The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018

BY NIGEL CORY | JANUARY 2019

When countries impose protectionist policies in high-value, high-tech sectors, they do not just damage competitors; they damage the entire global innovation system.

As they continue to compete in advanced technology industries, many countries are doubling down on digital protectionism and innovation mercantilism. While these forms of protectionism typically rely on behind-the-border regulations rather than tariffs to protect local firms, the objective and impact remain the same—either to replace foreign goods and services with local ones, or to unfairly promote exports, or both. These destructive "beggar-thy-neighbor" tactics often target the data, technologies, and services of high-tech firms involved in sectors such as Internet-based services, data analytics, and electronics.

Innovation mercantilist and digital protectionism measures do not just damage other economies and businesses; they damage the entire global innovation and trading system, leading to less overall innovation and productivity growth.

This sixth annual report documents what the Information Technology and Innovation Foundation (ITIF) views as the world's worst innovation mercantilist practices proposed, drafted, or implemented in 2018. As some countries put in place more than one mercantilist policy, eight nations or regions make the list this year:

- China: Enacted a new standardization law that shuns international principles and best practices and could be used to favor local tech firms and their products.
- China: Enacted a new law which could potentially force firms to store data only in China if it is related to privately funded, commercially focused research.

- Europe: Attempted to introduce a mercantilist digital services and digital profits tax that would have targeted U.S. tech firms almost exclusively.
- Kenya: Considered requiring forced local data storage for sensitive personal data as part of a draft data protection bill—which also included other mistaken policies, as Kenya blindly follows the European Union (EU) approach to data privacy.
- India: Enacted e-commerce regulations that specifically target and discriminate against foreign firms.
- India: Enacted unnecessary and discriminatory local data storage requirements for payment data.
- Indonesia: Enacted changes that allow it to enact tariffs on imports of digital products, such as downloads of movies, e-books, and software.
- Italy: Enacted rules to discriminate against video-on-demand streaming services to protect cinemas.
- Saudi Arabia: Enacted forced local data storage for various categories of data as part of its Cloud Computing Regulatory Framework.
- Turkey: Enacted forced local data storage for publicly listed firms.

Any analysis of trade mercantilism in 2018 would be incomplete without mentioning that the United States enacted a series of misguided policies and tariffs that distract and detract from the real need for coordinated and sustained effort to confront cases of innovation mercantilism and digital protectionism, especially in China. Raising dubious national security concerns about automotive imports and enacting tariffs on steel and aluminum imports from trading partners such as Canada, the European Union, and Japan means these partners are less likely to work with the United States on the much more pressing issue of innovation mercantilism in China. While the Trump administration's confrontation with China over its trade and economic policies is welcome and well overdue, without the help of its likeminded trading partners, the United States is not likely to succeed in changing China's policies.

THE NATURE OF INNOVATION INDUSTRIES

Reporting on, and ultimately responding to, cases of innovation mercantilism—and within it, digital protectionism—should matter to policymakers as they target the firms and sectors that play a key role in maximizing global innovation. A growing number of economists have come to recognize that it is not the accumulation of capital but rather innovation that drives countries' long-term economic growth. Innovation—the implementation of new or significantly improved products, services, processes, business models, or organizational methods—has become the central driver of economic well-being

and competitiveness for most countries. For instance, at least half of America's economic growth can be attributed to scientific and technological innovation.[1] Innovation also plays an indispensable role in helping address global challenges, such as developing sustainable sources of food, improving education, combating climate change, meeting the needs of growing and aging populations, and increasing per-capita incomes.

But innovation does not fall like manna from heaven. Rather, innovation is a product of complex national innovation systems, supported by a thoughtful and comprehensive set of innovation-enabling public policies that collectively impact the capacity and ability of both private and public actors to effectively innovate. Successful innovation requires industry and government to commit resources and take risks as part of an overall ecosystem that supports enterprises' ability to innovate.

To maximize innovation, the global trading system needs to get three key factors right: 1) ensuring the largest possible markets, 2) limiting nonmarket-based competition; and 3) ensuring strong IP protection.

What then are the attributes that define these innovative businesses and, by definition, innovation industries?[2] First, true innovation industries are ones for which the rapid and regular development of new processes, products, or services—many of them disruptive in nature—is critical to their competitive advantage. For example, industries such as biotechnology and semiconductors are innovative, as their success depends not on making a particular drug or semiconductor cheaper, but on creating the next-generation product.

Second, the marginal cost of selling the next product or service is significantly below the average cost of producing it in innovation-based industries. The digital content industry (e.g., software, movies, music, books, and video games) is perhaps the most extreme example of this. In some cases, the first copy costs hundreds of millions of dollars to create, while additional digital copies are produced at virtually no cost.

Finally, innovation industries depend more on intellectual property—particularly on science- and technology-based IP—than other industries. For example, software depends on source codes, life sciences on discoveries related to molecular compounds, aerospace on materials and device discoveries, and content industries on digital, copyright-protected content.

Innovation mercantilism and digital protectionism undermines the following three key factors needed to maximize innovation:

1. **Ensuring the largest possible markets:** For innovation industries with high fixed costs in design and development, but lower marginal costs of production, larger markets are critical because they enable firms to cover those fixed costs—so unit costs can be lower and revenues for reinvestment in the next generation of innovation higher. This is why firms in most innovation industries are global. If they can sell in, say, 20 countries rather than 5, although their sales expand by a factor of 4, their total costs increase by much less than that. Thus, numerous studies have found a positive effect of the ratio of cash flow to capital stock on the ratio of research and development investment to capital stock. But a host of different innovation mercantilist policies act to limit global market size, both at the enterprise and establishment levels.

2. **Limiting nonmarket-based competition:** Large markets enable firms to sell more. But if larger markets come with larger numbers of competitors, total sales per firm can remain the same or even fall. Conventional wisdom holds that this competition is good for innovation. However, many studies have demonstrated that innovation and competition can be modeled according to an inverted "U" relationship, with both too much and too little competition producing less innovation.[3] Some innovation mercantilist policies—including discriminatory government procurement practices, protected state-owned enterprises, and government bailouts—enable weak firms to enter into or remain in a market, siphoning off sales from stronger firms and reducing their ability to reinvest in innovation.

3. **Ensuring strong intellectual property protections:** Firms in innovation-based industries depend on intangible capital, much of it being intellectual property. Strong intellectual property protections are needed to enable inventors to realize economic gains from their inventions— further giving them the ability to reinvest those profits into the next generation of innovative activities. However, if competitors are able to enter into or remain in a market because they obtain an innovator's intellectual property for less than the fair market price (through either theft or coerced transfer), they are able to siphon off sales that would otherwise go to innovators.

Innovation mercantilist policies cause more global economic damage than mercantilist policies affecting other industries (e.g., clothing, lumber)—which is problematic. These trade-distorting policies also harm the nations that use them. Despite their promise of delivering some short-term employment and economic gains, these policies ultimately lead to far worse adverse consequences. They can lead to increased costs of key capital goods (e.g., information and communications technology products), which in turn reduces their overall use—and lowers a country's innovation and productivity. They can also limit countries' participation in global value chains for the production of high-technology products. These policies can lead to broad economic inefficiencies and cause reputational harm that can damage a country's attractiveness as a location for foreign direct investment. Tending to isolate nations from the global economy while often failing to achieve their intended aims, such policies are fundamentally unsustainable, in part because they engender reciprocal protectionist policies by other countries—which undermines the global economic order. Perhaps most importantly, they lead to unbalanced and unsustainable "dual economies," with weak productivity growth in non-favored sectors.[4]

Countries using these policies instead need to recommit to competitive markets, open trade, and economic liberalization. Strong productivity- and innovation-enhancing policies should be at the core of countries' economic development strategies, which should include investments in education, research, and digital infrastructures. Such an approach would prove a far more effective path for broad economic growth than shortsighted mercantilist

policies. At the same time, the community of nations committed to rules-based trade needs to do much more to push back against other nations' innovation mercantilist policies.

THE WORST INNOVATION MERCANTILIST POLICIES OF 2018

The following ten innovation mercantilist policies, including digital protectionism, are by no means an exhaustive list of unfair trade practices nations proposed, drafted, or implemented in 2018. We believe these are the most egregious, policies the policymakers and the global trading system needs to address as a top priority.

China Shuns International Principles and Enacts a New Standardization Law That Could Favor Local Tech Firms and Products

On January 1, 2018, China's new standardization law came into effect. Depending on implementation, the law could affect a significant range of economic and trade activity as it potentially favors local firms and goods and services through its reference of "indigenous innovation." China's refusal during the drafting process to reference either its World Trade Organization (WTO) commitments or its acceptance of existing international standards has raised further concerns about potential discriminatory intentions. China's creation of unique levels of standards (e.g. social and enterprise standards), when combined with uncertainty surrounding actual implementation and enforcement (e.g. whether voluntary standards are actually mandatory), adds further uncertainty for foreign firms. Such nontransparent and discriminatory standards can act as a significant barrier to trade, especially for high-tech goods and services.[5]

Standards unique to China make it more difficult and costlier for foreign firms and their products to be sold in China. This supports China's overarching goal to reduce reliance on foreign technology.

While standards are based on enabling free trade, they are an important (and often overlooked) component of global trade. A standard is a document, established by consensus, that provides rules, guidelines, or characteristics for activities or their results.[6] At their most basic, standards establish the size, shape, or capacity of a product, process, or system. They can specify performance of products or personnel. They define terms such that there is no misunderstanding among those using the standard. They reduce uncertainty by creating a common technological platform upon which any actor can develop new applications. Standards govern the design, operation, manufacture, interoperability, and use of nearly everything a firm produces.

Ensuring standards are compatible fosters economies of scale by making it relatively easy for firms to produce a good/service to a mutually accepted standard across markets. Standards development systems and the infrastructure necessary to ensure conformity to standards—including testing, certification, and laboratory accreditation—are therefore an important part of modern production and trade.[7] Well-organized, open, and transparent standards systems promote compatibility of key components in national infrastructure—especially in high-tech sectors such as telecommunications and computer networks.[8] In essence, standards form a bridge between markets and technologies.[9] A review of econometric studies shows there is often, but not always, a positive relationship between international standards and exports or imports—which is in line with the widely held view that international standards are supportive of trade.[10] Efficient international standards

regimes also facilitate the diffusion of innovative technologies and production techniques, and serve to increase network effects that in turn support innovation.[11]

China's new Standardization Law creates a potential barrier to trade that contravenes commitments China made when it joined the WTO to neither use standards as a barrier to trade nor set standards that discriminate against foreign products. Article 20 of the new law states: "The State supports the use of indigenous innovative technology to develop social organization standards and enterprise standards in key sectors, strategic emerging industries, critical & generic technology and other fields." This article, which read alongside others contravenes the WTO Technical Barriers to Trade (TBT) Annex 3 (paragraph d) provision that "The standardization body shall accord treatment to products originating [in] the territory of any Member of the WTO no less favorably than that accorded to like products of national origin."[12]

While the concept of "indigenous innovation" is not clearly defined in Chinese policymaking, past practice shows that it is normally a signal for favoring domestic firms and discriminating against foreign firms. In the standards context, it should be seen as an extension of China's past adeptness in using laws and regulations to create a framework to discriminate against foreign firms and their products. As ITIF's report "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" argues, China has made the development of indigenous technology standards, particularly for information and communications technology (ICT) products, a core component of its industrial development strategy. China has done so believing indigenous technology standards will advantage China's domestic producers while blocking foreign competitors and reducing the royalties Chinese firms pay for foreign technologies.[13]

China could have made clear it was committed to global rules and best practices on technical standards if it had explicitly acknowledged and reinforced both its WTO TBT commitments and its core principles—but it chose not to.[14] For example, in multiple provisions, China could have referenced its WTO TBT commitments—specifically Annex 3 of the TBT agreement—with respect to international standards , which includes language that upholds the globally accepted principles of international standardization.[15] China could have also made clear its aim was not to use standards as a trade barrier by including language that prioritized the use of existing international standards, where relevant, such as by adding the following phrase to relevant articles: "Where international standards exist, they shall be used as the basis for the standard except where they would be ineffective or inappropriate."[16] These types of provisions would have sent a clear signal that China wanted its approach to be consistent with global best practices.

Instead, in article 8, China included language ("[A]dopts international standards based on China's actual conditions") that allows it to not adopt international standards, which runs counter to common practice in many other countries. In a similar vein, China could have made its intentions clear by including framing language from the WTO TBT statement that "Technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade. For this purpose, technical regulations shall not be more trade-restrictive than necessary to fulfil a legitimate objective,

taking account of the risks non-fulfilment would create."[17] But again, China did not include any reference to the WTO and the TBT agreement in the law.

The Standardization Law also includes other potentially onerous (depending on implementation) requirements that will add unnecessary costs and risk disclosing sensitive company data and intellectual property, such as requiring firms to publicly disclose internal company practices.[18] Furthermore, foreign trade associations and firms lobbied the policymakers that drafted the law to include a dispute resolution mechanism that gives firms the right—and means—to appeal any rulings made by standards-setting organizations. In the end, because China chose not to include any such mechanism (which had existed in an earlier draft), all issues will be handled by processes under the auspices of the State Council—which is not a viable path for the speedy or impartial resolution of disputes.[19]

For foreign firms and trading partners, the new Standardization Law is simply one part of a broader wave of new standards laws, regulations, and implementing guidelines China has recently released, which together, create significant uncertainty.

