B. van Beuzekom, A. Vezzani, *World Corporate Top R&D Investors: Shaping the Future of Technologies and of AI*, A joint JRC and OECD Report (2019), http://www.oecd.org/sti/world-corporate-top-rd-investors-shaping-future-of-technology-and-of-ai.pdf.

### Stages of Biopharmaceutical R&D

| Stage | Purpose | Data Involved |
|---|---|---|
| General Research | Drug discovery, lab drug screening, drug target identification | Databases containing medical journals and studies; historical clinical trial data/results (if publicly available); libraries of chemical compounds and molecules, and their biological and pharmacological characteristics.* |
| Preclinical Studies | Determine safety of broader clinical trials | Same as above; *in vitro* or *in vivo* studies, and toxicity data. May also assess dosing and route of administration for the clinical trial context. |
| Clinical Trials | Determine whether a product is safe and effective for use in humans | • Phase 1 data often relates to pharmacokinetic parameters–e.g., absorption, distribution, metabolization rates, and excretion in healthy participants.<br>• Phase 2 data often relates to efficacy in those affected by the underlying condition, producing a dose response relationship.<br>• Phase 3 data often relates to large numbers of participants across demographics and populations. |
| Regulatory Review | Review evidence, issue marketing approval, and any changes/updates post-approval | Entire dossier of evidence developed through earlier stages of biopharmaceutical R&D. Multiple regulators review the same and/or related data sets, thus requiring cross-border exchange and collaboration. Real-world evidence datasets from different markets can also sometimes complement the traditional data package. |
| Post-Marketing Surveillance | Ensure product is safe and effective after marketing | Data collection through reporting of adverse events, and facility inspections to ensure that good manufacturing practices are being followed, etc. |

* See e.g., APEx Bio, *Screening Library* (2021), https://www.apexbt.com/screening-library.html.

## CROSS-BORDER DATA TRANSFERS FACILITATE THE EVALUATION OF SAFETY AND EFFICACY ACROSS GLOBAL POPULATIONS DURING PRECLINICAL STUDIES AND CLINICAL TRIALS

Cross-border data transfers help improve preclinical studies and clinical trials by reducing development cycles, improving data quality, facilitating participant adherence, and leading to more conclusive safety and efficacy findings. Trial processes may necessitate data transfers among participants located in different countries–sponsor(s), clinical trial sites, contract research organizations (CROs), recruitment vendors, central laboratories and imaging service providers, among others. This includes:

### Good Clinical Design and Practice in a Cross-Border R&D Context

Clinical trial design is often inherently cross-border in scope. Trial architects often consider relevant cross-border circumstances as they develop the protocols that set out a trial's objectives, design, and methodology. Likewise, regulators are designing more efficient approaches to cross-border trial design, as exemplified by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) E6 (Good Clinical Practice) and ICH E8 (General Considerations for Clinical Studies).

- **Cross-border outcome modeling.** Multi-country planning can improve trial design and outcome modeling, thus leading to better design protocols, predictive analysis, and risk management.
- **Cross-population representativeness.** Cross-border data transfers enable global insights and the early identification of patterns in trial data. "Global studies ensure that new products are safe and effective across different demographics, and [especially for rare and neglected diseases, can help identify]…a representative sample of trial subjects."[10]
- **International legal compliance.** A cross-border design helps ensure compliance with different countries' drug regulatory approval requirements, sectoral data privacy rules (e.g., General Data Protection Regulations (GDPR), Health Insurance Portability and Accountability Act), and perspectives of Independent Ethics Committee (IEC), and Institutional Review Boards (IRB). Yet, cross-border collaboration, including for public sector research, remains challenging.[11]

### Enabling Both Remote and Onsite Clinical Trials

Cross-border data transfers are important to the conduct of remote and onsite clinical trials in the following ways:

- **Cross-border clinical trial operations.** An accelerated trend toward cross-border digitization of clinical trial processes is regarded by some commentators as "the biggest innovation emerging from the COVID-19 crisis."[12] Cross-border cloud- and patient-centric clinical trial technologies can also help improve patient access, diversity, speed, and representativeness, especially as more than 80 percent of clinical trials don't meet initial enrollment timelines.[13]
- **New uses for wearables.** Cloud-based digital tools can evaluate data from wearables and Internet of Things devices in real-time, allowing for early identification of anomalies and promising results alike.[14] Supported by robust privacy protections, remote monitoring enabled by these technologies can also help improve clinical trial processes through higher recruitment rates, better compliance, and lower drop-out rates.

## CROSS-BORDER DATA TRANSFERS HELP REGULATORS ENSURE PRODUCT SAFETY AND EFFICACY

Cross-border data transfers are also critical to regulatory review in different countries–both for applicants and regulators who may seek to workshare, collaborate, or refer to one another's reviews. This includes:

- **Cross-border regulatory collaboration.** The US Food & Drug Administration (FDA) Oncology Center of Excellence launched Project Orbis, a cross-border collaborative framework to share information in regulatory reviews of oncology products across Australia, Brazil, Canada, Singapore, Switzerland, the UK, and the United States.[15]
- **Cross-border data sharing platforms.** Cross-border data exchange initiatives like the Accumulus platform can help facilitate coordinated global assessments of therapies in multiple countries.
- **Global regulatory structured data submissions.** Global regulators are beginning to introduce structured data submission frameworks to improve regulatory data management and regulatory review processes.[16] Applicants are also investing in Regulatory Information Management Systems (RIMS) that offer cloud-enabled approaches to managing and streamlining the submission of regulatory approval dossiers.[17]

### Project Orbis: Cross-Border Regulatory Collaboration in Oncology Product Reviews in Seven Countries

Project Orbis is an initiative of the FDA Oncology Center of Excellence, which provides a framework for concurrent submission and review of oncology products among international partners.

**PROCESS**

Applicants submit cross-border drug approval applications in seven countries for concurrent regulatory review.

Regulators meet quarterly to improve clinical trial design, data quality, and patient outcomes.

**JUNE 2019 TO JUNE 2020**

**60** oncology marketing applications filed, representing **16** unique projects.

Median time-to-approval: **4.2 months** in United States; **4.4 months** in other jurisdictions.

First approval: **November 2019** simultaneous United States, Canada, and Australia approval decisions for a new treatment of advanced endometrial carcinoma.

## CROSS-BORDER DATA TRANSFERS FACILITATE POST-MARKETING SURVEILLANCE AND GOOD PHARMACOVIGILANCE PRACTICE

Cross-border data transfers are integral to good pharmacovigilance practice (GVP) in the post-market surveillance context. This often includes cross-border reporting of data on adverse reactions with global regulators, regulatory inspections of global manufacturing facilities, and submission of risk management plans and post-authorization safety studies to regulatory authorities in different countries. This includes:

- **Cross-border adverse event reporting.** Information on adverse reactions to pharmaceutical products are collected and shared with regulators around the world, although personally identifiable information is only transferred in extraordinary circumstances and subject to extensive security controls. Such information must be able to move from wherever an event occurs to government regulators.
- **Cross-border facility inspections.** The ability of regulators from different countries to travel to global manufacturing facilities was curtailed during the COVID-19 crisis, leading to an increase in virtual remote facility inspections for certain limited purposes, such as documentation review.[18] Going forward, such cross-border virtual inspections could complement existing processes designed to ensure product safety and efficacy, including processes relating to pharmacovigilance and good manufacturing practice.

