The Worst Innovation Mercantilist Policies of 2016

BY NIGEL CORY | JANUARY 2017

When countries impose protectionist and trade-distorting practices in high-value tech sectors, they don't just damage competitors; they damage the entire global innovation system, leading to less overall innovation and productivity growth.

Around the world, countries are competing for market share in high-wage, innovation-based industries. Unfortunately, as this global race for innovation advantage intensifies, many countries have turned to "innovation mercantilism"—a strategy that seeks to achieve prosperity by imposing protectionist and trade-distorting policies that tip market scales to expand domestic technology production. These destructive "beggar-thy-neighbor" tactics—such as forcing companies to transfer the rights to their technology or relocate their production, research and development (R&D), or data storage activities—are intended to either replace imports with domestic production or to unfairly promote exports. Countries are increasingly using such innovation mercantilist policies in high-value tech sectors such as life sciences, renewable energy, computers and electronics, and Internet services. This report documents the 10 worst innovation mercantilist policies enacted by countries in 2016, finding China, Indonesia, Russia, and Vietnam to head the list.

Innovation mercantilist practices do not just damage competitors; they damage the entire global innovation system, leading to less overall innovation and productivity growth.[1] Moreover, they often do not even help the countries embracing the practices, particularly over the long run; instead, mercantilist policies lead them to neglect the greater opportunity to spur growth by raising the productivity of all sectors, not just high tech.

This fourth annual report documents what the Information Technology and Innovation Foundation (ITIF) sees as the 10 worst innovation mercantilist practices proposed, drafted, or implemented in 2016. Policies were chosen based on their detrimental effects globally, so some nations have more than one included, due to the policies' widespread impact.

SUMMARY OF THE WORST INNOVATION MERCANTILIST POLICIES OF 2016

- China: Introduced a new cybersecurity law that imposes extensive local data-storage requirements, audits that discriminate against foreign technology products, and forced intellectual property and source code disclosures.
- China: Introduced new cloud-computing restrictions that essentially exclude and prevent foreign firms from operating in the Chinese market.
- Germany: Introduced forced local data-storage requirements—ostensibly due to privacy and cybersecurity concerns—as part of a new telecommunications data law.
- Indonesia: Introduced forced local data-storage requirements for Internet-based, over-the-top content providers.
- Indonesia: Introduced a patent law amendment that undermines pharmaceutical intellectual property and forces local production and technology transfers.
- Russia: Introduced forced local data-storage requirements and encryption-key disclosure as part of a new telecommunications data law.
- Russia: Introduced new government procurement rules that ban the purchase of foreign software.
- Turkey: Introduced a new data-protection law with stringent transfer requirements that acts as de facto forced local data storage.
- Vietnam: Introduced forced local data-storage requirements for Internet-based, over-the-top content providers.
- Vietnam: Introduced a new network-security law that forces companies to disclose encryption keys and source code to the government as a condition of market access.

THE NATURE OF INNOVATION INDUSTRIES

A growing number of economists have come to see 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 one-half of America's economic growth can be attributed to scientific and technological innovation.[2] 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 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 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. What then are the attributes that define these innovative businesses and, by definition, innovation industries?[3] 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 can cost hundreds of millions of dollars to produce, but additional digital copies can be produced at virtually no cost.

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.

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

As a result, to maximize innovation by these types of industries, the global trading system needs to get three key factors right:

1. **Ensuring the largest possible markets:** For innovation industries with high fixed costs of design and development but lower marginal costs of production, larger markets are critical, since 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 20 countries rather than 5, expanding their sales by a factor of 4, their total costs increase by much less than a factor of 4. That is why numerous studies have found a positive effect of the ratio of cash flow to capital stock on the ratio of R&D investment to capital stock. But a host of different innovation mercantilist policies act to limit global market size either at the enterprise or establishment level.

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.[4] Some mercantilist policies—including discriminatory government procurement, protected state-owned enterprises, and government bailouts—enable weak firms to enter into or remain in a market, siphoning 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 intellectual property. Strong intellectual property protections are needed to enable inventors to realize economic gains from their inventions, which further gives them the ability to reinvest those profits into the next generation of innovative activities. However, if competitors are able to enter into and/or remain in a market because they obtain an innovator's intellectual property at less than the fair market price (either through theft or coerced transfer), they are able to siphon off sales that would otherwise go to innovators.

It is in this context that innovation mercantilist policies are so problematic, for relative to mercantilist policies affecting other industries (e.g., clothing or lumber), the global economic damages from innovation mercantilist policies are significantly worse.

Innovation mercantilist policies also harm the nations that use them. Such trade-distorting policies promise to deliver some short-term employment and economic gains; however, ultimately, they lead to a number of adverse consequences. First, they can raise the cost of key capital goods, such as information and communications technology (ICT) products, which reduces capital goods use by industries throughout an economy, lowering a country's overall innovation and productivity. Second, they can limit countries' participation in global value chains for the production of high-technology products. Third, they can lead to broad economic inefficiencies. Fourth, they cause reputational harm that can damage a country's attractiveness as a location for foreign direct investment. Fifth, they tend to isolate nations from the global economy, while often failing to achieve their intended aims. Sixth, such policies are fundamentally unsustainable, in part because they engender reciprocal protectionist policies by other countries, which undermines the global economic order. Seventh, and most importantly, they lead to unbalanced and unsustainable "dual economies," with weak productivity growth in non-favored sectors.

Countries using these policies instead need to recommit to—and indeed expand their embrace of—competitive markets, open trade, and economic liberalization. Strong productivity- and innovation-enhancing policies should be at the core of their economic strategies, which should include investment in education, research, physical and digital infrastructures, and technology adoption and commercialization. Such an approach will prove a far more effective path for broad and sustainable economic and employment growth than short-sighted mercantilist trade and economic policies. At the same time, the community of nations committed to rules-based trade need to do much more to effectively push back against nations' innovation mercantilist policies.