The impact of China's new Standardization Law could potentially be significant. A major concern (based on historical experience) is differential and discriminatory enforcement by implementing agencies. Standards unique to China make it more difficult and costlier for foreign firms and their products to be sold in China, as they need to reconfigure preexisting design and production processes to Chinese standards and pay royalty fees for providing products using the Chinese standards. This disrupts the global, generally standardized production processes on which many foreign companies rely in order to compete. Ultimately, it could cut foreign firms and technology from the Chinese market in strategically important technologies.

For foreign firms and trading partners, the new Standardization Law is simply one part of a broader wave of new standards laws, regulations, and implementing guidelines China has recently released, which together, create significant uncertainty. For example, following the passage of China's new cybersecurity law, China's information technology standards body TC 260 released 110 standards for comment between November 2016 and September 2017 alone, accounting for nearly half of all standards it has ever released for comment.[20] The varying efficacy of these new laws and regulations (as some are hastily drafted and vaguely detailed) leaves foreign trading partners and firms struggling to engage in the feedback process. Political and bureaucratic pressure in China to produce standards rapidly has led regulators to offer comment periods that often fall far short of China's WTO commitments under the TBT agreement—which calls for 60-day comment periods and a mandatory reply to all comments received from stakeholders. The number of draft standards and the timing and process for feedback are critical as China uses standards as a final implementing guideline of laws, meaning this standard-setting feedback process is often the last chance to push for changes.

The Standardization Law is the latest in a long line of examples wherein China develops national standards that deliberately differ from international standards. This has been a concern for some time. For example, according to the WTO, in 2007 only 46.5 percent of Chinese national standards were equivalent to international standards.[21] China's divergent

approach to standards is particularly clear when it relates to technologies with strong data security concerns. A report by the German think tank Mercator Institute for China Studies (MERICS) shows that Chinese standards for basic smart manufacturing correlate with about 70 percent of relevant international standards—which is only around 53 percent for key smart manufacturing technology standards, and zero for standards relating to cloud computing, industrial software, and big data.[22]

China's use of the Standardization Law to favor local firms and products is not incidental, but a key feature of China's economic plans to promote indigenous Chinese technology and intellectual property. Nor is the law's use of vague, unclear language unique, which China often uses to avoid WTO disputes, while allowing the government maximum flexibility and discretion to apply onerous and selective provisions where it sees fit. For example, China relies on many of the standards it sets being "recommended" and therefore supposedly voluntary, when in fact they are "mandatory"—which would thereby more clearly contravene WTO rules and global best practices. In 2017 alone, over 1,000 Chinese standards submitted to the WTO were downgraded from required national standards to recommendations.[23]

China enacted new rules that raise the potential for it to impose restrictions on the export of scientific data generated by private firms involved in strategic high-tech sectors.

China is adept at using all possible tools to achieve its high-level economic goals of ultimately reducing China's reliance on foreign technology. While lower-level technical officials involved in setting standards may understand and prefer stakeholder engagement and market-friendly standards, higher-level officials may have national development goals in mind. For example, a development strategy for establishing national standardization 2016–2020 lists "possessing indigenous intellectual property for critical technology in enterprise and social standards" among its important tasks, including, increasing the international influence of the "Chinese standard."[24] This has been enacted in specific sectors. For example, with the Internet of Things, China aims to create sensing and perception class standards with indigenous intellectual property.[25] The same goal is planned for autonomous vehicles.[26] A basic principle of China's New Energy Vehicle Plan is to "expedite the formation of technology, standards, and brands using indigenous intellectual property."[27]

China (Potentially) Blocks the International Transfer of Scientific Data

On March 17, 2018, China enacted a law that could allow it to force firms to store privately funded scientific data in China (a practice known as "data localization"). Whether the high-level principles in the Measures for the Administration of Scientific Data (the "Measures") will do this depends upon implementing guidelines and instructions from the Ministry of Science and Technology (MOST), which has yet to do this. The Measures raise concerns for foreign firms and trading partners because they were designed along the lines of other local data storage policies that have acted as barriers to digital trade (mainly broad, vague, and with plenty of room for differential and discriminatory enforcement) and the high-tech sectors potentially affected by it are those that China has prioritized as part of its strategic development plans (such as Made in China 2025).

The official goals of the Measures are to spur the dissemination of scientific data to accelerate technological innovation. Scientific data is broadly defined as "data generated through basic research, application research pilot development tests, or other such life production-type data and raw data and derivative data obtained through monitoring and observation, investigation, inspection and testing, and used for scientific research."[28] In some respects, it does support the dissemination of scientific data in pursuing the principles of openness, sharing, and full use of data related to research funded by the government. Article 24 requires the producer of scientific data to provide either free or low-cost access to data stored at scientific data centers whenever data will be used for a broad range of public-interest-related purposes, such as government decision-making, public security, national-defense-related construction, environmental protection, disaster prevention and relief, or nonprofit scientific research. When the use is for business purposes, the data owner and prospective data user must enter into an agreement that specifies rights, obligations, and fees.

The Measures apply to the "acquisition, generation, processing, organizing, dissemination, sharing and management" of scientific data when the data is "supported by government funds." The Measures indicate that central and provincial science and technology agencies will designate specific entities to set up and operate "scientific data centers." All scientific data generated by relevant institutions and firms that use government funds must be stored in China for "consolidation." At a minimum, the Measures require a local copy of scientific data (in the case of research connected to government funding) to be stored locally in case a foreign journal requires the underlying data to be submitted alongside an academic paper it is publishing. Notably, the Measures appear to apply not only to data generated in China, but also, under certain circumstances, to data generated outside of China, such as foreign research funded by the Chinese government.[29]

Foreign firms' main point of concern with the Measures is it potentially applies to their private, commercially funded research. As enacted, the Measures apply to research institutions, higher education institutions, and (potentially) private firms. The Measures "encourage" private firms to store scientific data in government-mandated data centers, where access to the data by the Chinese government is much easier. Whether this is actually voluntary or mandatory in practice has yet to be seen (which China often does in using vague language to avoid provoking a response from firms or trading partners, but backs "encouragement" by the "stick" of capricious enforcement of a variety of regulations).

Concerns about this potential application stem from China's overarching approach to innovation, data, and foreign technology, and its tendency to use these types of behind-the-border policies to disadvantage foreign firms. Indicative of this, the Measures explicitly mention that scientific data must meet the "secure and controllable" principle. This term has not been publicly defined by regulators but is understood by many trading partners, trade associations, and individual firms to mean "Chinese-controlled" in that it does not use foreign products and technologies.[30] A separate red flag about China's intentions is it

did not publish this measure in draft for public comment, nor provide a standard 60-day window for feedback, as per its WTO commitments.

Further feeding into concern about China's goals for these Measures is they potentially apply to privately funded research in a potentially broad range of commercial sectors. The Measures' vague and broad definitions could cover scientific data generated by institutions and firms that concerns state secrets, national security, or "societal and public interests." Indicative of the potentially wide scope of application, China's National Security Law uses a broad definition of national security, including in the areas of culture, food, and health, which have only a remote connection to military or intelligence security.[31] Under "societal and public interests," the Measures could apply to a broad range of private-sector economic activity, such as biochemical lab testing results, computational models, raw weather data, and records from clinical trials.

China's recent decision to restrict the transfer of genetics data is instructive in how this new law on scientific data could be implemented to create a barrier to international trade and research.

China's approach to genetics data is an example of why firms and trading partners are right to be concerned about the potential for this law to lead to data localization. In October 2018, China named and shamed several companies that had breached regulations (enacted in 1998) on the sharing of its citizens' genetic material and information.[32] There was no explanation as to why these breaches—some a few years old—were released; it was the first reported instance of enforcement. Although these regulations are supposed to have minimal impact on research, scientists say that complying with them is creating obstacles to sharing and transferring data. For instance, an international collaboration investigating genetic samples from more than 140,000 pregnant Chinese women had to send a data analysis expert to China because the data could not leave the country.[33] China's approach will have a broader chilling effect on the sharing of raw genetics data for research purposes as it prohibits the publishing of anonymized genetic data in academic journals. As Nicholas Steneck (who studies research integrity at the University of Michigan in Ann Arbor) stated in the *Nature* article on the case above, "The rise of nationalism in many countries means that governments will increasingly protect their national resources, including genetic data, even if it means slowing the progress of science."[34]

Ultimately, if the Measures only apply to Chinese-government-funded research, they would be somewhat consistent with policies encouraging open access to publicly funded research data in Europe, the United States, and elsewhere. (Other nations do not generally require local storage on government-mandated data centers.) However, in a worst-case scenario, if foreign firms operating in a range of high-tech sectors are "encouraged" to store their research and development data in these centrally designated data centers, it would raise trade issues. For example, the increased likelihood a firm's intellectual property would be exposed to theft (because the government or intermediary could transfer it to local firms). What would happen if a Chinese firm were doing outsourced research work for a foreign company (such as a pharmaceutical firm) and were bound by confidentiality provisions not to disclose this data, but were required under the Measures to disclose the data because it relates to the public (health) interest (as it is unclear whether there will be an exception for such confidentiality clauses)?[35] Likewise, it potentially exposes a firm's

data to unauthorized disclosure in the event the centralized data center is hacked (as the data center may not enact best-in-class cybersecurity measures), or via other unauthorized access by the government or other nongovernment actors. A centralized data center holding a range of commercially sensitive data for a number of high-tech sectors would be an attractive target.

Data localization for private-sector scientific data would disadvantage foreign firms and act as a barrier to trade. It could force firms to redesign how they generate, collect, store, and use data if they have to (at some stage) transfer some part or all of their dataset to the centralized data center. Also, firms rely on a seamless, free flow of data as part of research operations, which often span different business units around the world. Local data storage and the need for transfers to be approved limits how many foreign firms use data to drive innovation. While scientific data management policies differ by disciple and region, such a requirement would be unique and provide an opening for the government to target foreign firms and their privately developed commercial technologies.[36]

The European Commission has proposed a mercantilist "digital services tax" that would have nearly exclusively targeted U.S. tech firms.

While the Measures have already gone into effect, there remains significant uncertainty about the mechanisms described within and how they'll be implemented and enforced. In a best-case scenario, MOST provides clarifying advice that precludes any such discrimination, followed through with narrow, transparent, and fair implementation and enforcement, such that foreign firms are not caught up in a measure that largely targets research that is fully or partially funded by the Chinese government. However, no such clarification has been issued. Furthermore, in a WTO submission in October 2018, the United States asked whether China would suspend implementation of this measure so that it can seek public comment on it and revise it as appropriate in light of the concerns raised by stakeholders.[37] China has not done so.

Europe Attempts to Introduce a Mercantilist Digital Tax

In March 2018, the European Commission (EC) recommended its members agree to a mercantilist digital services tax (DST) that would tax the portion of a digital firm's revenues attributed to a European member state; and a digital profits tax (DPT) that would tax the corporate profits derived from member states. These taxes are nearly exclusively targeted at U.S. tech firms—France's finance minister called it a GAFA tax (for Google, Amazon, Facebook, and Amazon). The main motivation, not surprisingly, is money. Supporters of the EC's proposals, who are convinced large data companies—almost all of them American—earn too much money from European citizens, want to claw some of those funds back. Instead of waiting for an emerging international consensus (being developed by the Organization for Economic Cooperation and Development [OECD]) around how to improve taxation of international digital activity, the EC and key members wanted to push ahead the effort with the short-term goal of grabbing revenue and the long-term goal of disadvantaging U.S. tech firms.

The proposal included two parts. The first was to impose a 3 percent tax on Internet firms' topline revenues, instead of their bottom-line profits. The law would have only applied to

firms with roughly $850 million (€750 million) in global revenues, including at least $55 million (€50 million) generated by collecting data or selling services in the European Union—a class of firms comprising (mostly) American firms, while allowing many EU firms to escape. The second proposal would enact a permanent data services tax on the profits of these Internet companies. It would essentially rewrite current practice—which prevents a country from taxing a foreign company's profits unless the company has a permanent establishment inside the country's territory—on the dubious theory that much of the value Google, Facebook, Uber, and others create comes from European citizens.