### Privacy and Security Data Controls for Cross-Border Biopharmaceutical R&D

| Stage | Data Type | Is data protected by encryption? | Do cloud security protections apply?[a] | Is data pseudonymized or anonymized?[b] | Can privacy enhancing technologies be applied?[c] |
|---|---|---|---|---|---|
| Candidate Identification | Medical journals, compound libraries, etc. (containing no personal data) | Often | Yes | N/A | N/A |
| Preclinical Studies | Toxicity studies in vitro or in vivo (rarely human studies) | Yes | Yes | Rarely applicable | Rarely applicable |
| Clinical Trials | Bodily response data | Yes | Yes | Yes | Often |
| Regulatory Review | Marketing approval application and dossier | Yes | Yes | Yes | Often |
| Post-Market Surveillance | Monitoring and adverse event reports | Yes | Yes | Yes | Often |

[a] Cloud-based technologies can help improve data security, allowing investigators and participants to access clinical trial software applications protected by cloud-based cybersecurity, encryption, and other privacy-protective software solutions. See generally, BSA, *Moving to the Cloud–A Primer on Cloud Computing* (2018), https://www.bsa.org/files/reports/2018BSA_MovingtotheCloud.pdf.

[b] To protect subject privacy, including in a cross-border R&D context, organizations pseudonymize (or "de-identify") trial data, biospecimens, and other information. This process often involves replacing all direct identifiers with a subject identification code that is maintained confidentially at the trial site. The coded data sets may be transferred, often across borders, to contract research organizations or laboratories for analysis. EFPIA, IPMPC, MedTechEurope, and AdvaMed, *Transatlantic Healthcare Data Flows*, p. 3. Data anonymization safeguards (i.e., permanent removal of identifiers, leaving no way to link the data back to a subject) and data minimization safeguards (i.e., removal of key identifying data from certain data summaries) are also sometimes used as an effective supplementary measure to enhance privacy in certain cross-border medical R&D contexts. See e.g., Jack Shostak, *De-Identification of Clinical Trials Data Demystified*, https://www.lexjansen.com/pharmasug/2006/PublicHealthResearch/PR02.pdf; ALLEA, EASAC, FEAM, *International Health Data Sharing*, p. 12, Box 1.

[c] To add further layers of security in a cross-border R&D context, data analytics performed on combined data sets can also make use of privacy-enhancing technologies (PETs), including differential privacy and homomorphic encryption. See ALLEA, EASAC, FEAM, *International Health Data Sharing*, pp. 36–37, 47, Appendix 3.

## Endnotes

1 HIT Infrastructure, *Organizations See 878% Health Data Growth Rate Since 2016* (2019), https://hitinfrastructure.com/news/organizations-see-878-health-data-growth-rate-since-2016.

2 Arash Keshavarzi Arshadi et al., "Artificial Intelligence for COVID-19 Drug Discovery and Vaccine Development," *Frontiers in Artificial Intelligence* (August 2020), https://www.frontiersin.org/articles/10.3389/frai.2020.00065/full.

3 Joshua New, *Accelerating Data-Driven Drug Development* (2019), https://datainnovation.org/2019/09/accelerating-data-driven-drug-development/; see also, Duska Anastasijevic, *Mayo Clinic Completes Deidentification of Expansive Medical Dataset* (2020), https://newsnetwork.mayoclinic.org/discussion/mayo-clinic-completes-deidentification-of-expansive-medical-dataset/.

4 H. Dernis et al. *World Corporate Top R&D Investors: Shaping the Future of Technologies and of AI, A Joint JRC and OECD Report* (2019), http://www.oecd.org/sti/world-corporate-top-rd-investors-shaping-future-of-technology-and-of-ai.pdf.

5 See e.g., World Health Organization, *Global Research on Coronavirus Disease* (COVID-19), https://www.who.int/emergencies/diseases/novel-coronavirus-2019/global-research-on-novel-coronavirus-2019-ncov.

6 Semantic Scholar, *COVID-19 Open Research Dataset*, https://pages.semanticscholar.org/coronavirus-research; OpenHIE, *COVID-19 Task Force* (2020), https://wiki.ohie.org/display/SUB/COVID-19+Task+Force.

7 See e.g., Pharmaceutical Research and Manufacturers of America, Biotechnology Innovation Organization, *Our Commitment to Beat Coronavirus* (2020), https://phrma.org/-/media/Project/PhRMA/PhRMA-Org/PhRMA-Org/PDF/G-I/Industry-Principles-on-Coronavirus.pdf; IMI Innovative Medicines Initiative, *IMI Mission and Objectives* (2020), www.imi.europa.eu/about-imi/mission-objectives; *Novel Coronavirus Data Platform Data Sharing Agreement (DSA) Terms of Data Submission*, https://media.tghn.org/medialibrary/2020/01/nCoV_Data_Platform_Terms_of_Data_Submission_24Jan2020.pdf.

8 The public-private COVID-19 High Performance Computing Consortium offered global cross-border access to high-performance technologies with the power to "process massive numbers of calculations related to bioinformatics, epidemiology, and molecular modeling, helping scientists develop answers to complex scientific questions about COVID-19 in hours or days versus weeks or months." See *COVID-19 High Performance Computing Consortium*, www.covid19-hpc-consortium.org/; Sara Castellanos, "Supercomputers Help Researchers Speed Drug Discovery for Covid-19," *Wall Street Journal* (April 14, 2020), www.wsj.com/articles/supercomputers-help-researchers-speed-drug-discovery-for-covid-19-11586888735?mod=hp_minor_pos4; see also European Commission, *Using European Supercomputing to Treat the Coronavirus* (2020), https://ec.europa.eu/digital-single-market/en/news/using-european-supercomputing-treat-coronavirus (EU-based consortium of industry, research organizations, and three supercomputing centers).

9 Cascadia Data Alliance, *Data Science Collaborations* (2021), https://www.fredhutch.org/en/about/about-the-hutch/institutional-partners-collaborations/cascadia-data-alliance.html.

10 EFPIA, IPMPC, MedTech Europe, and AdvaMed, *Innovation without Borders: The Importance of Transatlantic Data Flows to Healthcare Innovation and Delivery*, Discussion Paper (2020) (hereinafter EFPIA, IPMPC, MedTechEurope, and AdvaMed, *Transatlantic Healthcare Data Flows*); see also, ALLEA, EASAC, FEAM, *International Health Data Sharing* (April 2019), https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/International_Health_Data_Transfer_2021_web.pdf.

11 See Tania Rabesandratana, "European Data Law Is Impeding Studies on Diabetes and Alzheimer's, Researchers Warn," *Science* (November 20, 2019), https://www.sciencemag.org/news/2019/11/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn; see also, EFPIA, IPMPC, MedTechEurope, and AdvaMed, *Transatlantic Healthcare Data Flows*; Dara Hallian et al., *International Transfers of Health Research Data Following Schrems II: A Problem in Need of a Solution* (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3688392; David Peloquin et al., "Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data," *European Journal of Human Genetics* (2020), https://www.nature.com/articles/s41431-020-0596-x; Santa Slokenberga, "EU Data Transfer Rules and African Legal Realities: Is Data Exchange for Biobank Research Realistic?" *9 International Data Privacy Law* 30 (2019), https://academic.oup.com/idpl/article-abstract/9/1/30/5076710?redirectedFrom=fulltext; Robert Eiss, "Confusion Over Europe's Data Protection Law Is Stalling Scientific Progress," *Nature* (2020), https://www.nature.com/articles/d41586-020-02454-7; PHG Foundation, *The GDPR and Genomic Data* (2021), https://www.phgfoundation.org/report/the-gdpr-and-genomic-data.