THE 10 WORST INNOVATION MERCANTILIST POLICIES OF 2016

The following 10 worst innovation mercantilist policies are just a sampling of unfair trade practices that nations proposed, drafted, or implemented in 2016 and that the global trading system needs to address as a top priority.

China: Cybersecurity Law Restricts Foreign Technology Companies, Reinforces Data Localization, and Forces Source-Code and Intellectual Property Disclosure

The Chinese government continues to use national security, cybersecurity, and other legal reforms as vehicles for mercantilist objectives. On November 7, China enacted a new Cybersecurity Law that introduces (further) restrictive requirements on foreign technology companies: *The Economist* aptly described it as a "techno-nationalist Trojan horse."[5] Just how restrictive this law will become depends upon implementing regulations that will be enacted before the law comes into force on June 1, 2017.

China continues to use national security, cybersecurity, and other legal reforms as vehicles for mercantilist objectives.

China's new cybersecurity law—through discriminatory standards and forced local data-storage requirements—reinforces existing policies that segment its citizens and tech firms, in addition to its broader Internet ecosystem, from the rest of the world. The law is significant, as it is China's first to enact rules on the collection and use of personal data. The law forces companies in "critical information infrastructure" to store users' "personal information and other important business data" in China, a concept known as "forced localization." However, the law does not spell out what—exactly—each term means. For example, the final law differed from prior drafts by broadening the scope of personal data from "citizen's personal data" to "personal data," which could mean that even the personal data of foreigners is subject to China's strict localization requirements.[6]

The cybersecurity law will affect a large part of China's technology market, as the country is likely to take an expansive view of what is "critical information infrastructure" (CII). The basis of China's position is thus far broadly defined as information infrastructure in sectors that may seriously jeopardize national security, the national economy, and people's livelihoods or public interest, should such infrastructures malfunction or be subject to damage or data leakages.[7] Indicative of this broad reach, sectors that have been cited for inclusion include public communication and information services, energy, transportation, water resources utilization, finance, public service, and e-government affairs.

China may use the law to expand an existing—and controversial—cybersecurity regulation that is highly discriminatory toward foreign tech firms and products. The cybersecurity law states that China will introduce a cybersecurity multilevel protection scheme (MLPS) for information technology (IT) products used in network security by CII sectors. This requirement is perhaps based off an existing MLPS that China has applied for information security (although this is unclear from the wording in the law).[8] This potential relationship raises serious concerns for foreign technology companies, as this earlier MLPS was highly discriminatory—it prohibited certain sectors from using foreign IT products and forced foreign companies to transfer intellectual property and source code to China for review.[9]

Equally troubling is the potential for China to use the law to revive the use of a high-discriminatory standard for IT products—the so-called "secure and controllable" concept—and intrusive security audits, both of which can be used to discriminate against foreign firms and to steal valuable intellectual property. The law calls for the use of "secure and trusted" network services and productions, without defining the term.[10] Current deliberations by China's National Information Security Standards Technical Committee on what this concept means (see below) and past Chinese government policy proposals point toward its mercantilist intent.[11] This concept, along with its analogous "independent and controllable," "secure and controllable," or "indigenous and controllable" terms have been a part of Chinese technology policymaking debates ever since the country backed down on implementing such a rule as part of a banking law in 2015. That proposed banking law used a "secure and controllable" provision as part of an explicit aim to replace foreign technology goods with local ones. China decided to "withdraw" this provision after it generated significant opposition from tech companies and trading partners, especially the United States.[12]

Fears about China's mercantilist intent have been confirmed during the process to define standards and key concepts under this cybersecurity law.

China essentially wants to force software companies, network-equipment makers, and other tech companies to disclose source code to supposedly prove their products can't be compromised by hackers.[13] Source code—the instructions that make a computer program run—enable technology to do the amazing things it does. For companies developing software, protecting source code is necessary to prevent other entities from stealing and free riding on the large research and development costs associated with software development. Source code is at the heart of a company's competitive advantage, but being digital, it is at heightened risk of duplication. Given China's poor protection of intellectual property, not to mention its role in the cybertheft of foreign trade secrets, it's unsurprising that foreign firms and trading partners, such as the United States, have reasonable fears that such intrusive inspections are simply a way to access and steal valuable intellectual property.

Fears about China's mercantilist intent have been confirmed during the process to define standards and key concepts under this law. Foreign companies submitted comments on implementing provisions, such as the definition of "secure and controllable," to China's National Information Security Standards Technical Committee (NISSTC) after the law was released. Some of Microsoft's comments focused on legitimate concerns about the utility in viewing source code for cybersecurity purposes, stating in its comments to NISSTC that "sharing source code in itself can't prove the capability to be secure and controllable. It only proves there is source code."[14] Yet, indicative of China's ulterior motives, the NISSTC rejected this feedback, saying that this comment was "not accepted."[15] This is despite the fact that Microsoft has already taken the significant step of providing Chinese authorities with viewing access to its source code at its "Transparency Center" in Beijing, a step that most other technology companies have not taken, given the risks of unauthorized disclosure. China's reaction to Microsoft's comments on the draft law is indicative of how intrusive the law is likely to be and how it may get even tougher than it already is for foreign technology companies to operate in China.