The proposals are clearly mercantilist in nature. It is highly unusual to implement a specific tax on only one type of firm, especially one not connected to profits. Because most of these companies are American, these changes would impose a large loss, on not just U.S. firms, but U.S. taxpayers as well. The latter would suffer to the extent firms could deduct the foreign tax from their U.S. taxes. As Germany's Council of Economic Experts warmed, the DST could be interpreted as a "unilateral EU tariff against the United States [which] could send negative impulses in the trade dispute with the United States."[38] The mercantilist intent of the tax became clear as the DST proposal was debated. The European Union, in its internal deliberations, also recognized there were questions regarding whether the DST would be "consistent with the EU's WTO obligations."[39] More specifically, the high revenue thresholds that subject a firm to the DST, and the exclusion of certain revenues widely earned by European firms (such as subscription fees earned by firms such as Spotify), platforms that facilitate financial trades, platforms that facilitate payments between households and firms, all forms of telecommunications, and crowdfunding platforms, create de facto discrimination against U.S. digital firms, in violation of the EU's national treatment commitment under the WTO General Agreement on Trade in Services (GATS).[40]

Virtually everyone agrees that international taxation needs significant reform and that corporations should pay their fair share of taxes. The challenge comes over which nations get to claim those taxes. The OECD is in the midst of a major effort on Baseline Erosion and Profit Shifting (BEPS). It issued an interim report in March 2018 on the tax challenges arising from digitization.[41] The report acknowledged several legitimate issues of concern and committed the members to a two-year effort to develop a consensus on these issues, including the concept of nexus and the allocation of profits. This commitment was affirmed at a recent G20 meeting of finance ministers. But rather than wait for this international initiative to bear further fruit (expected in early 2019), the EC was determined to push ahead.[42]

Thankfully, both digital tax proposals need(ed) unanimous approval among EU members to take effect. Beyond this, there is the potential to apply the seldom-used "enhanced cooperation" procedure within the European Union if nine or more-member states wish to take the proposal forward—but this has not been mentioned as a possibility. Both outcomes appear unlikely. Unanimous support is also unlikely as Ireland and Scandinavian countries, among others, have objected to the proposal. With this, on December 3, 2018,

EU finance ministers failed to agree on a digital tax, despite a last-minute Franco-German plan to salvage the proposal by narrowing its focus to companies such as Google and Facebook.[43]

Even with this defeat (or setback), the danger of EU countries subjecting U.S. companies to discriminatory taxes remains high as individual EU member countries are free to pass their own national laws, even if the European Union does not do so as a block. On January 1, 2019, France's minister of economy and finance, Bruno Le Maire, announced that a "GAFA tax," which extends to advertising revenue, platforms, and use of personal data, had come into immediate effect.[44] Meanwhile, several other European countries have announced a desire to impose a unilateral tax on the largest Internet companies.[45] The United Kingdom has already announced its intention to implement a 2 percent revenue tax on digital services.[46]

Kenya Mistakenly Follows the EU Approach to Data Privacy and Considers Data Localization for Sensitive Personal Data

Kenya's draft Data Protection Bill includes several misguided local-data-storage provisions and a willingness to blindly follow the European Union's approach without considering the actual impact on privacy and innovation.

In 2018, Kenya released a draft Data Protection Bill for comment that included a number of provisions that either directly or indirectly lead to data localization.[47] The bill is being debated and is open to revisions. It aims to implement the right to privacy, pursuant to Article 31 of Kenya's constitution. Kenya is emerging as a dynamic and growing digital economy, but this bill could hamper that development. The challenges facing Kenya are not unique as data protection is a relatively new and evolving area of law and policy in Africa—where only 17 of 55 countries have data protection laws.[48] However, the draft bill reflects the potential for countries to enact misguided rules around data protection and privacy that have broader economic and societal implications.

The main problem with the draft bill is its misguided belief that the geography of data storage improves data privacy and security. Forcing firms to store data locally—a concept known as data localization—does neither (as explained below).

Kenya's Data Protection Bill (part VI, section 44) states:

(1) Every data controller or data processor shall ensure the storage, on a server or data center located in Kenya, of at least one serving copy of personal data to which this bill applies.

(2) The cabinet secretary shall prescribe, based on strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data center located in Kenya.

(3) Cross-border processing of sensitive personal data is prohibited.[49]

The draft bill also includes other vague and potentially broad provisions that raise the specter of further localization and sudden changes to key legal requirements for firms managing data in or from Kenya. The draft bill allows the proposed data commissioner to create new categories of sensitive personal data (to be stored locally), and the cabinet secretary to designate categories of critical personal data that can only be processed in

Kenya on grounds of "strategic interests of the state or on protection of revenue." Beyond the vagueness of what "protection of revenue" means, together, these provisions raise considerable uncertainty for firms—especially foreign ones—about how to abide by Kenyan privacy law and how they operate in Kenya (or if they can, in the likely scenario the firm is foreign and uses IT systems based outside of Kenya). In addition, the bill repeatedly makes the false connection between the geography of data storage and processing and data protection by associating international transfers with risks and dangers. The draft bill (section 45.1.b) states that transfers of personal data outside of Kenya require people to give their explicit consent, "after having been informed of the possible risks of the transfer, such as the absence of appropriate security safeguards."[50]

The notion that data must be stored domestically in order to ensure it remains secure and private is false. Policymakers focusing on geography to solve cybersecurity and privacy concerns are missing the point. Consumers and business can rely on contracts or laws to limit voluntary disclosures to ensure data stored abroad receives the same level of protection as data stored at home. Obviously, countries have the prerogative to determine how companies use data (as in parts of this bill), but this again highlights how the focus should be on how companies treat data—and holding them accountable to it—rather than where data is stored.

Countries have the prerogative to determine how companies use data, but this highlights how the focus should be on how companies treat data—and holding them accountable to it—rather than where data is stored.

Local data storage can actually undermine personal data protection. Without an independent judiciary and set of legal protections, local data storage can facilitate easier access to personal data for governments, such as for social or political reasons, as they can bring more pressure and tools to bear in forcing local providers to disclosure data. The fact that Kenya's draft bill only requires a copy of data to be stored locally, rather than prohibiting transfers of all data, certainly lays the groundwork for such an outcome.

Furthermore, personal data may be more susceptible to inadvertent disclosures if the local data center is not committed to enacting best-in-class cybersecurity measures. Such security and data breaches can happen no matter where data is stored, as data centers everywhere are exposed to similar risks. Such inadvertent disclosures are the result of security failures. When it comes to data storage and protection, it is important the company involved (which either runs its own networks or uses a third-party cloud provider) be dedicated to implementing the most advanced methods to prevent such disclosures. The location of these systems has no bearing on security.

What this shows is that policymakers often misunderstand how the confidentiality of data does not generally depend on what country the information is stored in, but rather only on the measures used to store it securely. A secure server in Kenya is no different from a secure server in Brazil. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. For example, in a practice that protects both data privacy and security, some cloud-computing companies have upgraded security controls such that customers retain the keys used to encrypt data before it is uploaded, thereby preventing

third parties or the cloud companies themselves from accessing their data.[51] This highlights what the bill should focus on: ensuring firms that manage Kenyan personal data abide by relevant privacy requirements and use best-in-class cybersecurity measures.

This misguided connection focus on geography also highlights how many policymakers mistakenly conflate the issues of data privacy and security. "Privacy" concerns the collection and use of personal data, while "security" deals with the protection of data from unauthorized access. Some policymakers use forced data localization as an attempt to achieve better privacy or security, as the location of data can affect how organizations respond to lawful government requests for it. But controlling where organizations store data does not impact how organizations collect and use data (privacy)—or how they store and transmit data (security).

Moreover, some policymakers mistakenly believe data localization is the only way to enforce data-handling requirements on foreign organizations. But this is not the case. While any country can demand extraterritorial application of its laws, it may not always be able to enforce them. This is less likely to be a challenge in the case of privacy and security laws for many foreign firms doing business in another country because their local presence places them within the jurisdiction of that foreign country. For example, many businesses have foreign workers (e.g., sales teams) or foreign assets (e.g., real estate, products, or bank accounts) that give foreign countries viable mechanisms for enforcement of failures to abide by civil or criminal laws. Policymakers have leverage over firms doing business virtually because they can block access to domestic markets, such as by prohibiting local advertising.

Rather than adopt the "adequacy" standard used by the European Union, Kenya should adopt a duty-of-care provision to hold the actual companies managing personal data responsible, regardless of where they transfer or store data.

Kenya and other countries in Africa should take a careful and considered approach to enacting their own data protection and privacy regimes and avoid "copying and pasting" the European Union's approach to data privacy and protection and scrutinize each individual privacy provision, including data controller/processor registration, an "adequacy" approach to international data transfers, explicit consent, and the right-to-be-forgotten. Kenya should do this as privacy rules represent key building-block laws that have a considerable impact on a country's digital economy and ability to benefit from digital trade.

Unfortunately, Kenya's draft Data Protection Bill reflects key elements of the European Union's General Data Protection Regulation. For example, the draft bill (section 15) states all data controllers and data processors must register with the data commissioner, with some exceptions. The EU Data Privacy Directive, which was in force between 1995 and 2018, initially included a similar concept that was dropped after it proved unworkable. The broad range of firms such a requirement would cover—especially small and medium-sized enterprises—would prove particularly burdensome. Just as troubling is the bill including the "right to be forgotten," which provides people with the right to the "deletion of false or misleading data about them."

Furthermore, the draft bill adopts the European Union's misguided approach to international data transfers. The bill (part IV, section 22.1.h) requires data controllers or

data processers to ensure personal data is "not transferred outside Kenya, unless there is adequate proof of adequate data protection laws by the recipient country." This "adequacy" requirement mirrors the European Union's flawed approach to data protection in that it tries to make foreign countries responsible for enforcing Kenyan data privacy standards instead of using domestic regulators to hold companies responsible for breaches of Kenyan data privacy laws—regardless of where those companies store the data. A critical flaw in the European Union's approach is the mistaken logic that this country-by-country assessment is effective in promoting better data privacy and protection by companies that manage personal data.[52] This top-down approach is ultimately untenable, as differences in social, cultural, and political values, norms, and institutions are behind countries not regulating privacy the same way. For example, given the country's approach to data protection and privacy, it is inconceivable China would ever be deemed "adequate" from a European perspective.[53]

Rather than adopt the "adequacy" standard used by the European Union and copied by others, Kenya should adopt a duty-of-care provision. When it comes to handling data, companies doing business in a country should be responsible for their own actions and the actions of both their agents and business partners, regardless of where they are located. This could be made clear in law by declaring companies that do business in a country are legally responsible for any failures to protect the personal data of that country's citizens, regardless of whether those failures are the fault of the company in that country, or an affiliate or business partner in another nation. In other words, a country's data protection would travel with the data, regardless of where the data travels. Companies doing business in a given country would then have a strong incentive to assist their business partners outside that country in adhering to its privacy protections, because its citizens and the government could seek remedies for any privacy violations.

This duty-of-care approach to data privacy is shared by most nations, after all. For example, although the United States does not have an "adequacy" standard, companies in the United States need to enact proper data protection measures and safeguards when processing data outside the country, as they remain responsible for the data regardless of where it is processed. U.S. companies mitigate these risks by stipulating requirements in relevant data handling and processing contracts they implement with other companies. For example, Kenyan companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data—even if they move data to Nairobi. And, if a company's affiliate in Nairobi violates HIPAA, then U.S. regulators can bring legal action against the Kenyan company operating in the United States.

Interoperable privacy frameworks are the international extension of a duty-of-care approach such that data is still able to flow between different privacy regimes, and a country's data protection rules flow with it. This reflects a central point policymakers need to recognize when dealing with data privacy: Modern technology, especially the Internet, dictates each country's domestic data protection regimes be global in scope and application. The goal for

interoperability also reflects the fact that there will be no one global privacy regime. It is no surprise that interoperability is part of the goal of the leading data protection initiatives, such as at OECD and Asia-Pacific Economic Cooperation (APEC).

As part of this review, Kenya should identify in advance what metrics it will use to measure the effectiveness of any changes to Kenyan privacy law; base its approach on evidence to ensure laws and regulations are effective; and consider the economic costs of any piece of privacy legislation or enforcement action, as this law will have a major impact on Kenya's ability to develop a dynamic and innovative digital economy. For example, on the issue of measurement, Kenya should consider metrics for the number and size of data breaches, the amount of financial fraud from identity theft, the number of identity theft complaints, greater cross-border data flows, consumer privacy concerns in federal surveys, and many others could all give a clearer picture of the impact of any changes in law. Without a clear, predetermined understanding of what a "winning" privacy framework would look like, a new set of data privacy rules might simply create higher costs and more market uncertainty that reduce innovation and competitiveness.

India reversed course in welcoming foreign investment and operations in its e-commerce sector by introducing rules that specifically target and discriminate against foreign firms.

Kenya should consider the Data Protection Bill alongside its broader effort to develop a dynamic and innovative digital economy. Kenya clearly recognizes the potential for digital technologies to drive innovation and productivity in its Vision 2030, as well as its National ICT Policy.[54] There is enormous potential for Kenya to become a regional leader. Kenya is already home to IBM's first African research lab, Nokia's Africa Headquarters, and Google's first sub-Saharan Africa office (outside of South Africa). Unfortunately, the draft bill only briefly touches on this important connection in recognizing that privacy protections are in part needed "in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a Data Protection policy is critical for Kenya."[55] Creating more restrictive data privacy laws is rather straightforward, but creating such laws to have minimal disruptive effects on users and businesses is much more complex, which is why Kenya should include innovation as an explicit outcome in the bill, and ensure it is used when carefully reconsidering each proposed privacy provision.