12 Jerry Stewart et al., *COVID-19: A Catalyst to Accelerate Global Regulatory Transformation*, Journal of Clinical Pharmacology and Therapeutics, p. 2 (2020) (hereinafter "Global Regulatory Transformation").

13 See e.g., Kent Thoelke, "There's a Silent Crisis in Clinical Research. And It's Not Covid-19," *STAT* (October 28, 2020), https://www.statnews.com/2020/10/28/recruitment-retention-silent-crises-clinical-trials/.

14 EFPIA, IPMPC, MedTechEurope, and AdvaMed, *Transatlantic Healthcare Data Flows*, p. 4; Global Regulatory Transformation, p. 2; McKinsey, *Digital R&D: The Next Frontier for Biopharmaceuticals* (October 31, 2018), https://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/digital-rd-the-next-frontier-for-biopharmaceuticals.

15 See US Food & Drug Administration, *Project Orbis: Strengthening International Collaboration for Oncology Product Reviews, Faster Patient Access to Innovative Therapies* (2020), https://www.fda.gov/news-events/fda-voices/project-orbis-strengthening-international-collaboration-oncology-product-reviews-faster-patient; Clinical Cancer Research, *Project Orbis: Global Collaborative Review Program*, CCR Perspectives in Regulatory Science and Policy (2020), https://clincancerres.aacrjournals.org/content/26/24/6412; see also, Swissmedic, *The ACSS Consortium Welcomes the U.K. as Its Newest Member* (October 14, 2020), https://www.swissmedic.ch/swissmedic/en/home/news/mitteilungen/acss_consortium_neues_mitglied_mhra.html; ASEAN Joint Assessment Procedure for Pharmaceutical Products Public Announcement (July 2020), https://npra.gov.my/index.php/en/directive-general/1527125-asean-joint-assessment-procedure-for-pharmaceutical-products-public-announcement.html.

16 See e.g., European Medicines Agency, *Substance, Product, Organisation and Referential (SPOR) Master Data* (2021), https://www.ema.europa.eu/en/human-regulatory/research-development/data-medicines-iso-idmp-standards/substance-product-organisation-referential-spor-master-data; FDA, *Standardized Data for Pharmaceutical Quality/Chemistry Manufacturing and Control* (2018), https://www.federalregister.gov/documents/2018/08/22/2018-18080/standardized-data-for-pharmaceutical-qualitychemistry-manufacturing-and-control-public-meeting; FDA, *Regulatory Submissions Forum* (2020), https://www.fda.gov/media/135563/download; Health Canada, *Structured Format for Product Monographs* (2019), https://www.canada.ca/en/health-canada/services/drugs-health-products/public-involvement-consultations/drug-products/structured-product-monograph.html.

17 See generally, Gens & Associates, *2020 World Class Regulatory Information Management (RIM) Whitepaper* (2020), http://gens-associates.com/wordpress/wp-content/uploads/2020/11/GensandAssociates_Executive_WorldClassRIM_Whitepaper_Fall2020v_Release.pdf.

18 Global Regulatory Transformation, p. 2.

**About the Global Data Alliance**

The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, electronics, energy, financial and payment services, health, consumer goods, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance.

# EXHIBIT 43

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# CROSS-BORDER DATA TRANSFERS & ENVIRONMENTAL SUSTAINABILITY

This report helps to illustrate how responsible cross-border data policies help to mitigate climate change. Climate change is a defining challenge of our time. Beyond its impact on our quality of life and various ecosystems, the effects of climate change are expected to reduce global Gross Domestic Product (GDP) by 10 percent–or $23 trillion by 2050–barring urgent action to stop rising global temperatures and address the root causes of climate change.[1]

Meeting this challenge requires globally coordinated action and the kind of digital transformation that enables all stakeholders to achieve ambitious climate targets.[2] Especially for purposes of carbon tracking and predictive climate modeling, the cross-border movement of data, cross-border exchange of knowledge, and cross-border access to analytical tools are critical to global efforts to address climate change. Restricting the ability to share information across transnational IT networks, and mandating the localization of computing resources in particular regions, undermines the ability to analyze and respond climate challenges, as discussed below.

## CROSS-BORDER DATA TRANSFERS AND CARBON TRACKING

Addressing climate change requires assessing the carbon profiles associated with organizations, processes, and product and service offerings. To perform this assessment, it is necessary to gather data across transnational digital networks–transportation logs, meter readings, fuel purchase records, direct monitoring, or other methods for acquiring data from specific activities across the international value chain.[3]

**Restricting the ability to share information across transnational IT networks undermines cross-border efforts to analyze and respond to climate challenges.**

Under the Greenhouse Gas Protocol,[4] many enterprises now assess carbon-relevant data points across three phases of international supply and value chains.[5] This analysis requires cross-border access to diverse data sets and to cloud computing resources. For example, through Artificial Intelligence-of-Things (AIoT) integration, enterprises can more effectively integrate real-time activity level data and global asset inventory data, thus improving both data quality and data deployability to address real-world climate challenges.[6]

Similarly, cross-border data transfers and access to cloud resources are critical to improved understanding of the carbon profiles of power plants, transportation assets, and other major sources of global emissions. In this context, cross-border data analytics allow for the automated analysis of images of power plants and nearby infrastructure, accounting data, and other indicia of the carbon intensity of target activities.[7]

When countries impede the ability to access relevant data across transnational digital networks, they also complicate efforts to identify solutions to reduce carbon-intensive processes that contribute to climate change.

## CROSS-BORDER DATA TRANSFERS AND PREDICTIVE CLIMATE MODELING

Cross-border data transfers are also critical to predictive climate modeling, which focuses on a wide array of climate risks, including hurricanes, typhoons, wildfires, floods, droughts, and their collateral impacts–such as property damage and supply chain disruptions.[8] Predictive climate modeling improves disaster planning and recovery, and also improves predictions of actuarial risk, an area of particular urgency given the estimated $171 billion gap in climate insurance globally.[9]

**Cross-border predictive climate modeling requires the real-time application of data analytics to diverse climate-relevant data sets.**

Cross-border predictive climate modeling requires the real-time application of data analytics to diverse climate-relevant data sets.[10] Relevant multi-regional data includes satellite data, weather station data, topographical data, and various other data from sensors in the field.[11]

The World Bank's Global Facility for Disaster Reduction and Recovery (GFDRR), which leverages cross-border data in the cloud to bolster resilience in developing countries, offers one case study in predictive climate modeling. In Bangladesh, the GFPRR helped make datasets available across international and national organizations to map vulnerable areas and improve preparation for cyclones and floods in the Bay of Bengal. Using data sources and models gathered from thousands of global sources, Bangladesh authorities produced cyclone risk maps to guide investment plans for cyclone shelters across the country. Further, authorities assessed 35,000 schools for overall resilience and survivability during a natural disaster.[12]

A second case study involves the use of cloud-based digital twins. One well-known example is "Destination Earth," which will use cross-border observational data to create a twin model of the Earth that will serve as a digital test bed for climate change mitigation and sustainability plans.[13]

Predictive climate modeling, an inherently cross-border data intensive process, is critical to anticipating and slowing and mitigating the effects of climate change.[14] Without the ability to access and transfer relevant data across borders, this promising area of data science will not reach its full potential, undermining collective efforts to combat climate change.