China's underlying mercantilist intent was further evident in comments and feedback provided to the NISSTC by the chief engineer at China's Ministry of Public Security's Network Security Bureau, who commented on the draft regulations by stating "the big trend is called shifting to favour domestic production … but it can't be written that way, so one calls it independent and controllable." NISSTC's response was to mark the comment "approved."[16]

Beyond these headline issues, the law will have many other negative effects on China's digital economy. For example, the law requires network operators to provide "technical support" to authorities for national security and law enforcement purposes, which could include forcing companies to build backdoors to their encryption. Furthermore, China makes censorship a central part of its new cybersecurity law, threatening to punish companies if they allow "unapproved" information to be distributed online. The surveillance requirements are extensive, as the law requires network operators to monitor and record their network operations and to preserve related web logs for at least six months.[17]

China: Uses Regulation to Preclude Access to Its Cloud Computing Market

New regulations regarding cloud-computing services in China confirm its persistence in erecting barriers between its tech sectors and digital economy and that of the rest of the world. In March 2016, China made significant changes to the licensing and regulatory regime of Chinese telecom and Internet services that essentially exclude foreign technology firms involved in cloud computing, big data, and other information services from operating in China. These regulations, again, reinforced the requirement for forced local data storage.[18] For foreign cloud-service providers—which include many leading U.S. companies—these regulations have essentially closed access to the Chinese market.

China enacted regulatory changes to make it even harder than it already was for foreign companies to establish and operate Internet-based information services in the country. First, China released regulations for several services it considers valued-added telecommunication services (VATS). By categorizing Internet-based services (e.g., cloud computing, big data, and other information services) as telecommunication services, and not as "computer and related services," it has much greater freedom to restrict market access to foreign tech firms. This is because China made commitments as part of its accession to the World Trade Organization (WTO) in 2001 to provide nondiscriminatory treatment and market access to foreign firms in "computer and related services."[19] This category of Internet-based computer services includes email, voicemail, online information and database retrieval, electronic data interchange, and enhanced facsimile services, code and protocol conversion, and online information and/or data processing.[20] Essentially, China's approach is a technical work-around to avoid its commitment to open its market for Internet-based computer services to foreign competition.

Second, China introduced a requirement for telecom and Internet Service Providers (ISPs) to apply for licenses for each subcategory of services, raising the potential for government

agencies to discriminate against foreign firms. For example, China's new subcategory, "internet-based resources collaboration services," means that providers of cloud computing application services, platform as a service, and software as a service would potentially have to apply for multiple licenses, given some firms and services cross over into multiple categories.

Third, China released new requirements that articulate the very small and restricted cloud-computing services space where foreign firms are allowed to operate. In October 2016, the Ministry of Industry and Information Technology released the "Notice on Regulating Business Behaviors in the Cloud Service Market," which outlined how foreign cloud companies are forbidden from working via local partnerships in any capacity beyond "technical assistance." It is not specified what is allowed under "technical assistance," but based on current practice, it is likely to mean that foreign companies are only allowed to license their goods (software and hardware) to their (forced) local partners and show them how to use them. The notice further specifies several activities that cloud service providers cannot perform, such as sign contracts directly with end users.

These new restrictions on foreign cloud service providers make an already restrictive situation that much worse. Strict entry requirements and (an already highly) discriminatory licensing process have largely kept foreign firms out of China's market. To operate in China, foreign firms must set up a joint venture with a Chinese partner who must have majority ownership (i.e., greater than 50 percent). A joint venture was a prerequisite for foreign firms to even apply for a license from Chinese authorities. Although there are over 20,000 local companies licensed to provide VATS in China, only 30 or so licenses have been issued to foreign companies, including five U.S. companies.[21]

A few large foreign firms have successfully run the gauntlet and decided to operate in China within the confines of these strict conditions by partnering with large Chinese firms—for example, Microsoft with 21Vianet (China's largest private data center operator), SAP with China Telecom, and IBM with a group of local companies.[22] As described, these foreign firms are severely restricted in what they can do, often being constrained to arrangements whereby they license their products to their local partners, who set up and run the data centers and cloud services and manage relations with end users.

This mercantilist approach to cloud computing is consistent with China's ongoing efforts to develop a local cloud-computing sector that uses indigenously developed technology. China's ambitions in the sector started as part of the country's *National Medium and Long-Term Plan (MLP) for Science and Technology Development (2006-2020)*. Building on this in 2010, China identified cloud computing as one of 11 strategic emerging industries that would receive special attention and funding, all in pursuit of the goal of expanding access to cloud resources in China, developing indigenous cloud-computing technology, and creating an internationally competitive Chinese cloud-computing sector. More recently, the Ministry of Science and Technology's *12th Five-Year Plan (2011-2015)* paid particular attention to cloud computing, where the aim became to develop a cloud-computing

standard based on indigenously developed technology.[23] These policies, taken together, show China's efforts to use mercantilist policies at home to support the development of "local champions," who, ideally for China, will eventually become more innovative and competitive and able to compete in overseas markets—against the very tech firms that are unable to compete in China.

Germany: Forced Local Data Storage for Telecommunications Data

Germany and France have been at the center of efforts to force companies to store data only in Europe or even in country, such as through a "Bundescloud" (a cloud for government data) in Germany.[24] This preference for digital protectionism stands in stark contrast to Germany's otherwise open approach to global trade. In the latest example of this approach, on December 18, 2015, Germany introduced local data storage requirements for a type of telecommunications metadata, through a law that will come into force on July 1, 2017.[25]

The law aims to generate and retain telecommunications metadata—the who, when, where, and how, not the what (the content)—of telecommunications for law enforcement and security purposes. This can include citizens' call records, phone numbers, location information, Internet protocol addresses, time and data of Internet usage, and billing information.[26] This is the second time Germany has tried to enact such a law, as the German Federal Constitutional Court declared a similar 2008 amendment to the German Telecommunications Act to be unconstitutional due to piracy concerns—a court test that the new law also may face.[27]