India Enacts Regulations That Discriminate Against Foreign E-commerce Firms

On December 26, 2018, India reversed course in welcoming foreign investment and operations into its e-commerce sector by introducing rules that specifically target and discriminate against foreign firms. The Department of Industrial Policy and Promotion (DIPP) of the Ministry of Commerce and Industry Press Note No. 2 makes key changes to the conditions for foreign direct investment (FDI) in its e-commerce sector (particularly DIPP Press Note No. 3 of 2016) that specifically target foreign firms and the business model they have developed to succeed in India's e-commerce sector.[56] On top of this, India enacted the change without consulting stakeholders and with an unrealistically short implementation period (just over a month after the announcement, on February 1, 2019).

Many of the foreign firms affected by this policy (such as Amazon and Walmart) only recently responded to India's decision to allow FDI in its e-commerce sector by pouring

billions in capital into it. At the heart of these positive reforms was the decision to allow FDI of up to 100 percent ownership in entities engaged in the marketplace model of e-commerce (as opposed to an inventory-based model), subject to compliance with certain conditions.[57]

The policy (Press Note No. 2) outlines a number of restrictive changes to the conditions that foreign-owned marketplace models of e-commerce have to meet in order to continue to operate. The policy is discriminatory from the outset in that it does not apply to locally owned e-commerce firms. The new regulations reflect a clear understanding of the business models foreign-owned e-commerce platforms have used to compete, and succeed, in India's e-commerce sector.

The new policy prohibits foreign-owned e-commerce platforms from owning equity stakes in sellers on their platforms. This means Amazon may need to sell its 49 percent equity stake in Cloudtail (the largest seller of goods on Amazon's India platform) and 48 percent equity stake in Appario (another major seller of retail goods). Prior to this, India did not prohibit equity participation by e-commerce platforms in any seller operating on its platform. It is unclear how far this rule will apply in terms of whether it covers both direct and indirect equity participation (such as the subsidiary of an Indian owned and controlled company with a minority foreign ownership).

The new policy also prohibits foreign e-commerce platforms from having "ownership of" or "control over" the inventory of its sellers. If more than 25 percent of a seller's inventory is purchased from its e-commerce platform (or its associated companies), then the platform will be deemed to have control over the inventory sold by that seller. Failing this would mean the platform is acting as an inventory-based e-commerce firm, in which India does not allow foreign ownership or investment. Again, given its investment in some firms who are major sellers on its platform, this potentially impacts Amazon. For example, in 2015, about 40 percent of Cloudtail's growth was driven by categories such as electronics and fashion, two of the largest categories for Amazon India.[58]

The new policy also prohibits exclusivity contracts whereby sellers agree to only sell their goods on the foreign-owned e-commerce platform. This will have a potentially significant impact on foreign-owned e-commerce firms, as it has become an increasingly common method of attracting customers, especially for goods such as smartphones—which account for over half of all e-commerce sales in India. All the major e-commerce players in India, including both Amazon and Flipkart, have exclusivity arrangements with smartphone makers to attract customers, especially for new model launches or in the lead-up to discounting events. For example, Huawei's Honor brand of smartphone and Motorola's Moto G have signed strategic partnerships with Flipkart. In 2018 alone, Amazon and Flipkart signed over 100 exclusivity arrangements with smartphone makers.[59] Such exclusivity arrangements are a major marketing tool, as competition between the platforms is fierce. In effect, this change gives local e-commerce platforms an unfair competitive advantage (as this rule does not apply to them).

India's new policy also prohibits foreign-owned e-commerce platforms from offering the discounts and cashback offers that are a key feature of their business model. For example, offering customers anywhere from 5 to 20 percent cash back whenever they pay with a particular debit card, e-wallet, or online payment service. And e-commerce entities are prohibited from having a direct or indirect influence on the sale price of goods or services on its platform—and the platform should only have an "arm's length" relationship with sellers.

The policy's prohibition of several common business practices e-commerce platforms (as well as brick-and-mortar retailers) have used to compete in India makes it hard to conclude anything other than Indian policymakers would prefer to maintain an inefficient retail market, which results in consumers paying more for goods and services. Kiranas, which are effectively "mom and pop" corner stores, still control close to 90 percent of the country's more than $700 billion retail market.[60] Foreign retailors have a checkered history competing in India (with several firms entering and exiting the market). Furthermore, online retail accounts for only an estimated 2 percent of India's retail market.[61] However, despite all this, foreign e-commerce firms obviously see the opportunity to commit the capital and know-how to enter and compete in India.

No doubt a part of foreign firms' decision to enter India is the enormous potential for growth in e-commerce, as the number of Internet users in India reached an estimated 500 million in June 2018.[62] By targeting foreign investment in India's e-commerce sector, the new policy threatens a significant bright spot in India's economy. In October and November 2018, online retailers in India sold goods worth $4.3 billion—a 43 percent increase from the previous year. This includes around $2 billion worth of goods sold in discount/sale events hosted during this period by Flipkart ("Big Billions Day"), Amazon ("Great Indian Shopping Festival"), Paytm Mall ("Maha Cashback Sale"), and Snapdeal ("Mega Diwali Sale").[63] This growth reflects changing consumer preferences regarding the prices of goods and services offered by online retailers compared with traditional brick-and-mortar retailers—and shows there is obviously a role for foreign firms to play in India's changing retail market. However, it seems this success has provoked a response from some Indian policymakers who would prefer foreign firms did not disrupt things too much (by improving consumer welfare and making the retail sector more efficient) or that this opportunity be reserved for local e-commerce firms.

India is also shooting itself in the foot by discouraging foreign investment in the very sector that had boosted India's otherwise lackluster levels of (much-needed) foreign investment. After only launching in India in 2013, Amazon has announced a series investments in local operations totaling nearly $5 billion. Following this, in August 2018, Walmart announced it had paid $16 billion to acquire 77 percent of Flipkart, along with $2 billion in new equity funding to help grow the business.[64] This foreign investment allowed India, for the first time in years, to beat its strategic competitor China in terms of FDI received—in 2018, India received $39.5 billion in foreign merger and acquisition investment, compared with China 's $33 billion.[65]

India's lead may be short-lived given the significant political risk foreign firms face in India, with short-term political interests apparently having played a role in the lack of warning and industry engagement about this poorly thought-through policy. It seems the recent losses in state-level elections by members of Prime Minister Modi's ruling coalition led to this policy change in an attempt to appeal to parts of its base (such as local traders) in the lead-up to federal elections later in 2019. The new policy also shows some Indian policymakers remain wedded to protectionism and state intervention in the economy. In this case, to protect brick-and-mortar retailers who are unable to compete with foreign e-commerce platforms and to favor the emergence of locally owned e-commerce platforms (given large Indian conglomerates have reportedly taken an interest in entering or expanding operations in the sector given the success of foreign-owned e-commerce platforms).

India Enacts Data Localization for Payments Data

The Reserve Bank of India enacted unnecessary, trade-distorting, and discriminatory data localization requirements for payments data.

On April 5, 2018, the Reserve Bank of India (RBI) enacted unnecessary, trade-distorting, and discriminatory data localization requirements for payment data. The brief RBI notice announcing the policy stated, "It is observed that at present only certain payment system operators and their outsourcing partners store the payment system data either partly or completely in the country. In order to have unfettered access to all payment data for supervisory purposes, it has been decided that all payment system operators will ensure that data related to payment systems operated by them are stored only inside the country within a period of 6 months."[66] The data should include the full end-to-end transaction details, and information collected, carried, and processed as part of the message or payment instructions. The RBI set a short deadline for implementation (October 15, 2018), before which it asked companies to provide updates every two weeks. Despite various stakeholders (including the Payments Council of India and the U.S.-India Business Council) criticizing the measure as unnecessary and onerous—and the implementation period being far too short to reconfigure complex IT systems—the RBI persisted and asked for immediate compliance.

The RBI's notional reasons for data localization were concerns over regulatory oversight and cybersecurity, as the bank cited the need for "continuous monitoring and surveillance" of payment data in order to reduce the risk of data breaches by ensuring payment services use the best global cybersecurity standards.[67] At the heart of this regulation's focus on geography is the mistaken belief that data must be stored domestically in order for it to remain secure, private, and accessible to government.

Despite its claims, the RBI has provided no evidence of having faced regulatory issues around access to data—when it should be publishing every instance and pursuing such legal remedies as revoking offending firms' operating license or imposing fines. If access is a legitimate issue, the starting point should be an analysis of the legal framework whereby payment firms provide the RBI with timely access for regulatory oversight. Any legal remedies the RBI considers insufficient should be addressed via policy revisions. Also, rather than the geography of data storage, what should matter is how firms and their cloud

suppliers manage their IT and data-management systems, particularly when it comes to providing the RBI with access to data in a timely manner. Firms can readily use the convenience of modern information technologies (such as cloud computing) to facilitate such access with the simple click of a button. Where the data is stored is irrelevant in this scenario. Likewise, firms failing to provide the RBI with access to data because of privacy rules or other countries themselves enacting some form of data localization—thereby creating a "catch 22" for companies caught in the middle—also deserves to be highlighted, as that will be of broader interest to policymakers and other financial regulatory agencies.

As part of this, the RBI should focus solely on the provisions that provide the legal framework so that the RBI has sufficient confidence financial firms are properly managing their data and if need be can provide data on demand. The EC's efforts are a useful reference point for the Central Bank on this issue around access to data. As part of efforts to build a digital single market, the EC is working to remove barriers to the transfer of company, tax, bookkeeping, and financial data, and asking that member states focus on mandating access.[68] For example, in 2015, Denmark changed its local data storage requirement for accounting data such that companies could store their data anywhere, as long as Danish authorities were given easy access to it on request.[69] This is where the focus should be: putting in place the legal framework to ensure companies provide data to regulatory authorities in a timely manner.

If the RBI is worried that firms will avoid regulatory oversight by simply shifting data overseas, this is similarly mistaken. Financial firms doing business in India need to be approved by the RBI, which means they must have "legal nexus" in India in order to be put under the RBI's jurisdiction. As such, firms must comply with whatever rules the RBI has on data, regardless of whether it stores the data in the host country, the home country of the foreign firm, or even a third country. In this way, just as consumer safety and other laws apply to tangible goods that flow in and out of a country as part of international trade, cybersecurity and other rules apply to data and the financial firms that move and store data in another nation.

It is understandable that regulators are concerned about the cybersecurity measures in place at financial firms, but the focus on data localization is mistaken. As noted in the Kenya case, in regard to security, while certain laws may impose minimum security standards, the security of data does not generally depend on where it is stored, but rather only on the measures used to store it securely. As ITIF wrote in "The False Promise of Data Nationalism," data localization mandates do not increase commercial privacy or data security.[70] What matters are the technological and procedural methods of storing and transferring data when determining how safe data is, not the geographical location where the data is stored.[71] Data breaches are the result of security failures, not the location of the data. This highlights the central point that should guide the Central Bank's efforts to improve cybersecurity: What is of critical importance is the financial firm and its cloud storage service (i.e., a company with its own network or a third-party cloud provider) be dedicated to implementing the most advanced methods of preventing such attacks.

This data localization requirement will impose economic costs and negatively impact the ability of Indian firms to use data to provide innovative new services. Maximizing the value of data requires the ability to move it. Innovation and economic growth are increasingly driven by how firms collect, transfer, analyze, and act on data. Absent policy-created "data protectionism," digital trade and cross-border data flows are expected to continue to grow much faster than the overall rate of global trade. Cutting off cross-border data flows would undermine the innovative technologies that are central to the financial sector's competitive position. The benefits the financial services sector derives from cloud computing, big data analytics, and other innovative technologies at the heart of the data economy are only fully realized when there is ready access to large volumes of information, such as anonymized customer purchase data.

The RBI's data localization policy is a good example of digital protectionism because there are effective and readily available alternatives that address the underlying public policy issues. The RBI persisting with the policy despite this point being made it to by foreign firms and trading partners reveals a preference for protectionism. Further evidence is the RBI having given firms only six months (which ended in October) to comply, which itself is unfair given the complexity and cost involved in firms negotiating new service contracts with local cloud computing providers and having to rearrange global IT and data management systems in order to see whether and how data analytics and cybersecurity services geared for global systems can work on a brand new local IT system.

Indonesia is undermining the long-agreed WTO moratorium on enacting duties on data transmissions in trying to put in place tariffs on digital imports. Such a policy would open a major new avenue in digital protectionism.

Indonesia Moves to Enact Tariffs on Imports on Digital Goods

On February 15, 2018, the Indonesian government issued Regulation No. 17/PMK.010/2018, which added a new chapter on digital goods to its tariff schedule to allow it to enact tariffs on imports of digital goods, such as downloadable music, e-books, and software.[72] Indonesia cited the change as necessary to create "a level playing field" between online and offline sellers, and to raise tax revenue.[73]

While the current schedule sets these tariffs at zero (as it tries to figure out how to administer tariffs), enacting tariffs on digital imports would be a clear escalation of Indonesia's pursuit of digital protectionism.[74] Indonesia is the only country in the world that has added digital goods to its tariff schedule, with the new Chapter 99 of Indonesia's tariff schedule covering intangible goods that were previously not covered. Under Article 1 of Regulation 17, Chapter 99 (Software and Other Digital Goods) consists of:

Chapter Notes:

1. Software and other digital goods transmitted electronically referred to in heading 99.01 are those that are not related to machines or devices that have been or will be imported.
2. Software and other digital goods transmitted electronically related to machines or devices that have been or will be imported are classified with such machines or devices.