## CROSS-BORDER DATA TRANSFERS AND SUSTAINABLE CLOUD COMPUTING

Carbon tracking and climate modeling depend upon cross-border access to cloud-based computing resources. Cross-border access to regionally centralized cloud computing infrastructure has greatly reduced the need for individual businesses to maintain onsite data centers that would otherwise require millions of servers and computing resources

Cross-border access to data and software in the cloud has been estimated to allow enterprises to shrink their computing energy footprints by 87 percent, saving 23 billion kilowatt-hours annually–enough to power the city of Los Angeles.[15] In some cases, cloud services accessed across borders can be up to 93 percent more energy efficient than local on-premise enterprise datacenters, and 98 percent more carbon efficient.[16]

**Cross-border access to data and software in the cloud has been estimated to allow enterprises to shrink their computing energy footprints by 87 percent, saving 23 billion kilowatt-hours annually–enough to power the city of Los Angeles.**

Nevertheless, more can be done to build upon the carbon-beneficial shift from on-premises to cloud-based computing environments.

First, policymakers should not mandate the unnecessary construction of cloud computing infrastructure. Requirements to build redundant computing infrastructure in local jurisdictions would undo much of the progress seen in the shift to the cloud, as countries would force service providers to build and run duplicative data centers in numerous jurisdictions–an inherently emissions- and carbon-intensive process.

Second, despite the broader sustainability benefits of the shift to the cloud, emissions from data centers can also be reduced. Emissions produced by all buildings–including residential housing, office buildings, factories, data centers, and other structures–collectively account for up to 20 percent all emissions.[17] To help reduce their contribution to overall building-related emissions, cloud service providers are working to develop "green" data centers with reduced carbon footprints, including by powering data centers with renewable hydro, wind, or solar energy; feeding excess heat produced back into local heating networks; installing more energy-efficient computing hardware; and deploying Building and Information Modeling ("BIM") software solutions to optimize cooling systems and improve the sustainability of construction.[18] For both data centers and other types of structures, BIM software solutions are particularly promising based on estimates that many buildings' carbon footprints can be reduced by nearly 90% through retrofit strategies.[19] Another area of promise is the development of sustainable coding and computing protocols and best practices that are less taxing on computing resources.[20]

## CONCLUSION

Powerful analytical tools for combating climate change–including carbon emissions tracking and predictive climate modeling–depend on the ability to freely access cross-border data transfers. When countries restrict the ability to share knowledge, information, and data across transnational IT networks–and restrict the ability to track emissions and model climate change scenarios–they undermine coordinated international efforts to address this urgent global challenge.

## Endnotes

1 https://www.swissre.com/institute/research/topics-and-risk-dialogues/climate-and-natural-catastrophe-risk/expertise-publication-economics-of-climate-change.html

2 https://www.bsa.org/files/policy-filings/12062022sustainabilityprinciples.pdf

3 https://www.forbes.com/sites/mikehughes1/2020/12/23/digital-transformation-the-key-to-tackling-climate-change/?sh=2a5a31f25bb7

4 Greenhouse Gas Protocol | (ghgprotocol.org); https://www.epa.gov/climateleadership/ghg-inventory-development-process-and-guidance

5 https://www.epa.gov/climateleadership/ghg-inventory-development-process-and-guidance; https://www.epa.gov/climateleadership/scope-3-inventory-guidance These three phases comprise direct emissions from the company's own operations (Scope 1 emissions); emissions required to generate the electricity that the company uses (Scope 2 emissions); and indirect emissions that go into the production and consumption of the company's products across its value chain, from upstream suppliers to downstream customers (Scope 3 emissions).

6 https://www.weforum.org/agenda/2021/07/fight-climate-change-with-technology/; https://www.zdnet.com/article/10-technologies-most-likely-to-help-save-planet-earth/ ("Networked sensors as small as a dime are already monitoring air and water quality, identifying pollutants, tracking acidification, and capturing real-time data on phenomena that are crucial to our social and economic wellbeing. Wearable air quality sensors are on their way, and localized sensor networks monitoring energy and water usage in buildings are cutting down on waste.")

7 For example, Carbon Tracker relies on cross-border data analytics to analyze emissions for 4,000 to 5,000 power plants around the world, supporting meaningful carbon accountability and effective climate change mitigation strategies. https://www.nationalgeographic.com/environment/article/artificial-intelligence-climate-change; https://news.microsoft.com/apac/features/ai-for-earth-helping-save-the-planet-with-data-science/ (AI-powered predictive modeling has enabled impressive "strides …in land cover mapping–traditionally a time-consuming, expensive tool that is essential for environmental management and precision conservation. Recently, the entire United States was mapped by machine-learning algorithms that processed nearly 200 million aerial images in just over 10 minutes. Done the usual way, such a project would have taken many months and cost a fortune. Deployed globally and locally, this new way of mapping could revolutionize how we mitigate the effects of urbanization, pollution, deforestation, and even natural disasters.")

8 https://www.weforum.org/agenda/2018/01/8-ways-ai-can-help-save-the-planet/ ("A new field of "Climate Informatics" is blossoming that uses AI to fundamentally transform weather forecasting and improve our understanding of the effects of climate change. … AI techniques may also help … predict extreme events and be used for impacts modelling."); https://hai.stanford.edu/news/environmental-intelligence-applications-ai-climate-change-sustainability-and-environmental ("Predicting, detecting, and mitigating or incentivizing environmental transitions: Understanding past changes in environmental behavior and their consequences (e.g., land and water use, agricultural practices, pest management) can lead to both the early detection of big transitions and the seemingly small transitions with potentially big ripple effects. Early detection of changes could lead to prepared responses, mitigation of bad outcomes, or the ability to incentivize promising responses.")

9 https://www.forbes.com/sites/robtoews/2021/06/20/these-are-the-startups-applying-ai-to-tackle-climate-change/; https://www.weforum.org/agenda/2021/08/how-is-machine-learning-helping-us-to-create-more-sophisticated-climate-change-models/ ("With machine learning, we can use our abundance of historical climate data and observations to improve predictions of Earth's future climate. And these predictions will have a major role in lessening our climate impact in the years ahead.")

10 https://www.techrepublic.com/article/how-ai-could-save-the-environment/ ("74% of the 200 environmental sustainability professionals agreed that AI, which involves cross-border data analytics, will help solve long-standing environmental challenges.")

11 https://www.zdnet.com/article/10-technologies-most-likely-to-help-save-planet-earth/ ("Sensing technology and more accurate prediction models will fine-tune energy production to avoid overproduction, and better battery technology will enable storage of renewably sourced energy.")

12 https://www.worldbank.org/en/news/feature/2021/04/19/deploying-digital-tools-to-withstand-climate-change-in-low-income-countries

13 https://www.asme.org/topics-resources/content/digital-twins-for-the-future-of-climate-change. Another example of cross-border data-driven digital twins for climate modeling is provided by the recently announced Earth-2 (E-2) system, which would create a digital twin of the Earth in an open platform built for virtual collaboration and real-time physically accurate simulation. This system would analyze data sourced from all over the world in a virtual environment that combines GPU-accelerated computing, deep learning and physics-informed neural networks.