The new law forces companies to store this metadata locally in Germany, not even in any other European Union (EU) member state where the General Data Protection Regulation applies. Companies need to store metadata for 10 weeks and location data for 4 weeks. Restricting data storage to Germany, and not to European Union member states, is a change from the 2008 amendment, which allowed metadata to be stored in the European Union. This restriction potentially violates rules that protect the freedom of services provided by the *Treaty on the Functioning of the European Union* and the free flow of personal data under the EU's Data Protection Directive.[28]

Germany's use of data localization as a way to protect privacy and cybersecurity is misguided, as it is based on the false belief that data stored at home is more secure or better protected for privacy, and that, if transferred overseas, the data is somehow inherently less secure. As ITIF argues in *The False Promise of Data Nationalism*, what matters are the actual protective measures used to store and transfer the data and the enforcement of these measures.[29] As long as the company involved has legal nexus in a nation, it is subject to the privacy and cybersecurity laws and regulations of that nation; moving data overseas, or storing it elsewhere, does not give the company a free pass to ignore a nation's laws. It is either in compliance with the privacy laws and regulations of that nation, or it is not.

Germany's own deliberations over this forced data localization requirement also reveal the hypocrisy in the European Union's response to U.S. surveillance programs and the

implications this has for cross-border data flows, data protection, and privacy.[30] In debating this law, Germany's legislature explicitly stated that the metadata should be stored in Germany, and not in other European countries, as it does not trust that its fellow European Union members would not access the data.[31]

This lack of consistency should not obscure the fact that governments have a legitimate right to access data, such as for law enforcement and national security. However, the focus should be on accessibility, and the rules and legal protections governing such access, rather than geography. There should be clear legal repercussions if telecommunications companies are unable to provide timely access to requested data, but it should not matter where the data is stored, just that the company can produce it upon request. For example, similar metadata retention laws in the United Kingdom and Australia do not stipulate such data localization.[32]

Indonesia: Data Localization Requirement for Over-the-Top Service Providers

Indonesia is using forced localization and other restrictions in a misguided attempt to protect local technology and traditional telecommunications companies from foreign firms that provide innovative Internet- and app-based services.

Indonesia is doubling down on its pursuit of policies that force companies to store data locally—in other words, forcing data localization—in a misguided attempt to protect local technology and traditional telecommunications companies and to disadvantage innovative Internet- and app-based services. On March 31, 2016, Indonesia's Ministry of Communications and Informatics issued Circular Letter No. 3, which notifies companies about new regulations for over-the-top (OTT) services, such as requirements for forced data localization and the need for foreign OTT firms to establish a permanent office in Indonesia as a condition of market entry.[33]

OTT services are those delivered via the Internet and are some of the most popular and innovative services available. In broadcasting, OTT service providers (such as Netflix, Hulu, and HBO Go) deliver audio, video, and other media over the Internet without users having a subscription with the usual intermediaries, such as cable companies. For messaging, OTT service providers, such as WhatsApp, Skype, and Facebook, provide instant-messaging services as an alternative to text-messaging services provided by traditional mobile network operators. In using the Internet, OTT service providers and their customers can bypass traditional telecommunications network service providers to compete with services (such as voice) from telecommunications companies. These technological innovations have changed consumer behavior in media and telecommunications markets, among others, allowing consumers to change how they access and consume media and communicate. This is especially the case in developing countries that have deployed mobile-phone services before (or instead of) traditional phone services, thereby leapfrogging costly fixed-line infrastructure, which also led to a vibrant app and digital economy.

The letter from Indonesia's Ministry of Communication and Informatics notified foreign OTT service providers that upcoming regulations will require these providers to abide by a number of mercantilist and trade-distorting measures, such as:

- Forcing fee-for-service OTT providers (such as those that require a subscription) to form a joint venture with a local telecommunications provider;[34]
- Requiring companies to disclose source code as a condition of market access;
- Forcing companies to store data locally;
- Requiring companies to establish a permanent local office to operate in Indonesia;
- Requiring firms to use content filtering in accordance with Indonesian law, such as for security purposes (such as terrorism) or social/cultural purposes (such as pornography);
- Forcing firms to use an Indonesian Internet protocol number; and
- Forcing firms to use Indonesia's National Payment Gateway, a government-owned and run process that aims to make Indonesia's four payment systems interoperable, but in doing so, discriminates against foreign payment providers in a misguided attempt to coerce more local financial activity in e-commerce and other sectors.[35]

Unfortunately, these regulations for OTT services show that Indonesia has again turned to tried and failed interventionist and protectionist industrial development policies instead of positive policies that support innovation in Indonesia and its place in an open and vibrant global digital economy. In particular, the requirement to form a joint venture with local telecommunications firms shows that President Jokowi's government has succumbed to calls for protectionism from its inefficient and uncompetitive (and often state-owned) telecommunications companies.[36] Indicative of this, in January 2016, Indonesia's biggest (state-owned) telecommunications provider, Telekom Indonesia, blocked Netflix's entry into Indonesia because it did not have the right license and due to concerns about the content it carries.[37] Following this, Telkom Indonesia found a foreign company willing to abide by Indonesia's strict entry requirements to launch a video-streaming service—Hooq, a Singapore-based company—while still blocking Netflix.[38]

Indonesia: New Patent Law Undermines Intellectual Property Rights for Pharmaceuticals

On August 28, 2016, Indonesia introduced an amendment to its Patent Law that expands the mercantilist tools the government can use in the life-sciences sector.[39] The amendment includes vague and potentially expansive compulsory licensing and other provisions that undermine pharmaceutical intellectual property and that can ultimately be misused to force foreign companies to produce their products locally and/or to transfer their technology and intellectual property.