Subheading Notes

1. Tariff line 9901.40.00 covers only software that is a renewal or update of said software for machines or devices that have already been imported.

No	HS Code	Description of Goods	Import Duty
	99.01	Software and other digital products transmitted electronically	
10287	9901.10.00	Operating system software	0%
10828	9901.20.00	Application software	0%
10829	9901.30.00	Multimedia (audio, video, or audiovisual)	0%
10830	9901.40.00	Supporting or driver data, including design for machinery systems	0%
10831	9901.90.00	Other software and digital products	0%

Indonesia's efforts to enact this form of digital protectionism raise a number of issues. For one, the law raises questions about the lack of clarity in terms of what is a good versus a service in the digital era (although the WTO's GATS is theoretically applicable to measures restricting cross-border data flows). In 2014, Indonesia enacted a new trade law that defines goods and service imports as, "Goods: any object, whether tangible or intangible, moveable or immovable, that either can be spent or cannot be spent, that can be traded, used or utilized by consumers or business communities; and Imports: activities of bringing Goods into the Indonesian customs area."[75] Hence, Indonesia has taken this one step further in trying to actually apply tariff duties on imports of digital "goods," even though the last description for "other software and digital products" is a vague catchall category that could mean anything.

Indonesia is running into the practical issue of whether it is even feasible for countries to enact duties on digital imports. It is evident that Indonesia enacted this policy without much thought as to how or whether it is technically feasible to do so in terms of how Indonesian customs authorities expect to run and supervise the declaration process for firms that are "importing" these digital "goods" given they do not come through a physical entry point. In meetings with stakeholders, Indonesian authorities have reportedly struggled to understand both how modern firms involved in digital trade operate and that there are different business models involved (e.g., software-as-a-service versus direct digital downloads of products versus market places for apps). Indonesian authorities are reportedly considering several potential mechanisms to implement tariffs, such as relying on a voluntary declaration by major firms and intermediaries; relying on marketplaces or payment services (such as credit card companies) to be duty collectors; some form of direct carrier billing; or relying solely on payment services to identify and collect duties.

In this way, Indonesia is ascertaining whether it is feasible for it to at least indirectly levy duties on imports of digital products by using legal and enforcement tools to coerce major firms involved in digital product distribution to (voluntarily, but reluctantly) provide internal company data about their imports as a means of extracting duties on digital imports. Such a system, which relies on either key firms voluntarily providing data or key intermediaries identifying and extracting duties, would likely be selective and potentially discriminatory given it would mainly target major foreign tech firms over small and medium-sized local firms. Furthermore, it would be difficult for Indonesia to audit firms to "inspect" for digital imports—unlike with physical goods, they cannot simply open and inspect a shipping container. Enforcement raises other issues, such as Indonesia potentially resorting to blocking data flows or access to websites from targeted firms (as it did to Netflix in relation to concerns over content and market-entry restrictions), or targeting key intermediaries involved in digital product imports (e.g., asking payment services to stop processing payments for targeted firms).

Indonesia's efforts to enact tariffs on digital goods threatens—and potentially contravenes—the long-standing moratorium among WTO members not to enact duties on the data transmissions that constitute e-commerce. The moratorium was first agreed to in 1998 and has been renewed on a rolling two-year basis, most recently at the end of 2017 (which included Indonesia). At the time it was drafted, putting customs duties on electronic transmissions was not technologically possible. Indonesia may find that it still is not, at least not in any comprehensive manner (as compared with customs authorities inspecting and collecting duties on imports of physical goods).

"Electronic commerce" is generally understood to mean the production, distribution, marketing, sale, or delivery of goods and services by electronic means.[76] In 1998, digital products such as software and e-books were in their infancy, so the moratorium was a rather commendable—and successful—prediction of the digital future of trade and a statement of faith about the need to preemptively protect e-commerce and digital trade from traditional barriers to trade. However, the WTO always knew that digital products would increasingly substitute for their physical analogues.[77]

Indonesia takes a distorted view of the WTO moratorium in thinking that it does not apply to digital content, but rather only to the data transmissions that distribute them.[78] While the Internet and the concept of modern digital trade were very different when the WTO moratorium was initially enacted, even at that early stage the distinction between taxing content and the underlying data transmissions was ambiguous, if not considered the same. At a minimum, this policy reflects an effort by Indonesia to circumvent the spirit of the commitment, if not the legality of it.

Enacting duties on digital goods is bad for many reasons, not least of which is by raising the price of information communication technologies (ICTs) they are undermining a central driver of productivity growth in modern economies. ICT is a key driver of productivity because it is what economists call a "general purpose technology" (GPT).

GPTs have historically appeared at a rate of once every half century, and represent systems of fundamentally new technologies that change virtually everything, including what economies produce; how they produce it; how production is organized and managed; the location of productive activity; the skills required for productive activity; the infrastructure needed to enable and support production; and the laws and regulations needed to maintain or even allow it.[79] In a conclusive review of over 50 scholarly studies on ICT and productivity published between 1987 and 2002, Dedrick, Gurbaxani, and Kraemer found that "the productivity paradox as first formulated has been effectively refuted. At both the firm and the country level, greater investment in ICT is associated with greater productivity growth."[80] In fact, nearly all scholarly studies from the mid-1990s have found positive and significant effects of ICT on productivity.[81] The beneficial effects of ICT on productivity have been found across different levels and sectors of economies, from firms to industries to entire economies, and in both goods- and services-producing industries.[82]

If Indonesia is allowed to do this, it will likely open the floodgates as other countries follow in a misguided effort to chase a new source of tax revenue.

Unfortunately, Indonesia is correct in asserting the moratorium is not a "covered agreement" and therefore will not be subject to dispute settlement if it does proceed.[83] However, this does not mean there are no potential trade responses. Digital tariffs would make it (even more) difficult for Indonesia to join the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), or potentially, the WTO e-commerce subgroup (if it moves to, and completes, negotiations, given the moratorium is likely to be a part of negotiations). Major trading partners, especially the United States, could withdraw the substantial benefits Indonesia enjoys under its Generalized System of Preferences, which was worth nearly $2 billion in 2017 (9.6 percent of Indonesia's total trade with the United States).[84] Longer term, if Indonesia's actions lead to the dissolving of the moratorium, it potentially opens itself up to a broad range of WTO disputes over so-called "TRIPS non-violation complaints" (as the moratorium on these cases is politically linked to the e-commerce moratorium), which would be a major issue for Indonesia, given its many intellectual property issues.

Fearing the same scenario that is unfolding in Indonesia, several countries have used bilateral and regional trade negotiations to enact a permanent, clearer, stronger, and enforceable moratorium, such as in the CPTPP and the U.S.-Mexico-Canada Trade Agreement (USMCA). The CPTPP includes a provision on customs duties in the e-commerce chapter that states, "No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party." It also includes a definition for digital products: "[D]igital product means a computer programme, text, video, image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically."[85] Meanwhile, the USMCA goes even further in elaborating on the moratorium: "No Party shall impose customs duties, fees, or other charges on or in connection with the importation or exportation of digital products transmitted electronically, between a person of one Party and a person of another Party." The same goes for its definition of digital goods: "[D]igital product means a computer

program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically. For greater certainty, digital product does not include a digitized representation of a financial instrument, including money."

The potential ramifications of Indonesia's efforts are significant. As we have seen with other regulatory issues involving the digital economy, such as restrictions on over-the-top services, data localization, and digital taxation, once one country provides a model, many others will follow. This is especially true when the policy provides a new source of revenue for a government. While Indonesia is the only country to have added electronic transmissions to its tariff schedule, it will not be alone for long. If it perseveres and enacts a collection system—even a highly flawed one that only targets large, well-known foreign firms—it will send a signal to protectionists in other developing countries that there is (at least some) revenue to be raised in levying digital tariffs.

Italy is joining France and others in enacting new legislation that seeks to protect cinemas from Internet-based streaming services. It is a classic case of incumbents seeking government protection from tech disruption.

Indonesia's new regulation reflects the growing appeal of digital protectionism. India, South Africa, and a broader group of Africa countries have expressed interest in enacting tariffs on digital imports.[86] These countries are likely attracted to the strategy laid out in a a recent United Nations Conference for Trade and Development (UNCTAD) report, which claims that the moratorium removes "policy space" for developing countries to enact digital industrial strategies that seek to replicate tried-and-failed state-directed protectionist strategies, such as import-substitution.[87] While the moratorium had always been renewed without much debate in the past, these countries made a bigger effort to oppose it during the last renewal as they were reluctant to sign away their ability to impose tariffs on digital products (even though they eventually did). Some CPTPP members were also reluctant to include moratorium language for this same reason (even though they also eventually did). Indonesia's policy, if left unchallenged, could potentially expose the global digital economy to a major new trade barrier.

Italy Enacts Rules to Protect Cinemas and Discriminate Against Video-on-Demand Services

In October 2018, Italy enacted legislation that seeks to protect cinemas from Internet-based streaming services by forcing the latter to wait 105 days after a film's theatrical screening before being permitted to stream the film.[88] This attempt to protect Italian cinema operators and film distributors mirrors other tech-disrupted sectors wherein incumbent firms struggle to adapt to new digital competitors by calling for government protection.

Italian cinema and film groups recently cited two recent issues—film festivals accepting nominations from Netflix, and same-day cinema and streaming movie releases—as reasons behind calling for new rules that will disadvantage Netflix. These groups opposed Netflix's efforts to enter six movies for consideration at the prestigious Venice Film Festival, which follows the Cannes Film Festival's refusal to accept nominations from Netflix (also in 2018). Italy's two largest exhibition trade bodies, ANEC (Associazione Nazionale Esercenti

Cinema) and ANEM (Associazione Nazionale Esercenti Multiplex) criticized the film festival's embrace of Netflix. These groups were also angry that the Italian police-brutality drama, *On My Skin* played in several Italian cinemas (via local Italian distributor Lucky Red) on the same day it was distributed globally on Netflix—which was also only a short time after its festival debut.

These Italian film and cinema groups called for new rules to disadvantage this day-and-date streaming (without explicitly naming Netflix), which they say only helps the "short-term interests of one party, to the detriment of others."[89] In their view, the Venice Film Festival is condoning a weakening of the "value chain" in the local film and cinema market: "This is a very sensitive issue that should be dealt with in agreement with all the operators of the film supply chain, especially in a period of serious crisis for exhibition due to structural problems of the market." They went on to say they will "oppose this proposal [day-and-date releasing of big movies] by any means necessary if the issue of shortening windows is disregarded without the approval of Italian Cinema."[90]

These incumbents appealed for government protection as Netflix is disrupting their reliance on traditional cinemas. The battle over Netflix's role in the Venice Film Festival comes as Italian box office revenues decreased 5 percent to $631 million in 2018—the worst result in a decade—on the back of weaker Hollywood blockbusters. Furthermore, Italian ticket sales dropped to around 86 million in 2017 and 2018, the first time in a decade the number of tickets sold was below 100 million.[91]

The new Italian law is indicative of a broader trend in Europe and around the world whereby traditional film distributors and cinemas are seeking protection from new streaming services. HDF Kino (Germany's largest cinema association) says it agrees with their Italian counterparts in criticizing Netflix's presence at the Venice Film Festival and that it would not welcome Netflix films at the Berlin Film Festival, which already does not allow Netflix films in its main competition category. The Amazon-backed *Don't Worry, He Won't Get Far On Foot* film played in the Berlin Film Festival's main competition this year, but only due to the fact it was also released in local cinemas. Meanwhile, the European exhibition body UNIC (which represents cinema associations across 37 territories) supports Netflix's exclusion, "The cinema industry can exist alongside streaming providers, but believes that their—and the audience's—best interests are served by a film receiving a proper cinema release, including a clear and distinct window. Films belong on the big screen…"[92] Likewise, Cinepolis (Mexico's biggest theater chain) announced it would not be showing Mexican director Alfonso Cuarón's *Roma* because it requires films to have a 90-day theatrical window before becoming available on streaming services. Cinepolis hoped Netflix might push *Roma*'s streaming launch from December 2018 to February 2019 so that it could release the film in cinemas, but that request did not pan out. Showing the changing dynamics in the market, Netflix decided to launch *Roma* globally via streaming on December 14, 2018.[93]

Thankfully, in the case of Italy, some local film producers and distributors recognize the need to adjust to new technology and changing consumer preferences, and the futility in fighting these trends. Lucky Red (the Italian film distribution company that worked with Netflix to bring the movie *On My Skin* to cinemas) defended the day-and-date plans for the movie, saying the release plan represents a "big opportunity" for audiences (i.e., gives consumers choices). It stated, "This is not an imposition. It's a choice."[94] Likewise, the CEO of Cattleya (Italy's leading independent film and television producer), Riccardo Tozzi, told journalists that "I have no problem with Netflix being at Venice—we are in a different age" and that "it's unthinkable that we could keep the same distribution mechanisms as decades ago. Audiences consume movies in different ways today and we need to have different releases for different movies."[95] Indicative of the futility in fighting the changing nature of movie and TV production is the fact that Netflix will spend $12–13 billion on content in 2018—more than any Hollywood studio spends on films or TV networks spend on sports licensing. In 2018, Netflix will produce 82 feature films in a when Warner Brothers (the biggest movie producer in Hollywood) will only produce 23 films for cinema release.[96]