14 https://www.nationalgeographic.com/environment/article/artificial-intelligence-climate-change ("Climate informatics covers a range of topics: from improving prediction of extreme events such as hurricanes, paleoclimatology, like reconstructing past climate conditions using data collected from things like ice cores, climate downscaling, or using large-scale models to predict weather on a hyper-local level, and the socio-economic impacts of weather and climate.")

15 https://software.org/wp-content/uploads/Every_Sector_Software_SmartEnergy.pdf

16 *See id.*

17 https://www.forbes.com/sites/robtoews/2021/06/20/these-are-the-startups-applying-ai-to-tackle-climate-change/. See also https://world101.cfr.org/global-era-issues/climate-change/how-can-artificial-intelligence-combat-climate-change ("[E]missions from the large data farms and processing centers underpinning the information and communications technology sector are comparable to those of the aviation industry.")

18 https://www.technologyreview.com/2018/08/17/140987/google-just-gave-control-over-data-center-cooling-to-an-ai/; https://www.technologyreview.com/2019/06/20/134864/ai-climate-change-machine-learning/ ("Intelligent control systems can dramatically reduce a building's energy consumption by taking weather forecasts, building occupancy, and other environmental conditions into account to adjust the heating, cooling, ventilation, and lighting needs in an indoor space. A smart building could also communicate directly with the grid to reduce how much power it is using if there's a scarcity of low-carbon electricity supply at any given time."); https://www.forbes.com/sites/robtoews/2021/06/20/these-are-the-startups-applying-ai-to-tackle-climate-change/ (In one case study, a data center operator used data analytics and machine learning techniques to optimize the data centers' cooling systems, reducing overall energy consumption by up to 40%–by other other things–taking advantage of winter conditions to produce colder than normal water and thus reducing the energy required for cooling.)

19 *See id.; See also,* https://www.nature.com/articles/s41558-020-0837-6.

20 https://www.sciencedaily.com/releases/2021/03/210302185414.htm; https://www.forbes.com/sites/robtoews/2020/06/17/deep-learnings-climate-change-problem/?sh=16fad9456b43

Artificial Intelligence–and the training and implementation of data analytics and machine learning models–can be a particularly carbon-intensive process, leading to calls for "researchers to plot energy costs against performance gains when training models. Explicitly quantifying this tradeoff will prompt researchers to make more informed, balanced decisions about resource allocation in light of diminishing returns"; to use "more efficient hyperparameter search methods, reducing the number of unnecessary experiments during training, employing more energy-efficient hardware"; and developing new computer science disciplines focused on the discovery of more efficient "efficient ways to model intelligence in machines."

# EXHIBIT 44

GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

# SUPPLY CHAIN RESILIENCE ISSUE BRIEF

## CROSS-BORDER DATA TRANSFERS & ARTIFICIAL INTELLIGENCE

Cross-border data transfers are integral to the effective deployment of data analytics solutions to enhance economic growth, help advance scientific progress, promote cutting-edge research and development (R&D), and solve pressing health-, climate-, and other challenges. Science- and innovation-oriented organizations at the international and national levels make clear that these activities depend on the application of data analytical techniques to data sourced globally.

Cross-border data transfers are integral to the effective deployment of data analytics solutions to enhance economic growth, help advance scientific progress, promote cutting-edge research and development (R&D), and solve pressing health-, climate-, and other challenges. Science- and innovation-oriented organizations at the international and national levels make clear that these activities depend on the application of data analytical techniques to data sourced globally.

From developing predictive models to deploying and using analytical solutions, data analytics systems are "trained" by ingesting large data sets to identify underlying patterns, relationships, and trends that are then transformed into mathematical models that can make predictions based on new data inputs. These data sets often originate from geographically dispersed sources across transnational digital networks, making it imperative that data can move seamlessly and securely across borders. To secure the insights and other benefits that data analytics can provide, it is important to permit access and consolidation of data sets across borders.

Smart and responsible deployment of data analytics solutions, supported by data inputs from across the globe, can help advance improvements in healthcare, modernize education, expand accessibility tools, strengthen cybersecurity, and increase business productivity and competitiveness. For example, analytical techniques applied to health data transferred across transnational digital networks helped fast-track COVID-19 vaccine development, cutting timelines from years to months, as researchers analyzed data from around the world to quickly identify potential treatments.

# EXHIBIT 45

**Response to**
**United States Agency for International Development**
**Request for Information on an**

**AI in Global Development Playbook**

March 1, 2024

The Global Data Alliance[1] (GDA) welcomes the opportunity to share its views on the United States Agency for International Development (USAID) Request for Information on an AI in Global Development Playbook (RFI).

## I. Introduction

The RFI covers a broad range of topics, including principles, tools, and best practices for advancing AI in a risk-aware manner. Our comments focus on how the facilitation of cross-border access to knowledge, information, ideas, and digital tools can support AI for global development.

The GDA is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. GDA members share a deep and abiding commitment to supporting economic development across regions, technologies, and business models. The GDA engages on the cross-border data policy matters with diverse economies, including Bangladesh, Cambodia, India, Indonesia, Kenya, Malaysia, Nigeria, Pakistan, the Philippines, South Africa, Vietnam, and other countries across Africa, Asia, Latin America, and the Caribbean.[2]

We strongly endorse the RFI's support for the more effective development and deployment of AI to facilitate economic development goals. Cross-border data transfers are critical to the development and deployment of human-centric and development-centric AI for the benefit of communities across the globe. The AI in global development playbook should recognize the importance of AI to businesses across sectors and the role of cross-border data transfers in supporting the responsible development and use of AI systems worldwide.

In the discussion that follows, we address the role of cross-border data to AI in global development specifically and to economic development goals more broadly.

## II. Cross-Border Data and AI in Global Development

AI is critical to advancing economic developing and digital inclusion goals, including under the UN's Sustainable Development Goals 2030. Cross-border access to knowledge, information, and digital tools is necessary to realize the benefits of AI, even in everyday uses.

AI involves the application of analytical techniques to a variety of data (structured and unstructured) available or generated in various locales, that can be accessed or transferred across borders, and then consolidated into larger data sets. From developing predictive models to deploying and using analytical solutions, AI systems are trained and fine tuned by consolidating large and diverse data sets from around the world to identify underlying patterns, relationships, and trends that are then transformed into

mathematical models that can make predictions based on new data inputs. These data sets often originate from geographically dispersed sources, such as data from IoT sensors, across global digital networks, making it imperative that data can move and be accessed seamlessly and securely across borders.