Indonesia's law also outlines situations where the government could issue compulsory licenses including:

- Granting a compulsory license to produce a pharmaceutical product that is patented in Indonesia for the treatment of a disease;
- Granting a compulsory license to import a pharmaceutical product that is patented in Indonesia but cannot be manufactured in Indonesia for the time being for the purpose of treatment of a disease; and

- Granting a compulsory license to export a pharmaceutical product that is patented in Indonesia and is manufactured in Indonesia for the purpose of treatment of a disease. This is done upon request by a developing or a least-developed country.[40]

Compulsory licenses—when a government allows someone else to produce a patented product or process without the consent of the patent owner—should be a last resort and reserved only for extraordinary situations.[41] Such licenses should not be a tool for industrial policy.

Indonesia's localization policies in the pharmaceutical sector, and past misuse of compulsory licensing, raise concerns about its use of the new law for mercantilist ends. Indonesia already uses extensive local production and forced technology transfer requirements in the pharmaceutical sector as part of a law introduced in 2008.[42] Indonesia has issued nine compulsory licenses for "government use" —in 2004, 2007, and 2012— and done so in a way that raises concerns about whether it will actually enter into good faith negotiations with rights holders in the future as part of this patent amendment.[43] In such a framework, companies are essentially negotiating under duress. These provisions create uncertainty, as the government has not elaborated on how the new law will work. While countries are able to determine the criteria to grant compulsory licenses under the Trade-Related Aspects of Intellectual Property (TRIPS) agreement, there are rules, norms, and steps to follow.[44] However, the new law makes these steps even harder to use. The new law makes it harder for pharmaceutical rights holders to enter into voluntary licensing agreements—which are supposed to be the preferred mechanism, short of a compulsory license—by requiring the disclosure of the terms of such agreements. This discourages companies from negotiating voluntary licenses in the first place, as it means they need to expose highly sensitive confidential information about their operations and their product.[45]

The new patent law also undermines Indonesia's attractiveness for pharmaceutical research and development by introducing a new restrictive criterion for assessing the patentability of pharmaceutical products. TRIPS states that a patent shall be available for an invention provided that it is new, involves an inventive step, and is useful.[46] Indonesia's new law adds a fourth criteria of "increased meaningful benefit," which will prevent pharmaceutical innovation that builds on prior knowledge to develop new and improved treatments, new dosage forms and combinations, and delivery mechanisms (e.g., oral medication instead of an injection, reducing the number of doses needed). Promulgating these new conditions places Indonesia in violation of its TRIPS commitments.

Unfortunately, the patent amendment was not the only trade-distorting, discriminatory policy that Indonesia enacted in the pharmaceutical sector in 2016. A January 2016 stimulus package included funds and policies to replace imports of raw materials for medicines and medical devices with domestic production.[47] Furthermore, on June 8, 2016, President Jokowi sent a presidential directive—on the "Acceleration of the Development of the Pharmaceutical and Medical-Equipment Industries"—to ministers to get them to enact a range of protectionist and discriminatory policies, including through expedited processing

for domestic production of medical ingredients, medicines, and medical equipment and favouring domestic goods in government procurement.[48]

Russia: Forced Local Storage for Telecommunications Data

The Russian government's parallel moves toward mercantilism and authoritarianism come together in a new surveillance law that includes extensive data localization requirements for telecommunications data, adding an additional layer to already extensive barriers to cross-border flows between Russia and the rest of the world. On July 6, 2016, Russia enacted a new law that forces telecommunication companies and ISPs to retain user communications for six months and communications metadata for three years. The law will apply to companies in Russia and overseas. Companies have until July 1, 2018, to implement these measures.[49]

Russia's new surveillance law includes extensive data localization requirements for telecommunications data, adding an additional layer to already extensive barriers to cross-border flows.

The law aims to help Russian authorities fight terrorism, but its impact will be felt economy-wide (and society-wide), especially by Russia's digital economy. First, the surveillance and localization requirements are much broader than other countries' telecommunications data-retention requirements, such as those of Germany, as it requires companies to store the actual content of users' communications for six months, such as voice data, text messages, pictures, sounds, and video, not just the metadata (the who, when, and how long of communications). Second, it requires telecommunications companies and ISPs to cut services to a user if they fail to respond to a request from law enforcement to confirm their identity (which raises a range of privacy issues). Third, it forces companies to help government authorities in decrypting user communications and prohibits encryption measures unless a decryption tool is available should Russian authorities need it. Fourth, it applies to foreign companies that fall within the broadly defined category of telecom providers and "facilitators of information dissemination by means of the Internet," such as online messaging services, email providers, social media and blogging sites, voice over Internet protocol services (which use the Internet to transmit voice and multimedia), and news sites.[50]

Russia already has one of the most extensive data localization laws in place, and once this law comes into force, the impact it will have on Russia's economy will increase. In 2015, Russia enacted a law that forces companies with Russian personal data to store it locally.[51] Russian telecommunications companies have complained about the large potential costs of implementing these extensive and intrusive laws. MegaFon, Russia's second-largest mobile-phone company, said that equipment and operating costs of implementing this new law are estimated to be around $3.6 billion.[52] These costs inevitably get passed on to customers, which drags down economic growth. Tele 2, another Russian mobile-phone provider, said that it would likely have to raise prices two- to three-fold to cover the costs of implementation.[53] Beyond the implications for privacy and freedom of expression in Russia, these policies will certainly chill Russia's digital economy, as it makes it harder and costlier for both domestic and foreign firms to operate.