Unfortunately, Italy looked to France as a model in forcing streaming services to wait until three years after they debut in theaters before being permitted to make available titles for streaming. France considered changing its law in favor of local streaming services and content by shortening this window to 15 months (or 13 months for movies that prove unpopular) for traditional French services like CanalPlay and FilmoTV (which negotiate agreements with the government to invest in French content via a tax on production). In contrast, foreign streaming services that do not pay this local production tax must still wait three years. Even with this differential treatment, Netflix recently decided not to start paying this tax.[97] However, indicative of the restrictiveness of this model, CanalPlay has been lobbying the French government to reduce this window to help it compete with foreign streaming services.[98]

These changes in Italy, France, and Germany are reflective of a broader set of concerning changes in the European Union's regulatory framework for streaming services. Germany and others are considering a levy on foreign video on-demand services to fund local content production, while the EC considers a region-wide quota of 30 percent local material for on-demand service providers.[99] Instead of local content requirements and taxes, countries should step back and look at the framework to encourage streaming services to produce more locally and to use platforms to distribute this work globally. Netflix' chief content officer announced that it expected to release more than 100 new original projects out of Europe, the Middle East, and Africa in 2018.[100] Netflix is increasingly known for strong local-language TV series such as *Dark* in Germany and *Suburra* in Italy. In 2018, Netflix announced a range of new Italian-language content, including Italian original films, TV series, and a docuseries about Italian Serie A football team Juventis. Furthermore, in October 2018, Netflix CEO Reed Hasting announced plans for a French production hub, which would be its fourth in Europe, alongside London, Amsterdam, and Madrid.[101] This

raises an important question for policymakers in Italy as to why these streaming services have not setup a production hub in Italy and what policies need to change to possibly rectify this.

Saudi Arabia Introduces Data Localization as Part of Cloud Computing Regulatory Framework

In 2018, Saudi Arabia issued its cloud computing regulatory framework, which includes data localization requirements for various categories of data.[102] The framework entered into force 30 days from its publication on February 6, 2018, and thus came into effect on March 8, 2018.

Saudi Arabia enacted a cloud computing framework that runs directly counter to the distributed nature (and benefits) of the technology by requiring local data storage.

Local data storage is applied to certain categories of data. The framework categorizes data according to four levels. Level 1 and 2 involve a range of sensitive and non-sensitive customer data and data from private firms that are not subject to sector-specific restrictions. Level 3 involves data from private-sector-regulated industries (it is unclear what these are), sensitive data from public authorities (it is unclear how this is different from level 4), and lower categories of data if clients request a higher level of protection (i.e., treating level 1 and 2 data as level 3). Level 4 is data that is highly sensitive and related to the government. The framework (section 3.3.8) states that no level 3 data may be transferred outside of Saudi Arabia, for whatever purpose and in whatever format, whether permanently or temporarily (e.g., for caching, redundancy, or similar purposes), unless expressly allowed by the government. Furthermore, the framework (section 3.3.9) states that cloud providers are not allowed to transfer, store, or process level 3 data in any public, community, or hybrid cloud unless registered with local authorities. Cloud providers must also register and disclose where their data centers are in Saudi Arabia, and the countries where they have data centers process, store, transit, or transfer data from Saudi Arabia. Furthermore, the framework enacts barriers to the sharing of data between countries as part of law enforcement, financial oversight, and other areas of potential cooperation.

Saudi Arabia's Communications and Information Technology Commission is right in recognizing that the ICT sector is undergoing rapid change, and encouraging firms to adopt and use cloud computing is central to this—but it is wrong in believing data localization will help do this (as it claims).[103] Policymakers—such as those in Saudi Arabia—who subscribe to digital protectionism believe that if they restrict data flows, their countries will gain a net economic advantage from companies that will be forced to relocate data-related jobs to their nations.[104] These supposed benefits of data-localization policies are misunderstood. Data centers have become more automated, meaning the number of jobs associated with each facility—especially for technical staff—has decreased. While data centers do contain expensive hardware (which is usually imported) and create some temporary construction jobs, they employ relatively few full-time staff.[105] For example, in 2011, a $1 billion data center built by Apple in North Carolina created only 50 full-time jobs and another 250 support jobs in areas such as security and maintenance. Similarly, a new Microsoft data center in Virginia was expected to create at most only several dozen permanent jobs.

As ITIF argues in "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" data localization affects the development and use of cloud computing in an economy as it affects the price and availability of all IT services.[106] At the firm level, barriers to data flows make firms less competitive, as they are forced to spend more than necessary on local IT services that are also likely to be less reliable and useful than foreign providers. Such barriers also prevent Saudi Arabian companies that operate internationally from transferring data needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative IT services. Likewise, companies may be compelled to spend more on compliance activities, such as hiring data-protection officers or putting in place software and systems to get individuals' or the government's approval to transfer data. These additional costs are borne by either customers or the firms themselves, which undermines their competitiveness (especially foreign firms that are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins. This economic impact ripples throughout an economy as barriers to data flows affect data processing and Internet services—or any services that depend on the use of data for delivery, which in today's economy is most of them.

Turkey enacted new rules that force publicly traded firms to store data locally as part of a misguided oversight measure that not only disadvantages foreign tech services, but hampers the ability of Turkey's leading firms to compete globally by preventing them from using the lowest-cost and best-in-class IT services.

Turkey Introduces Data Localization for Publicly Listed Firms

On January 5, 2018, Turkey's Capital Markets Board (CMB) enacted new rules (the Communiqué on the Management of the Information Systems (VII-128.9)) for how publicly traded firms should manage their IT systems—which included data localization—in requiring primary and secondary IT systems only be in Turkey.[107] As in other cases, the regulatory authorities have provided no justification for this requirement, such as evidence firms had not been providing timely access to data for prudential oversight.

The rules cover Turkey's leading firms and all their IT systems. CMB defines the primary IT system as "the complete system comprising of [sic] the infrastructure, hardware, software, and data … required for the institutions, establishments, and associations to perform obligations stated under the legislation, if and when required, and enabling the access to such information in a secure manner."[108] The secondary IT system is essentially the backup to ensure firms have uninterrupted access to information. The regulations cover a broad range of firms and organizations, including all publicly traded companies, the Istanbul Stock Exchange; organized markets; pension funds; the Istanbul Clearing, Settlement and Custody Bank; the Central Securities Depository of Turkey; custodians; the Capital Markets Licensing Agency; capital markets institutions; the Turkish Capital Markets Association; and the Turkish Appraisers Association. The data localization requirement is part of a broader CMB revision in setting the rules, policies, and procedures regarding the management, security, sustainability, and efficiency of firms' IT operations. It also includes rules regarding the independent audit of firms' IT systems (Communiqué III-62.2). This includes periodic internal and external audits of IT and data management systems.

Turkish companies that have regional or global operations likely need to spend additional time and money reconfiguring IT systems that may potentially use global IT services. This

data localization requirement disadvantages these companies, and those that aim to expand internationally, as it likely forces them to spend more using local IT service providers—that may not be as cost competitive or have the most cutting-edge cybersecurity, data analytics, and other services. Furthermore, forcing these firms to use local data centers affects the broader economy as these cost and service impacts flow through to their clients, which detracts from economic productivity.

While this impact may be hard to quantify and identify, it will inevitably affect these firms, even if CMB only enforces this data localization requirement over time. On March 8, 2018, CMB released clarifying guidance that the IT systems of publicly held companies not currently subject to independent audit are not required to keep their primary IT systems in Turkey. CMB plans to gradually expand the number of publicly held companies subject to independent auditing, after which they will be obliged to keep their primary IT systems in Turkey.[109]

Turkey's focus should be on the framework for auditing how firms manage their IT and data, and provide data to regulators as part of oversight duties—not the location of the data storage.

Unfortunately, CMB's new data localization requirement is simply the latest to target payment and financial data. In 2013, Turkey enacted a law—the Law on Payments and Security Settlement Systems, Payment Services and Electronic Money Institutions—that forces Internet-based payment services, such as PayPal, to store all data in Turkey for 10 years. PayPal withdrew from the country after refusing to abide by this data localization requirement.[110]

It is understandable that CMB would want to improve its legal framework for ensuring publicly traded firms and those involved in capital markets are checking, testing, and improving their IT systems. However, at the heart of the proposal's focus on geography is the mistaken belief that data must be stored domestically to ensure it remains secure, private, and accessible to government. As already covered in the Kenyan and Indian cases, this is false.

CMB is mistaken if it is concerned that firms will avoid regulatory oversight by simply shifting data overseas. Financial firms under its jurisdiction would need to be approved by CMB and other regulatory authorities, meaning the firms would be required to have "legal nexus" in Turkey. As such, the firm must comply with whatever rules CMB has on data regardless of whether it stores the data in the host country, the home country of the foreign company, or even a third country.

The United States' experience with this same issue should be instructive for CMB. The U.S. Treasury and financial regulators recently reconsidered a policy that would have allowed data localization for financial data, but instead enacted a policy framework that focuses on maintaining access to data. U.S. regulators' concerns were based on their experiences in the global financial crisis when they had issues getting access to data in key banks' (i.e., Lehman Brothers') IT systems during bankruptcy proceedings. The U.S. Federal Reserve and Federal Deposit Insurance Corporation's (FDIC) ability to use and analyze Lehman's IT system and data was reportedly hindered as the bank's network became fragmented, overseas subsidiaries were sold off, some IT systems in overseas

subsidiaries were turned off, some key IT staff departed, and restrictions on data flows were imposed due to insolvency filings in other countries—as was the case when the United Kingdom's financial regulator took over Lehman Brothers' European division.[111] This made it difficult for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom.[112]

However, subsequent legal reforms (e.g., Dodd-Frank Act, enacted in 2010) have addressed these concerns by focusing on how companies disclose to regulators the way they manage their IT and data as part of regular prudential compliance activities. This means that, in the event of a crisis, regulators know the company will be able to provide the data they will want. The law outlined extensive new rules that require "systemically important financial institutions" (SIFIs) to prepare "resolution plans"—also known as "living wills"—that specify a company's strategy for "rapid and orderly resolution in the event of material financial distress or failure of the company."[113] U.S. living wills achieve this by requiring firms to meet stringent requirements about how their IT systems are organized and how data is stored, accessed, and managed on an ongoing basis (as part of periodic compliance activities) in the event of a crisis.[114]

Turkey should look to emulate the U.S. review process whereby regulators check IT plans and provide advice to individual firms about how to improve the way they manage and report on their IT and data management systems. If the independent audits identify issues about how firms are organizing and reporting their IT and data systems, CMB could then issue additional sector-wide advice for all firms. The focus should be on this framework and process, not the location of data storage.

CONCLUSION

Looking back over this and past years' reports shows several trends. It is troubling that a growing range of countries are following the early adopters of innovation mercantilism and digital protectionism—especially the world leader, China. China and these other countries are also extending these discriminatory and trade distorting rules to new categories of data, digital services, and forms of behind-the-border regulation. As this trend evolves, it is possible to give policymakers in certain countries the benefit of the doubt in that they may have inadvertently considered or enacted policies that discriminate against foreign technology firms and their goods and services. However, in the majority of cases, policymakers make the flimsiest of cases—if they make a case at all—in trying to justify their mercantilist approach, without any serious effort to weigh up the effect of their approach or whether there are other non-trade-distorting alternatives that address the underlying public policy objective. This represents a dangerous and growing threat to the potential for a rules-based, open, and innovative global economy.

While mercantilist barriers grew in 2018, there were also some positive counter-developments. The United States, European Union (and its member states), Japan, and others are beginning to realize (to varying degrees) they need to individually and collectively respond to Chinese innovation mercantilism. The collective response is the key

to long-term, sustainable success in getting China to change its trade and economic policy, as no single country has the leverage to achieve meaningful change. Some steps have already been taken, such as new measures that target predatory, state-subsidized, non-market-driven foreign investment and technology acquisition by Chinese firms. The United States also initiated several cases involving the theft of trade secrets from high-tech U.S. firms. Multilaterally, it will require more cases before the WTO—as well as wide ranging reforms at the WTO—the debate on which is only just starting.

Positive developments on protecting and supporting data flows and digital trade include the CPTPP coming into effect among its 11-member countries. Its e-commerce provisions protecting data flows, source code, and other digital issues sets the high-water mark in terms of new global rules. In a first, Brazil committed to CPTPP-like e-commerce provisions in its trade agreement with Chile. The USMCA builds on the CPTPP with even stronger digital trade rules, but still needs to be enacted. Finally, a subgroup of WTO members launched a much-needed effort toward discussing (and eventually, negotiating) digital trade and e-commerce issues. Whether these countries can avoid the same stalemate over data flows (the onus is on the European Union to break the potential for deadlock) that doomed the Trade in Services Agreement remains to be seen. If countries can get past it, the agreement would go a long way toward putting in place a new global norm for protecting data flows in the digital economy.