Responsible development of AI systems, supported by data inputs from across the globe, can help mitigate the impacts of climate change, fuel advancements in healthcare, transform education, optimize agriculture, improve access to finance, reinforce the operation of global telecommunications networks, enhance customer engagement, and create new economic opportunities.[3] Examples of AI for global development include:

- Predictive climate modeling to prepare for severe weather events in developing economies based on computational analysis of satellite data, weather station data, topographical information, and various IoT and sensor data.[4] Similarly, improved carbon tracking and mitigation to reduce climate change impacts in developing economies based on computational analysis of transportation logs, meter readings, fuel purchase records, atmospheric pollution tracking, and visual monitoring of power plants and other facilities, and other data sources.[5]
- Computational analysis to map vulnerable seaside areas in low-lying archipelagos and delta regions (e.g., in Bangladesh) to produce cyclone risk maps and guide investment plans for cyclone shelters, schools, health facilities, and other infrastructure for disaster planning and survivability.[6]
- Cross-border data analytics can help speed the early identification of potentially useful drug candidates, including for tropical and rare diseases, shortening pharmaceutical discovery timelines from years to months. This analysis depends upon data transferred from across the world containing information on "chemical properties [and] genetic information…to improve target-based discovery."[7] For example, AI helped fast-track the COVID-19 vaccine, cutting timelines from years to months, as researchers analyzed data transferred from around the world to quickly identify potential vaccine treatments.[8]
- In healthcare delivery, AI tools can help improve health outcomes for remote and medically underserved populations across developing countries, in contexts where: (1) supporting online healthcare education tools used by international health and development agencies; (2) cross-border consultations between remote providers in one country with specialists located at research facilities abroad; (3) cross-border consolidation of anonymized data sets from around the world to enhance real-time analysis and response to emerging epidemics or localized disease outbreaks; and (4) cross-border humanitarian assistance is also possible through "telemedicine networks [that]…deliver humanitarian services on a routine basis, many to low-income countries."
- AI-driven models to combat financial fraud, money laundering, corrupt payments, and terrorist financing: AI is an essential tool in the fight against a range of financial challenges that are particularly relevant to US relations with developing country partners. For example, core operations of financial institutions include payments and remittance services that require the use of AI-based fraud prevention tools as part of transactions processing. To build effective anti-fraud and other financial tools, transactions need to be analyzed instantaneously via AI tools in centralized locations to identify potentially problematic activity. Requiring the localization of such data and infrastructure results in less effective AI models and make it more for developing economies to combat fraud, money laundering, or other improper financial practices.

As developing countries consider approaches to AI policies, they should avoid isolation, fragmentation and undue restrictions on cross-border access to knowledge, information and digital tools (e.g., via data localization mandates or onerous transfer restrictions) that will impede the ability to maximize the potential of AI for global development.

## III. Cross-Border Data and Economic Development

Cross-border access to knowledge, information, ideas, and digital tools are not only critical to AI in global development, but also economic development and digital inclusion more specifically. As the World Bank has noted, "[r]estrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services." Restrictions on cross-border access to knowledge, information, and digital tools harm GDP (minus 0.7-1.7%); investment flows (minus 4%); productivity (4.5% loss); and small business (up to 80% higher trade costs).

These burdens are borne most heavily by developing and least developing economies. As the United Nations has stated,

> Regulatory fragmentation in the digital landscape…is most likely to adversely impact low-income countries, less well-off individuals, and marginalized communities the world over, as well as worsen structural discrimination against women. A future of exclusionary digital development must be avoided at all costs.

As stated by UNCTAD:

> Divergent data nationalism...reduces market opportunities for domestic MSMEs to reach worldwide markets, [and]...reduces opportunities for digital innovation, including various missed opportunities for inclusive development that can be facilitated by engaging in data-sharing through strong international cooperation....[M]ost small, developing economies will lose opportunities for raising their digital competitiveness.

Despite their heavy costs to developing economies, cross-border data restrictiveness continues to increase, including among the largest economies. It is estimated that these restrictions increased by 600% between 2013 and 2019 in the Asia-Pacific, and increased at a rate five times higher in 2022 than in 2021.

The world now faces the threat of significant lost opportunities for economic development and digital inclusion among small developing economies as a result of exclusionary data policies adopted by large developed economies (like the EU, China, or the United States) or large developing economies (such as India or South Africa). According to the World Bank and World Trade Organization, developing countries have benefited from the most rapid growth in services exports (primarily digital services) among all economy income groups.

- Between 2001 and 2021, commercial service exports increased by 300% for least developed economies and by 250% for other developing countries.[9]
- As of 2021, Micro-, Small-, and Medium-Sized Enterprises (MSMEs) accounted for 67 percent of all cross-border services exports.[10]

- Between 2001 and 2021, there has been a 58% increase in female employment in services in low-income economies, outpacing the rate of increase in all other country income groupings. 6 in 10 employed women work in the services sector, including digital services.[11]
- According to the World Bank, "[s]tudies show that countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies."
- The Organisation for Economic Co-operation and Development has found that a 0.1 point reduction in a country's level of digital services trade restrictiveness is associated with a 145% increase in overall exports.
- As USAID has stated, digital ecosystems have the potential to equip informal merchants, women entrepreneurs, small farmers, and small businesses engaged in cross-border trade with access to markets and information facilitated by cross-border data flows.[12]
- There is a 15% estimated increase in developing country share of global services if developing countries fully adopt digital tools, including through cross-border access to cloud and software-enabled technologies – many powered by AI.[13]
- AI-focused jobs have high growth potential in developing countries – with recently projected growth rates of 400% in Malaysia and 130% in the Philippines (among other markets).[14]
- Digital tools help MSMEs in Asia reduce export costs by 82% and transaction times by 29%.[15]

Cross-border access to knowledge, information, and digital tools is critical to many developing country economic and other policy objectives: Not only do restrictive cross-border polices fail to protect privacy and personal data,[16] but they also hurt developing countries[17] and small businesses;[18] impede financial equity and inclusion;[19] undermine data security and cybersecurity;[20] threaten human rights;[21] slow science and innovation;[22] and impair various health and safety,[23] environmental,[24] and other regulatory compliance priorities.[25] Data transfers are critical to the health of developing economies across all sectors[26] and at every stage of the value chain.[27]

For more information, please see the Annex to this submission, as well as the GDA's Report on Cross-Border Data Transfers & Economic Development, GDA Cross-Border Data Policy Index,[28] the GDA Sector Studies,[29] and the GDA Issue Briefs.[30]

## IV. Conclusion

Thank you for the opportunity to provide comments. We look forward to serving as a resource as you continue to create an AI in global development playbook.

---

[1] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA member companies are headquartered across the globe and are active in over 15 industry sectors. For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org

[2] For access to prior GDA submissions to developing economies on cross-border data policy matters, please see this webpage: Global Data Alliance, Filings – Search Function (2024), at: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&posts_filtered=1

[3] *See* BSA | The Software Alliance, Everyday AI for Businesses, available at https://www.bsa.org/files/policy-filings/08012023aibusiness.pdf.