Russia: New Government Procurement Rules Ban the Purchase of Foreign Software

In 2016, Russia continued its move away from the principles of the open and rules-based trading system it signed up to when it joined the World Trade Organization in 2012 by adding software to its mercantilist aims to replace foreign goods and services with domestic ones. On January 1, 2016, a new law (Federal Law No. 188-FZ) introduced a registry of domestic software programs that are allowed to participate in federal, state, and municipal government procurement programs.[54] This effectively bans foreign software companies from selling to Russian national and subnational government agencies.

The ban on foreign software matters, because governments are among the biggest consumers of software products and services. Given the global nature of the software sector, and the fact that software can be developed and sold anywhere via the Internet, the law raises further concerns about Russia extending its protectionist and mercantilist policies into the digital economy. This restriction on software follows a 2015 law that forces firms that collect Russian personal data to store the data in Russia.[55] This data localization measure has the potential to segregate Russia's digital economy from the rest of the world, as not all foreign technology companies have the means to pay for or to arrange to shift data to Russian data centers, which likely do not provide best-in-class features in terms of services and cybersecurity. Indicative of Russia's approach, on November 17, 2016, Russia's communications regulator ordered ISPs to block access to the social-networking site LinkedIn, as it had not shifted its data pertaining to Russian customers to Russia.[56]

Onerous regulatory requirements and discriminatory procurement policies threaten the ability of foreign software, Internet, and other information-technology firms to provide products and services in Russia.[57] The software sector joins a growing list of economic activity—both new economy and traditional—where Russia has used industrial policy and government procurement to systemically discriminate against foreign providers. For example, in 2015, Russia restricted procurement of medical devices to a list of domestic manufacturers from the Eurasian Economic Union (Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia). Russia also enacted its mercantilist "Pharma 2020" strategy of forced localization for pharmaceutical production. Russia uses subsidies, price preference, procurement restrictions, and other policies as part of an explicit import-substitution goal of making local production account for at least 50 percent of total domestic pharmaceutical sales by 2020.[58]

Russia can enact these discriminatory policies as procurement is not subject to national treatment obligations—the basic principle to treat imported and domestic goods alike—under the General Agreement on Tariffs and Trade, and Russia has not acceded to the WTO's Government Procurement Agreement (GPA). Russia agreed to start the process to join the GPA as part of its commitment to join the WTO, but while Russia has technically lived up to its commitment to start negotiations to join, its introduction of discriminatory government procurement policies suggests that it plans to drag out negotiations, or possibly, never complete negotiations.[59]

Turkey: New Privacy Law Introduces De Facto Data Localization

Turkey's government has targeted foreign technology companies through several policies in recent years, so it's not a surprise to see Turkey introduce new data-privacy measures that act as a de facto data localization requirement. In April 2016, Turkey's new Data Protection Law came into force, placing burdensome obligations on data controllers and processors, requiring "express consent" from individuals to transfer personal data to another country. Along with other parts of the law, and previous data localization measures, it represents another move toward mercantilism in Turkey.

Turkey's approach to data privacy adds an additional barrier for foreign technology and Internet companies trying to do business in the country. It has not been clarified what "express consent" means under the new law, but the need for specific and individual engagement holds the potential to act as de facto data localization, as it makes it that much harder for foreign companies to use their existing infrastructure (such as data centers) to process personal data to design and deliver digital goods and services to customers in Turkey.

Onerous data-protection requirements threaten the data-driven business platforms that are playing an increasingly instrumental role in facilitating services trade, as these services are able to quickly and cheaply connect suppliers and sellers based on their collection and analysis of user data.[60] These innovative services enable the accumulation of data on a centralized platform that simultaneously aggregates supply and demand from two sides of a marketplace, giving rise to "multisided" or "bidirectional" business models that have transformed a number of services markets, such as Airbnb in hospitality, Uber in transportation, and Google in Internet search. The modern relationship between service platforms and consumers is truly two-way, as users are explicitly rewarded for sharing data about their behavior, preferences, and social networks. However, burdensome data-protection requirements undermine these businesses' ability to deliver broadly similar innovative services in countries around the world.

Like the earlier German case, Turkey's approach is misguided in its intent to enact stringent data-transfer requirements for personal data as a protectionist tool that favors local technology companies and data centers. At the heart of this approach is the misguided notion that data stored at home is more secure or better protected for privacy, and that if transferred overseas, the data is somehow inherently less secure.[61]

Turkey's new law adopts a similarly untenable and unrealistic approach to international data flows and protection as that of the European Union by requiring country-by-country assessments of privacy protections. The European Union currently only allows transfers of personal data to 12 countries that it has assessed on a country-by-country basis to determine whether they provide an "adequate" level of data protection.[62] Similarly, Turkey's newly formed "Data Protection Board" (staffed with political appointees, not technical staff) will assess whether other countries provide an "adequate" level of privacy protection. Under this law, if the country receiving data from Turkey does not offer

"adequate" protection, the Data Protection Board must provide permission for each transfer.[63] However, it is not hard to see how this strict approach to data privacy starts to unravel when one considers how easily data flows to other countries with arguably weaker data protections. Data flows between the European Union and China provide a clear example of how untenable this country-by-country process is. In October 2015, a report for the European Parliament showed that China has little-to-no data protection, but that data flows should not be cut off due to commercial and political considerations.[64] This tempered approach stands in contrast to the ongoing calls to cut off data flows between the European Union and the United States, despite the negotiation of a data-protection agreement, the Privacy Shield.