ENDNOTES

1. Executive Office of the President National Science and Technology Council Advanced Manufacturing National Program Office, "National Network for Manufacturing Innovation Program: Annual Report" (Executive Office of the President, February 2016), https://www.manufacturing.gov/files/2016/02/2015-NNMI-Annual-Report.pdf.
2. Robert Atkinson, "Designing a Global Trading System to Maximize Innovation," Global Policy Journal 5, no. 1 (February 2014): 57–62.
3. For a review of studies, see Michelle A. Wein and Stephen J. Ezell, "How to Craft an Innovation Maximizing T-TIP Agreement" (Information Technology and Innovation Foundation, October 2013), http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf.
4. Stephen J. Ezell, Robert D. Atkinson, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy" (Information Technology and Innovation Foundation, September 2013), https://itif.org/publications/2013/09/25/localization-barriers-trade-threat-global-innovation-economy.
5. Office of the United States Trade Representative (USTR), "2018 National Trade Estimate Report on Foreign Trade Barriers" (Washington D.C.: USTR, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.
6. As defined in International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Guide. https://www.iso.org/obp/ui/#iso:std:iso-iec:guide:2:ed-8:v1:en.
7. National Research Council, *Standards, conformity assessment, and trade: into the 21st century*, (Washington D.C.: National Research Council of the National Academies of Science, 1995), https://www.nap.edu/read/4921/chapter/6#105.
8. Stanley Besen and Leland Johnson, "Compatibility standards, competition, and innovation in the broadcasting industry" (Rand Corporation, 1986), https://www.rand.org/pubs/reports/R3453.html.
9. Donald E. Purcell, "Strategic Standardization Overview" (presentation, Catholic University School of Engineering, Washington, D.C., May 18, 2011).
10. G. M. Peter Swann, *International Standards and Trade: A Review of the Empirical Literature* (Paris: Organization for Economic Cooperation and Development Working Papers, No. 97, June 2, 2010), https://www.oecd.org/trade/benefitlib/45500791.pdf.
11. Ibid.
12. "Agreement on Technical Barriers to Trade," World Trade Organization website, accessed January 10, 2019, https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm#annexIII.
13. Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (Information Technology and Innovation Foundation, December 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.
14. "China's National People's Congress Officially Promulgates Standardization Law," American National Standards Institute website, accessed January 10, 2018, https://www.ansi.org/news_publications/news_story?menuid=7&articleid=7ab2aae7-c29b-438a-8a7d-0f19b94ee737.
15. "Committee on Technical Barriers to Trade, G/TBT/1/Rev.8," World Trade Organization website, accessed January 10, 2019; "Agreement on Technical Barriers to Trade," World Trade Organization website.
16 "China's National People's Congress Officially Promulgates Standardization Law," American National Standards Institute.
17. "Agreement on Technical Barriers to Trade," World Trade Organization website.

18. See Article 27.
19. "China's National People's Congress Officially Promulgates Standardization Law," American National Standards Institute.
20. Dean Garfield, "Market Access Challenges in China" (written testimony to the U.S. Senate Committee on Finance Subcommittee on International Trade, Customs, and Global Competitiveness, April 11, 2018), https://www.finance.senate.gov/imo/media/doc/11APR2018GARFIELDSTMNT.pdf.
21. World Trade Organization, "Restructuring and further trade liberalization are keys to sustaining growth" (news release, WTO, June 2, 2010), http://www.wto.org/english/tratop_e/tpr_e/tp330_e.htm.
22. Jost Wübbeke et al., "Made in China 2025: The making of a high-tech superpower and consequences for industrial countries" (Mercator Institute for China Studies, December 2016), https://www.merics.org/sites/default/files/2018-07/MPOC_No.2_MadeinChina2025_web.pdf.
23. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business In China" (The Center for Strategic and International Studies, August 2, 2018), https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.
24. "Notice on the Release of the Development Strategy for Establishing National Standardization," website of the State Council of the Peoples Republic of China, December 17, 2015, http://www.gov.cn/zhengce/content/2015-12/30/content_10523.htm.
25. "Internet of Things Standardization White Paper" (China Electronics Standardization Institute, January 18, 2016), http://www.cesi.cn/cesi/guanwanglanmu/biaozhunhuayanjiu/2016/0119/12330.html.
26. "Notice on the Implementing for Advancing 'Internet Plus' Convenient Transportation and Promoting the Development of Smart Technologies" (China's National Development and Reform Commission and the Ministry of Transport, July 30, 2016), http://www.sdpc.gov.cn/zcfb/zcfbtz/201608/t20160805_814065.html.
27. Energy-Saving and New-Energy Automotive Industry Development Plan (2012-2020) § 6(2)(2) (State Council of the People's Republic of China, Guo Fa [2012] No. 22, issued June 28, 2012).
28. "New scientific data rules in China: China claims 'data sovereignty,'" Hogan Lovells website, accessed January 11, 2019, https://hoganlovells.com/~/media/hogan-lovells/pdf/2018/2018_6_5_education_alert_new_scientific_data_rules_in_china.pdf.
29. "The Impact of Scientific Data Administrative Measures on Foreign Companies in China," Ropes and Gray website, accessed January 11, 2019, https://www.ropesgray.com/en/newsroom/alerts/2018/08/The-Impact-of-Scientific-Data-Administrative-Measures-on-Foreign-Companies-in-China#Footnote_2.
30. "New scientific data rules in China: China claims 'data sovereignty,'" Hogan Lovells website; The US-China Business Council, "Technology Security and IT in China: Benchmarking and Best Practices: July, 2016" (trade association report, U.S.-China Business Council, July 2016), https://www.uschina.org/sites/default/files/Technology%20Security%20and%20IT%20in%20China%20-%20%20Benchmarking%20and%20Best%20Practices.pdf.
31. Lester Ross, "China's new research rules will shackle Xi's innovation drive," *Nikkei Asian Review,* July 3, 2018, https://asia.nikkei.com/Opinion/China-s-new-research-rules-will-shackle-Xi-s-innovation-drive.
32. David Cyranoski, "China's crackdown on genetics breaches could deter data sharing," *Nature,* November 13, 2018, https://www.nature.com/articles/d41586-018-07222-2.
33. Ibid.
34. Ibid.
35. "New scientific data rules in China: China claims 'data sovereignty,'" Hogan Lovells.
36. For example, see: "Recommended Data Repositories," *Nature* website, accessed January 14, 2019, https://www.nature.com/sdata/policies/repositories; "Data repositories," Open Access Directory website, accessed January 14, 2019, http://oad.simmons.edu/oadwiki/Data_repositories; National Science

Foundation, *Today's Data, Tomorrow's Discoveries: Increasing Access to the Results of Research Funded by the National Science Foundation* (Alexandria, Virginia: National Science Foundation, March 18, 2015), https://www.nsf.gov/pubs/2015/nsf15052/nsf15052.pdf.

37. World Trade Organization (WTO), "Measures Adopted and Under Development by China Relating to its Cybersecurity Law" (Geneva: Communication from the United States to China at the WTO Council for Trade in Services, S/C/W/378, October 5, 2018), https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/248583/q/S/C/W378.pdf.
38. The German Council of Economic Experts, "Setting the Right Course for Economic Policy," (Annual Report 2018/19, November 7, 2018), https://www.sachverstaendigenrat-wirtschaft.de/en/publications/annual-reports/annual-report-201819.html.
39. "Taxation of Digital Activities in the Single Market," (draft European Union document, February 26, 2018), https://www.politico.eu/wp-content/uploads/2018/02/taxation-of-digital-economy-2.pdf.
40. Gary Clyde Hufbauer and Zhiyao Lu, "The European Union's Proposed Digital Services Tax: A De Facto Tariff" (Peterson Institute for International Economics, June, 2018), https://piie.com/system/files/documents/pb18-15.pdf.
41. Organization for Economic Cooperation and Development (OECD), "Tax Challenges Arising from Digitalisation – Interim Report 2018" (Paris: OECD, March 16, 2018), http://www.oecd.org/tax/tax-challenges-arising-from-digitalisation-interim-report-9789264293083-en.htm.
42. Joe Kennedy, "Europe's assault on American internet companies escalating," *Fox Business,* December 3, 2018, https://www.foxbusiness.com/technology/europes-assault-on-american-internet-companies-escalating.
43. Leigh Thomas, "EU ministers fail to break digital tax deadlock," *Reuters,* December 3, 2018, https://www.reuters.com/article/us-eu-tax-digital/eu-ministers-fail-to-break-digital-tax-deadlock-idUSKBN1O22MR.
44. "GAFA tax: in France, the giants of the Internet will be taxed from January 1," BFM TV, December 17, 2018, https://www.bfmtv.com/economie/taxe-gafa-en-france-les-geants-de-l-internet-seront-taxes-des-le-1er-janvier-1590424.html.
45. Joe Kennedy, "Resist Unilateral EU Efforts to Change International Tax Law for Corporations," Innovation Files blog, July 26, 2018, https://itif.org/publications/2018/07/26/resist-unilateral-eu-efforts-change-international-tax-law-corporations.
46. Natalie Sherman, "US attacks UK plan for digital services tax on tech giants," BBC, October 31, 2018, https://www.bbc.com/news/business-46050724.
47. "Request for comments on the Proposed Privacy and Data Protection Policy and Bill, 2018," Kenya's Ministry of Information, Communication, and Technology website, accessed January 11, 2019, http://www.ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/.
48. "Data protection in Kenya," (Kenya ICT Action Network, 2018), https://www.kictanet.or.ke/?wpdmpro=data-protection-in-kenya.
49. Sensitive data is defined as data revealing a person's race, health status, ethnic social origin, political opinion, belief, personal preferences, location, genetic data, biometrics, sex life or sexual orientation, and personal financial expenditures.
50. "Data protection in Kenya," (Kenya ICT Action Network, 2018).
51. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

52. See: Robert Atkinson, "Don't Just Fix Safe Harbor, Fix the Data Protection Regulation," Euractiv, December 18, 2015, https://www.euractiv.com/section/digital/opinion/don-t-just-fix-safe-harbour-fix-the-data-protection-regulation/.

53. For example, a report for the European Parliament on data protection in China states that there is "no common ground … found between two fundamentally different systems both in their wording and in their raison d'etre." The report takes a relativist approach by saying China's culture and approach to human rights means the European Union should treat China differently when it comes to trade and privacy issues, despite the fact that "China does not have a general data protection act but traces of data protection may be found in a multitude of sector-specific legal instruments." Paul de Hert and Vagelis Papakonstantinou, "The Data Protection Regime in China" (Brussels: report for the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, October 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

54. Kenya's Ministry of Information, Communication, and Technology, "The Kenya National ICT Masterplan: Towards a Digital Kenya" (Nairobi, April 2014), http://www.ict.go.ke/wp-content/uploads/2016/04/The-National-ICT-Masterplan.pdf.

55. "Request for comments on the Proposed Privacy and Data Protection Policy and Bill, 2018," Kenya's Ministry of Information, Communication, and Technology website.

56. "Press Note 2 (2018 Series)," India's Department of Industrial Policy and Promotion website, accessed January 11, 2019, https://dipp.gov.in/sites/default/files/pn2_2018.pdf.

57. A marketplace-based model of e-commerce is a model of providing an information technology platform by an e-commerce entity on a digital and electronic network to act as a facilitator between buyer and seller. An inventory-based model of e-commerce is a model wherein inventory of goods and services are owned by an e-commerce entity and are sold to consumers directly.

58. Prasannata Patwa, "Cloudtail India posts 27% rise in sales in 2017-18," *LiveMint,* October 14, 2018, https://www.livemint.com/Companies/Uf0f7vHlRVP6wyR3kpSy4N/Cloudtail-India-posts-27-increase-in-sales-to-7149-crore.html.

59. Anirban Sen, "Flipkart, Amazon in tight race for exclusive tie-ups with phone makers," *LiveMint,* October 5, 2018, https://www.livemint.com/Companies/0kg99mEITjiWdU429gZIfM/Flipkart-Amazon-in-tight-race-for-exclusive-tieups-with-ph.html.

60. Eric Bellman and Vibhuti Agarwal, "India's Biggest Competitors to Walmart and Amazon? Mom and Pop," *The Wall Street Journal,* May 28, 2018, https://www.wsj.com/articles/indias-biggest-competitors-to-walmart-and-amazon-mom-and-pop-1527512400.

61. Ananya Bhattacharya, "Buying Flipkart was the easy part. The real test for Walmart starts now," *Quartz India,* May 10, 2018, https://qz.com/india/1273483/walmart-flipkart-deal-all-the-e-commerce-hurdles-walmart-will-face-in-india/.