[4] Schneider et al., *Harnessing AI and computing to advance climate modelling and prediction*, 13 Nature Climate Change 887 (2023), at: https://www.nature.com/articles/s41558-023-01769-3; World Economic Forum, *The role of machine learning in helping to save the planet* (2021), at: https://www.weforum.org/agenda/2021/08/how-is-machine-learning-helping-us-to-create-more-sophisticated-climate-change-models/; Kaak et al., *Aligning artificial intelligence with climate change mitigation*, 12 Nature Climate Change 518 (2022), at https://www.nature.com/articles/s41558-022-01377-7; Xin et al., *Artificial Intelligence for Climate Change Risk Prediction, Adaptation, & Mitigation*, Ecological Processes (2021), at:

https://www.springeropen.com/collections/AICC; Chantry et al., *Opportunities and challenges for machine learning in weather and climate modelling*, 379 Phil. Trans. R. Soc. 83 (2020), at: https://doi.org/10.1098/rsta.2020.0083 (2020).
[5] *See e.g.,* Global Data Alliance, *Cross-Border Data Transfers & Environmental Sustainability* (2023) (internal citations omitted), at: https://globaldataalliance.org/wp-content/uploads/2023/04/04192023gdacbdtsustainability.pdf
[6] *See id.*
[7] *See generally,* Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical R&D* (2022), at: https://globaldataalliance.org/wp-content/uploads/2021/09/09092021cbdtbiopharma.pdf
[8] Ganes Kesari, *Why Covid Will Make AI Go Mainstream In 2021*, Forbes (Dec. 2020), https://www.forbes.com/sites/ganeskesari/2020/12/21/why-covid-will-make-ai-go-mainstream-in2021-top-3-trends-for-enterprises/?sh=48c8f9cd797a; Arshadi et al., *Artificial Intelligence for COVID19 Drug Discovery and Vaccine Development*, Front. Artif. Intell. (Aug. 2020), https://www.frontiersin.org/articles/10.3389/frai.2020.00065/full
[9] The World Bank and the WTO, *Trade_in Services_and_Development* (2023)
[10] *Id.*
[11] *Id.*
[12] USAID Digital Strategy, 2020-2024, 37, *available at* https://www.usaid.gov/sites/default/files/2022-05/USAID_Digital_Strategy.pdf.pdf.
[13] *Id.* at 4.
[14] Brenda Quismorio, *Capability building for data analytics and artificial intelligence*, UNCTAD Intergovernmental Group of Experts (IGE) on E-Commerce and the Digital Economy (2019), at: https://unctad.org/system/files/non-official-document/tdb_ede3_2019_p11_BQuismorio_en.pdf
[15] Alphabeta, *Micro-Revolution: The New Stakeholders of Trade in APAC* (2019).
[16] Global Data Alliance, *Cross-Border Data Transfers & Privacy* (2023), at: https://globaldataalliance.org/issues/privacy/
[17] Global Data Alliance, *Cross-Border Data Transfers & Economic Development* (2023), at: https://globaldataalliance.org/issues/economic-development/
[18] Global Data Alliance, *Cross-Border Data Transfers & Small Businesses* (2023), at: https://globaldataalliance.org/issues/small-businesses/
[19] Global Data Alliance, *Cross-Border Data Transfers & Finance* (2020), at: https://globaldataalliance.org/sectors/finance/
[20] Global Data Alliance, *Cross-Border Data Transfers & Cybersecurity* (2023), at: https://globaldataalliance.org/issues/cybersecurity/
[21] Freedom House, *Countering an Authoritarian Overhaul of the Internet* (2022), at: https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet Freedom House explains the nexus between data transfer restrictions and human rights abuse as follows (emphasis added): "In at least 23 countries covered by Freedom the Net, laws that limit where and how personal data can flow were proposed or passed during the coverage period. … The transfer of data across jurisdictions is central to the functioning of the global internet and benefits ordinary users, including by improving internet speeds, enabling companies to provide critical services worldwide, and allowing the storage of records in the most secure data centers available. … [S]ome [countries] have buried problematic obligations that either mandate domestic data storage, feature blanket exceptions for national security or state actors without safeguards, or delegate increased decision-making power to politicized regulators—all of which renders users vulnerable to government abuse despite improvements pertaining to the use of personal data for commercial purposes. Such contradictory "data washing" measures ultimately fail to strengthen privacy and further fragment the internet…."
[22] Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2023), at: https://globaldataalliance.org/issues/innovation/
[23] Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical R&D* (2022), at https://globaldataalliance.org/sectors/biopharmaceutical-rd/; Global Data Alliance, *Cross-Border Data Transfers & Medical Technology* (2023), at: https://globaldataalliance.org/sectors/medical-technology/; Global Data Alliance, *Cross-Border Data Transfers & Healthcare* (2022), at: https://globaldataalliance.org/sectors/healthcare/
[24] Global Data Alliance, *Cross-Border Data Transfers & Environmental Sustainability* (2023), at: https://globaldataalliance.org/issues/environmental-sustainability/
[25] Global Data Alliance, *Cross-Border Data Transfers & Regulatory Compliance* (2023), at: https://globaldataalliance.org/issues/regulatory-compliance/
[26] Global Data Alliance, *Cross Border Data - Creating Jobs in Every Sector* (2020), at: https://globaldataalliance.org/wp-content/uploads/2021/07/GDAeverysector.pdf
[27] Global Data Alliance, *Jobs in All Sectors Depend upon Data Flows* (2020), at: https://globaldataalliance.org/wp-content/uploads/2021/07/infographicgda.pdf
[28] Global Data Alliance, *Cross-Border Data Policy Index* (2023), at: https://globaldataalliance.org/resource/cross-border-data-policy-index/
[29] Global Data Alliance, *GDA Sector Studies* (2023), at: https://globaldataalliance.org/sectors/
[30] Global Data Alliance, GDA Issue Briefs (2023), at: https://globaldataalliance.org/issues/

# Annex

## The Benefits to Economic Development of Cross-Border Access to Knowledge, Information, and Digital Tools

Cross-border data transfers are critical to economic development. Cross-border access to data, which may embody knowledge, technological tools, and new business opportunities, are critical to enhancing living standards for the world's most vulnerable populations.

As explained below, the ability to transfer data across borders and leverage the benefits of data originating from different geographies is critical to: (1) delivering productivity benefits to MSMEs and other companies, and helping them access overseas markets and supply chains, and buyers and suppliers; (2) growing agricultural output; (3) delivering diagnostic services, developing new medical treatments, and otherwise protecting population health; and (4) ensuring digital trust and security. We address each of these points below.

**The ability of MSMEs in developing countries to access global markets and to offer and sell their services and products abroad** depends upon cross-border access to the data and cloud-enabled technologies. Cross-border access to e-commerce platforms, purchasers, suppliers, and other commercial partners allow local MSMEs to engage in international transactions and create jobs at home. Kenya, one of Africa's leading digital economies, makes this case in its 2019 Digital Economy Blueprint, noting that "[e]very citizen will benefit and find value" in a cross-border digital economy that makes their "goods, services and expertise… accessible across borders, opening up markets and catapulting Kenya to join 1st world markets where citizens benefit from direct access to global markets." Cross-border digital market access offers Kenya "a leapfrogging opportunity on economic development."[1]

**Agricultural output** in developing countries can be increased through technologies that depend upon cross-border access to data and cloud enabled technologies. Small- and large-scale farmers alike are better positioned for success in planting, harvesting, and selling their agricultural products when they benefit from cross-border access to: (a) satellite and meteorological data across regions, (b) real-time insights on planting and harvesting seasons, and (c) information on cost-effective techniques for crop development and protection as well as sales opportunities.

**Remote health services for medically underserved populations, and the search for tomorrow's medical treatments** also depend upon cross-border access to data and cloud enabled technologies. Cross-border access to remote health service technology platforms help remote and medically underserved population groups secure diagnostics, consultation, and preventative care and treatments that might otherwise not be available. Similarly, cross-border access to clinical testing and other biopharmaceutical R&D data aids in the study and development of treatments for diseases – including infectious and lifestyle diseases that are globally prevalent, as well as rare and neglected diseases.