Turkey's past use of mercantilist policies to create a discriminatory advantage for local technology companies should raise suspicions about the purpose of the new Data Protection Law. In 2015, Turkey tried to misuse World Trade Organization safeguard measures to add new tariffs on smartphones, just three months after a local Turkish company manufactured its first domestically made smartphone.[65] Later that year Turkey introduced the Law on Electronic Payments, which mandated that all electronic and mobile payment operators store their data in country for a minimum of 10 years.[66] For one of the world's leading payment processors, PayPal, this was untenable, and on June 6, it announced that it was no longer going to operate in Turkey. PayPal uses a global platform to operate across more than 200 markets and cannot maintain dedicated infrastructure in each country, as this would undermine the globally distributed nature of its business and its ability to best protect consumer data and services.[67] It's coincidental that Turkey launched its own national payment system—called Troy—in April 2016. The absence of major alternative payment services, such as PayPal, will encourage consumers to seek out more traditional payment methods at Turkey's major banks, all of which have agreed to use Troy.[68]

Turkey's past use of mercantilist policies to create a discriminatory advantage for local technology companies should raise suspicions about the purpose of the new data protection law.

Vietnam: Server Localization Requirements for Over-the-Top Service Providers

In 2016, Vietnam introduced measures that make it more difficult for innovative over-the-top service providers (both local and foreign) to do business in Vietnam. As in the prior Indonesian case, OTT services deliver content or services over the Internet, which allows these companies and their customers to bypass traditional telecommunication providers. These new restrictions on OTT services add to Vietnam's already extensive restrictions on cross-border data flows and tight controls over how its citizens connect and use the Internet and engage in the global digital economy.

In January 2016, Vietnam released a draft regulation—Draft Decree Amending Decree 72—for OTT services that included a forced data localization requirement and the transfer of power to control OTT services to domestic telecommunications firms.[69] The circular requires OTT firms to locate servers in Vietnam, which would raise costs, diminish the incentives for service providers to offer OTTs, and potentially weaken data protection and cybersecurity measures, given the need to set up and manage duplicative infrastructure or to use data-center providers who do not use best-in-class protective measures. The draft

regulation also restricts how foreign OTT services operate in Vietnam by forcing them to form a joint venture with Vietnamese telecommunications companies. Meanwhile, it promulgates differentiated regulations for free and fee-based OTT services, as the latter need to get a license from the government, while the former do not.[70]

By introducing data localization requirements, the Vietnamese government reduces the benefits that come from competition among foreign OTT services (such as WhatsApp, Viber, and Tango), local providers (such as Zalo, Mocha, and VietTalk), and traditional telecommunications service providers. OTT services are obviously meeting a market demand that traditional carriers are not, given that 20 million Vietnamese had OTT apps on their smartphones in 2015.[71] For a country with a population of 90 million, and an estimated 36 million Internet users, OTT services have a substantial share of the market.[72]

The problem is that Vietnam seems intent on using regulation to protect traditional telecommunications providers that are unable to (or simply do not want to) compete with innovative OTT service providers and to discriminate against foreign firms in order to protect local firms (both those involved in traditional telecommunications and in OTT services). Indicative of this approach, Vietnamese media reported that Vietnam's prime minister ordered the Ministry of Information and Communications to restrict free OTT apps, such as Viber and Zalo (a local app), due to the impact these apps were having on traditional mobile carriers. As a Zalo representative rightly pointed out, free email services took over from postal services, but no one banned these services, yet the government seems intent on trying to do this with OTT services.[73]

If Vietnam wants a vibrant, competitive, and world-class digital economy, it should reverse these types of policies. Vietnam should not be prescribing how users access and use digital services and how these digital services operate, as this limits both consumer choice and engagement as well as business innovation. Consumers and businesses benefit when there is healthy competition between network and service providers, which is what should be happening between OTT service providers and traditional telecommunications firms. First, by requiring local data storage, the government increases operating costs for local and foreign firms. Second, by forcing companies to form joint ventures, the government limits the number and ability of firms to innovate and compete, especially small apps-makers involved in OTT services. However, while local firms may be affected by both measures, the burden falls disproportionately on foreign firms.

The unfortunate reality is that data localization for OTT services comes on top of extensive existing restrictions on data flows and Internet usage in Vietnam.[74] Vietnam forbids direct access to the Internet through foreign ISPs. Furthermore, all Internet companies, social networking sites, and websites that provide information or commentary about "politics, economics, culture, and society" based in the country need to register and obtain an operating license. Many of these same websites and social networks also need to store their data locally, such as keeping information posted online by users for 90 days and certain metadata for two years. ISPs also need to store information transmitted over their networks

for at least 15 days and to provide "technical assistance" and workspace to public security agents.[75]

Vietnam: New Law on Network Information Security Includes Forced Disclosure of Encryption Keys and Source Code

Over the past decade, the tech sector has made a significant contribution to Vietnam's rapid economic growth and development. However, while open for trade and foreign investment in many areas, Vietnam has also introduced mercantilist technology policies that are more reminiscent of its northern neighbor, China. A new law focused on network security contains cryptographic-key and source-code disclosures that can be used to steal valuable intellectual property.[76]

On July 1, 2016, the Law on Information Network Security (LONIS) came into effect. It opens the door to mandatory source-code and cryptographic-key disclosure, and applies onerous licensing and permitting requirements to millions of ICT products containing cryptographic capabilities. The vaguely drafted law indicates it would require companies to hand over the technical measures, norms, and plans (i.e., source code and other intellectual property) as a condition of market access and force handover of cryptographic keys to the government.[77] Alongside accompanying implementing legislation drafted by Vietnam's Ministry of Information and Communications (MIC) and Ministry of Defense (MOD), it places Vietnam's emerging ICT sector at risk while unnecessarily extending regulations to parts of the digital economy that are not related to privacy, cybersecurity, or national security.[78]

Vietnam's new law on network security forces cryptographic-key and source-code disclosures that can be used to steal valuable intellectual property.