62. Surabhi Agarwal, "Internet users in India expected to reach 500 million by June: IAMAI," *Economic Times,* February 20, 2018, https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms; Bellman and Agarwal, "India's Biggest Competitors to Walmart and Amazon? Mom and Pop," *The Wall Street Journal.*

63. Durba Ghosh, "Indian e-commerce companies had record-breaking festive sales—again," *Quartz India,* November 29, 2018, https://qz.com/india/1478164/amazon-india-flipkart-paytms-festive-sales-break-records-again/.

64. Walmart, "Walmart and Flipkart Announce Completion of Walmart Investment in Flipkart, India's Leading Marketplace eCommerce Platform," news release, August 18, 2018, https://news.walmart.com/2018/08/18/walmart-and-flipkart-announce-completion-of-walmart-investment-in-flipkart-indias-leading-marketplace-ecommerce-platform.

65. "India's $40bn FDI pips China's $33bn in 2018," *The Times of India,* December 29, 2018, https://timesofindia.indiatimes.com/business/india-business/indias-40bn-fdi-pips-chinas-33bn-in-2018/articleshow/67294714.cms.
66. Reserve Bank of India, "Statement on Developmental and Regulatory Policies (April 5, 2018), press release, April 5, 2018,.
67. Ibid.
68. Julia Fioretti, "EU looks to remove national barriers to data flows," *Reuters,* September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q.
69. "Requirements for Exemption to Store Electronic Accounting Records Abroad Will Be Abolished," Horten website, accessed November 9, 2017, http://en.horten.dk/News/2015/February/Requirement-for-exemption-to-store-electronic-accounting-records-abroad-will-be-abolished.
70. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
71. Ibid.
72. "Intangible Goods are Now Subject to Import Duty," Baker McKenzie website, March 7, 2018, accessed January 11, 2019, https://www.bakermckenzie.com/en/insight/publications/2018/03/intangible-goods-import-duty-indonesia.
73. Stefani Ribka, "Indonesia: Duties for digital goods won't violate rules," Asia News Network, December 22, 2017, http://annx.asianews.network/content/indonesia-duties-digital-goods-wont-violate-rules-63681.
74. Alan Beattie, "Data protectionism: the growing menace to global business," *Financial Times,* May 13, 2018, https://www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb; Nigel Cory, "Post-Hearing Written Submission for the United States International Trade Commission Regarding Investigations Global Digital Trade 1 (No. 332-562) and Global Digital Trade 2 (No. 332-563)" (The Information Technology and Innovation Foundation, March 29, 2018), http://www2.itif.org/2018-testimony-global-digital-trade.pdf.
75. "Intangible Goods are Now Subject to Import Duty," Baker McKenzie website.
76. World Trade Organization (WTO), "Work Programme on Electronic Commerce" (Geneva: WTO, WT/L/274, September 30, 1998), https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/31348/T/WT/L/274.DOC.
77. Ludger Schuknecht and Rosa Pérez-Esteve, "A Quantitative Assessment of Electronic Commerce" (Geneva: Report for the World Trade Organization, September 1999), https://www.wto.org/english/res_e/reser_e/ae9901_e.htm.
78. Ribka, "Indonesia: Duties for digital goods won't violate rules," Asia News Network.
79. Robert D. Atkinson, "The Past and Future of America's Economy: Long Waves of Innovation that Power Cycles of Growth" (Northampton, Massachusetts: Edward Elgar, 2004).
80. Jason Dedrick, ViJay Gurbaxani, and Kenneth L. Kraemer, "Information Technology and Economic Performance: A Critical Review of the Empirical Evidence," ACM Computing Surveys 35, no. 1 (March 2003), 1.
81. For several of the numerous literature surveys, see: Mirko Draca, Raffaella Sadun, and John van Reenen, "Productivity and ICT: A Review of the Evidence" (discussion paper no. 749, Centre for Economic Performance, August 2006), http://eprints.lse.ac.uk/4561/; Tobias Kretschmer, "Information and Communication Technologies and Productivity Growth: A Survey of the Literature," OECD Digital Economy Papers, no. 195 (2012), http://dx.doi.org/10.1787/5k9bh3jllgs7-en; M. Cardona, T. Kretschmer, and T. Strobel, "ICT and Productivity: Conclusions from the Empirical Literature,"

Information Economics and Policy 25, no. 3 (September 2013): 109–125, doi:10.1016/j.infoecopol.2012.12.002.

82. Jack E. Triplett and Barry P. Bosworth, "Productivity Measurement Issues in Services Industries: 'Baumol's Disease' has Been Cured," FRBNY Economic Policy Review 9, no. 3 (2003): 23–33; see also Carol A. Corrado et al., "Sectoral Productivity in the United States: Recent Development and the Role of IT," Productivity Measurement and Analysis (OECD Publishing, 2008), https://www1.oecd.org/std/productivity-stats/44516351.pdf#page=437; Sophia P. Dimelis and Sotiris K. Papaioannou, "Technical Efficiency and the Role of ICT: A Comparison of Developed and Developing Countries," Emerging Markets Finance & Trade 47 (July 2, 2011): 40–53, doi:10.2753/REE1540-496X4704S303; Jason Dedrick, Kenneth L. Kraemer, and Eric Shih, "Information Technology and Productivity in Developed and Developing Countries," *Journal of Management Information Systems* 30, no. 1 (July 1, 2013): 97–122, doi:10.2753/MIS0742-1222300103).
83. Ribka, "Indonesia: Duties for digital goods won't violate rules," Asia News Network.
84. Nigel Cory and Robert Atkinson, "Time to Restrict GSP Benefits to Fight Trade Mercantilism" (The Information Technology and Innovation Foundation, August, 2018), https://itif.org/publications/2018/08/20/time-restrict-gsp-benefits-fight-trade-mercantilism.
85. "TPP: Chapter 14: Electronic Commerce," (New Zealand Ministry of Foreign Affairs and Trade website), https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.
86. "On the moratorium, the African Group are still discussing it in view of the revenue implications of the current moratorium on customs duties, particularly in the context of increasing digitization of goods and services. For all these reasons, the renewal of the moratorium should not be seen as automatic." See the various statements from India, South Africa, and the Africa Group at "MC11 documents: e-commerce," World Trade Organization website, accessed January 11, 2019, https://www.wto.org/english/thewto_e/minist_e/mc11_e/documents_e.htm.
87. United Nations Conference for Trade and Development (UNCTAD), "Rising Product Digitalisation and Losing Trade Competitiveness" (Geneva: UNCTAD, 2017), https://unctad.org/en/PublicationsLibrary/gdsecidc2017d3_en.pdf.
88. Nick Vivarelli, "Italy Set to Regulate Theatrical Windows Following Netflix Controversy," *Variety,* November 15, 2018, https://variety.com/2018/film/global/italy-regulate-theatrical-windows-netflix-controversy-1203029390/.
89. Andreas Wiseman, "Venice's Warm Embrace Of Netflix Irks Italian Cinema Associations, " *Deadline,* July 30, 2018, https://deadline.com/2018/07/netflix-venice-policy-1202436362/.
90. Ibid.
91. Nick Vivarelli, "Italian Box Office Drops 12.5% in 2017; Local Movies Suffer, While Hollywood Stays Strong," *Variety,* December 28, 2017, https://variety.com/2017/film/news/italian-box-office-drops-2017-local-movies-suffer-hollywood-strong-1202647872/; Nick Vivarelli, "Italian Box Office Sinks to Worst Result in a Decade," *Variety,* January 3, 2019, https://variety.com/2019/film/news/italy-2018-box-office-worst-result-in-a-decade-1203097615/.
92. Andreas Wiseman, "Germany's Largest Cinema Org Issues Netflix Warning As Streamer Encounters Growing Euro Heath," *Deadline,* September 28, 2018, ttps://deadline.com/2018/09/netflix-germany-berlin-film-festival-hdf-kino-eu-1202465672/.
93. Zack Sharf, "Ted Sarandos: Theatrical Windows are 'Disconnecting People from Movies,' Not Netflix," *IndieWire,* December 4, 2018, https://www.indiewire.com/2018/12/ted-sarandos-netflix-theatrical-windows-disconnecting-people-from-movies-1202025231/.
94. Andreas Wiseman, "Marone! Venice's Warm Embrace Of Netflix Divides Italian Biz: 'It's A Wake-Up Call,'" *Deadline,* August 3, 2018, https://deadline.com/2018/08/netflix-venice-film-festival-cannes-debate-1202438850/.

95. Ibid.

96. "Netflix is moving television beyond time-slots and national markets," *The Economist,* June 30, 2018, https://www.economist.com/briefing/2018/06/30/netflix-is-moving-television-beyond-time-slots-and-national-markets?fsrc=scn/fb/te/bl/ed/netflixismovingtelevisionbeyondtimeslotsandnationalmarketsthetelevisionwillberevolutionised.

97. Elsa Keslassy, "Proposals to Shorten Windowing in France Unveiled," *Variety,* March 9, 2018, https://variety.com/2018/film/news/proposals-shorten-windowing-france-unveiled-1202722537/.

98. Melanie Goodfellow, "Canal Plus renews commitment to French cinema," *Screen Daily,* November 9, 2018, https://www.screendaily.com/news/canal-plus-renews-commitment-to-french-cinema/5134424.article.

99. Andreas Wiseman, "Germany's Largest Cinema Org Issues Netflix Warning As Streamer Encounters Growing Euro Heat," *Deadline,* September 18, 2018, https://deadline.com/2018/09/netflix-germany-berlin-film-festival-hdf-kino-eu-1202465672/.

100. Netflix, "Netflix Continues to Bring New and Diverse Stories From Europe, Middle East, and Africa to the World," news release, April 18, 2018, https://media.netflix.com/en/press-releases/netflix-continues-to-bring-new-and-diverse-stories-from-europe-middle-east-and-africa-to-the-world.

101. "Netflix to Open French Office, Agrees on More Local Content and 2% Tax on Revenues," European Documentary Network, October 4, 2018, http://edn.network/news/news-story/article/netflix-to-open-french-office-agrees-on-more-local-content-and-tax-on-revenues/?tx_ttnews%5BbackPid%5D=139&cHash=e80eef0bae1e21aa174dca9c17282acb.

102. Saudi Arabia's Communications and Information Technology Commission, Cloud Computing Regulatory Framework (Riyadh, 2018), http://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf.

103. "Saudi Arabia's Communications and Information Technology Commission," Cloud Computing Regulatory Framework.

104. For example: "Indian Cloud Data Centres Will Make or Break Digital India," *FirstPost,* October 30, 2015, http://www.firstpost.com/business/sponsored-indian-cloud-data-centres-will-make-or-break-digital-india-2475598.html.

105. Michael S. Rosenwald, "Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-Down Towns," *The Washington Post*, November 24, 2011, http://www.washingtonpost.com/business/economy/cloud-centersbring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html; Henry Blodget, "The Country's Problem in a Nutshell: Apple's Huge New Data Center in North Carolina Created Only 50 Jobs," *Business Insider*, November 28, 2011, http://www.businessinsider.com/apple-new-data-center-north-carolina-created-50-jobs-2011-11; Darrell Etherington, "Apple to Build a $2 Billion Data Command Center in Arizona," *TechCrunch*, February 2, 2015, https://techcrunch.com/2015/02/02/apple-to-build-a-2-billion-data-command-center-in-arizona/; Rich Miller, "The Economics of Data Center Staffing," Data Center Knowledge, January 18, 2008, http://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing/.

106. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? (The Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

107. Serra Hiziroglu and Ayça Sarıkamış, "Communiqués recently published by capital markets board on information systems management and independent audit of information systems," Lexology, February 7, 2018, https://www.lexology.com/library/detail.aspx?g=c6601e1b-6d4b-40c6-81ed-834fc60cea3c.

108. Nezihe Boran Demir, "Management of Information System," Erdem and Erdem website, March 2018, accessed January 11, 2018, http://www.erdem-erdem.av.tr/publications/newsletter/management-of-information-systems/.

109. Ibid.

110. Ingrid Lunden, "PayPal to halt operations in Turkey after losing license, impacts 'hundreds of thousands,' *TechCrunch,* May 31, 2016, https://techcrunch.com/2016/05/31/paypal-to-halt-operations-in-turkey-after-losing-license-impacts-hundreds-of-thousands/.

111. Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, "Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" (Washington, D.C., July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," PricewaterhouseCoopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

112. "Lehman Brothers International (Europe)."

113. "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.

114. These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states: "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

ACKNOWLEDGMENTS

The author wishes to thank the following individuals for providing input to this report: Robert D. Atkinson, Stephen Ezell, Daniel Castro, and Joe Kennedy. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Nigel Cory is associate director, trade policy, with the Information Technology and Innovation Foundation. He previously worked as a researcher at the Sumitro Chair for Southeast Asia Studies at the Center for Strategic and International Studies. Prior to that, he worked for eight years in Australia's Department of Foreign Affairs and Trade, which included positions working on G20 global economic and trade issues and the Doha Development Round. Cory also had diplomatic postings to Malaysia, where he worked on bilateral and regional trade, economic, and security issues; and Afghanistan, where he was the deputy director of a joint U.S./Australia provincial reconstruction team. Cory holds a master's in public policy from Georgetown University and a bachelor's in international business and a bachelor's in commerce from Griffith University in Brisbane, Australia.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.