**Building trust in developing digital economies by keeping personal data confidential, secure, and free from misuse** often depends upon cross-border access to data and cloud enabled technologies. Cross-border access to cloud-based and AI enhanced cyber security solutions that

reside in data centers abroad helps protect developing country users from cyber-crime, fraud, theft of valuable information, and other abusive online behavior. A digital economy that can support economic development requires first and foremost an environment that offers adequate security and confidentiality for persons to be able to freely engage remotely with others in personal and business interactions without fear of being compromised. From a technological perspective, cloud-enabled software security solutions require the real-time ability to consolidate and analyze data from diverse sources and regions in order to identify anomalies and security risks.

**Advances in financial inclusiveness, financial transparency, and financial security** across developing countries also depend upon cross-border access to data and cloud-enabled technologies. There are over 2.5 billion unbanked people worldwide, many living on remote and isolated locations lacking in banks or other on-the-ground financial service providers.[2] Technologies that leverage data flows are powerful tools to increase access to financial services, helping individuals achieve sustainable livelihoods. These include:

- Microlending: Increasingly, microfinance institutions use technologies based on data flows to allow them to provide better loans, achieve greater repayment rates, and lower interest rates for applicants. For example, in many developing countries, local financial institutions are able to offer micro-loans to citizens and businesses that would not otherwise have access to credit, using cloud-enabled data analytics to determine credit risk profiles and deliver loans through automated processes.[3]

- Remittances to developing countries: More than ever, remittances are of vital importance in developing countries. According to the World Bank, remittances to low and middle-income countries reached a record high of $529 billion in 2018.[4] Companies are also exploring the use of emerging technologies such as blockchain to provide speedier and cheaper remittance processes. Financial institutions that participated in the program reported savings between 40 and 70% in foreign exchange costs, and payment times averaging a few of seconds. Various other financial service companies are exploring innovative ways to leverage similar technologies to reduce costs and provide better remittance services to benefit more people.[5]

- Credit-scoring for MSMEs and individuals in developing countries: MSMEs, as well as some specific demographics may not have access to optimal lending opportunities if traditional credit scoring methods are employed. Cutting edge technologies such as data analytics (to review available past data) and artificial intelligence (to anticipate future outcomes) play an important role in the expansion of credit channels available to these underserved customers. These technologies heavily rely on cross border data flows. Oftentimes, the data used to enable the cloud-based service being delivered must travel across borders, even if the financial service provider and its customer are in the same country.[6]

- Financial transparency, anti-corruption, and anti-money laundering: As compared with cash-based transactions, increased use of “mobile transfers” and “mobile money”, which often depend upon cross-border access to cloud-based financial service platforms, allow

for enhanced transparency in public sector spending; reduced corruption and 'off the books' cash transactions; and increased confidence, efficiency, and predictability in the banking system. Access to cross-border technologies also allows for data analytics that are better able to identify potential cases involving money laundering, terrorist financing or other criminal financial transactions. In these ways, cross-border data transfers enhance financial legal compliance and improve the ability of financial regulators to identify and respond to emergent criminal activity or other risks.

## The Costs of Data Transfer Restrictions and Data Localization Mandates

The unintended economic consequences of unreasonable data transfer restrictions and data localization mandates must not be underestimated. Such measures have consequences in terms of jobs, exports, and investment. For both local enterprises and foreign-invested enterprises, such measures disrupt operations; raise the costs and challenges of providing services and manufacturing goods; and make it harder to invest and keep local workers employed. Among other things, such measures effectively deprive end-users of advanced services and put them at a competitive disadvantage compared with companies in other countries. We elaborate on each of these points below.

First, data localization mandates and unreasonable data transfer restrictions are **particularly damaging to local industries, including agriculture, logistics, and manufacturing (e.g., textiles)**. In fact, it has been estimated that 75% of the value of data transfers accrues to traditional industries.[7] Data transfers enable MSMEs to connect and find prospective customers in overseas export markets. MSMEs and other firms also rely on data flows to increase their productivity, drive quality, and improve output in other ways. Companies depend upon the ability to integrate software and other emerging technologies at every stage of the production and value chain. Data-enabled software innovations are connecting suppliers, manufacturers, and service providers around the world, while accelerating efficiencies relating to product design, engineering, production, logistics, marketing, and servicing. Cross-border data transfer restrictions impede the ability to realize these efficiencies.

Second, data localization mandates and unreasonable data transfer restrictions **raise the costs of international trade**. Data transfers are critical to reducing the costs to local firms of exporting to other markets. One recent study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%.[8] Likewise, electronic commerce platforms, which operate on the basis of cross-border data transfers, are estimated to reduce the cost to local firms of distance in trade by 60%.[9] When countries impose unreasonable data transfer restrictions and data localization mandates, they prejudice their local industries' ability to realize these significant welfare-enhancing benefits and efficiencies.

Third, data localization mandates and unreasonable data transfer restrictions **hurt local innovation and competitiveness**. A country that limits cross-border data transfers limits its own industries' access to technologies and data sources that are critical to growth and innovation, business operations, and the transfer of technology. These include: (a) productivity-enhancing software solutions; (b) scientific, research, and other publications; and (c) manufacturing data,

blueprints, and other operational information. Faced with higher software costs and an unpredictable environment for R&D investments, local industries face challenges keeping technological pace with foreign competitors — threatening both domestic and export market sales. Furthermore, as data restrictions place an undue burden on industries operating in countries imposing them, they also undermine those countries' attractiveness as a destination for investment and R&D.

Fourth, data localization mandates and unreasonable data transfer restrictions **undermine access to tailored data-enhanced analytics and insights that can help address economic and societal challenges**. A country that limits cross-border data transfers also may exclude itself from the development of data analytics and AI-driven technology solutions that can help address economic and other challenges. Local industries and economies can face competitive harm if they are deprived of the insights that come from consolidating local data sets within larger regional or global data sets for purposes of data analysis.

In the foregoing ways, data localization mandates and data transfer restrictions harm local MSMEs and other local enterprises.

---

[1] *See* https://ca.go.ke/wp-content/uploads/2019/05/Kenyas-Digital-Economy-Blueprint.pdf
[2] USAID, US Global Development Lab website, available at: https://www.usaid.gov/digital-development/digital-finance
[3] *Alternative Lending in Mexico* https://lending-times.com/2018/02/08/alternative-lending-in-mexico/
[4] https://www.worldbank.org/en/news/press-release/2019/04/08/record-high-remittances-sent-globally-in-2018.
[5] https://blogs.worldbank.org/psd/paying-across-borders-can-distributed-ledgers-bring-us-closer-together
[6] Innovative technologies based on data are important to enhance the accuracy of credit scoring for MSME's, which employ a large percentage of the population worldwide and help fuel the global economy. For example, Tradeteq, a smart technology trade finance platform, uses a credit model based on artificial intelligence that goes beyond financial information, and includes socio-economic, geographical and other information about the company, that are used to base finance investment decisions. The algorithms used to power this tool also rely on a large amount of data collected, processed, and analyzed in various parts of the world. Tradeteq, the AI-driven trade finance investment platform, available at https://www.finyear.com/Tradeteq-the-AI-driven-trade-finance-investment-platform_a40656.html
[7] *See* Global Data Alliance, *Cross-Border Data Transfer – Facts and Figures* (May 2020), at : https://globaldataalliance.org/downloads/gdafactsandfigures.pdf
[8] Micro-Revolution: The New Stakeholders of Trade in APAC, Alphabeta, 2019.
[9] Concept Note, p. 30.