Source code is the intellectual property at the heart of modern digital innovation, but as it is digital, it can be easily copied, transferred, and replicated. For companies developing software, or those that embed software within hardware (such as semiconductors), protecting source code is necessary to prevent other entities from stealing and free riding on the large R&D costs associated with development. Indicative of the sensitivity around source code is the fact that when one purchases software or goods with software embedded, the software is generally compiled in "object code" form, and not with the actual source code, as this would make it much easier for thieves, hackers, and others to copy and misuse.

It's important to remember that the United States does not have a law that requires a source-code audit as a condition of market entry. Furthermore, from a commercial perspective, not disclosing source code is standard practice, given the intellectual property and security implications. In enacting this legislation, Vietnam is following in the mercantilist path laid by China, which in an effort to gain valuable foreign IP, has used similar policies to require companies to transfer or allow access to source code as a condition of market entry.[79] Vietnam could avoid this association with China-style mercantilism and demonstrate its commitment to respect intellectual property by expanding the list of businesses exempted from applying for a license to ensure it only covers those businesses that are directly engaged in areas of national security.[80]

REFLECTIONS ON 2016 AND LOOKING AHEAD TO 2017

Four years of releasing this report shows that innovation mercantilism is an increasingly popular strategy in many countries, and across a growing range of tech sectors. Some key trends and takeaways are worth elaborating: that forced data localization continues to grow; that there's a vacuum in which mercantilist policies will only grow given the failure to update global trade rules as part of new trade agreements (e.g., the Trans-Pacific Partnership and the Trade in Services Agreement); that China remains the world leader in innovation mercantilism; and that other countries are emulating its approach, given the lack of consequences and a clear response from its trading partners.

To elaborate on these trends, first, data localization remains a central feature of this year's report on innovation mercantilism, as more countries resort to data localization, and some countries enact it in multiple areas. As issues around data feature in a growing range of policy issues, policymakers need to take the time to discern between the broader purpose of a law and the handling and protection of the data involved. Nothing is inherently wrong with governments arranging processes to facilitate legitimate access to data, such as for tax or law-enforcement purposes. However, it becomes a problem when policymakers focus on where data is stored rather than how it is stored and protected.

Forced data localization for telecommunications metadata is an example of this misguided approach to data protection. Policymakers remain predominantly focused on the geography of metadata storage (such as in Germany and Russia) instead of the measures for data protection (as in new metadata laws in Australia and the United Kingdom). As this report and others from ITIF have established, the notion that data must be stored locally to ensure it remains secure and private is false.[81] Regarding security, while certain laws may impose minimum security standards, the security of data does not depend on where it is stored, only on the measures used to store it securely.

This year's report shows that data localization can be both explicit (as in Vietnam, China, Russia, and elsewhere) and de facto (such as in Turkey). Obviously, a need exists for a careful balance between ensuring that data is properly protected and that privacy is protected, but this, too, can simply be indirect localization by making the process for cross-border data transfers so difficult that in practice it becomes unworkable, thereby forcing companies to store data locally. There is no "one size fits all" approach to privacy protections, as different countries have different legal and societal values and approaches to the issue. This is why various international forums emphasize making privacy regimes interoperable, so that both privacy protections and data flows can take place at the same time. Despite what some public advocates want people to believe, there is not a trade-off between transferring data overseas and maintaining data protection. What matters are the rules that travel with the data and that a company needs to abide by these rules, wherever they store the data, and that these rules are properly enforced.

Second, the cases covered in this and prior reports show that countries feel confident to enact protectionist and trade-distorting policies, since the current framework of trade rules,

including those governed by the World Trade Organization, are out-of-date, inadequate, and unlikely to result in any repercussions. Unfortunately, several important opportunities to update trading rules across major parts of the global economy failed in 2016, including through the Trans-Pacific Partnership trade agreement, the Transatlantic Trade and Investment Partnership between the United States and European Union, and the Trade in Services Agreement. The successful completion of one (or ideally all) of these agreements would have sent an important signal that key trading nations would defend the global trade system, change international norms to account for modern trade issues, and enact rules that forbid many of the mercantilist policies highlighted in this year's report. Unfortunately, the current vacuum (in terms of new rule-setting) is set to persist into 2017, given the lack of venues or vehicles that are likely to take on the challenge posed by these mercantilist policies.

Third, this report shows that China remains a world leader in innovation mercantilism: China features prominently in this year's report, as it has in past years, and as it will likely do so again in 2017. Next year's report will likely cover the outcome from the various processes underway to define and enact key definitions and rules to implement provisions of the new cybersecurity law, such as for personal information and critical information infrastructure. This captures one of the many issues with policymaking in China—that while many laws contain provisions that are clearly mercantilist, many other laws and provisions are drafted in a vague way that makes their impact uncertain. It then falls away from the limelight that is placed on new legislation to administrative bodies and government agencies that are responsible for fleshing out the vital details of these laws, which ultimately determine whether the law is pro-competition or discriminatory and mercantilist. Trading partners, such as the United States and European Union, focus on major legislative announcements in China, but then fail to sustain efforts to push back against trade-distorting policies that come through implementing agencies.

Trading partners, such as the United States and European Union, focus on major legislative announcements in China, but then fail to sustain efforts to push back against trade-distorting policies that come through implementing agencies.

China's pursuit of restrictive and discriminatory "secure and controllable" provisions is a clear example of the country's commitment to innovation mercantilism. In April 2015, China halted its first attempt to enact "secure and controllable" provisions as part of a new banking law only after the draft law provoked a fierce reaction from trading partners and foreign firms.[82] Nevertheless, the draft law sent a clear signal to the market that the Chinese government wanted Chinese financial firms to buy ICT goods and services from local firms and not foreign ones. Foreign technology companies continue to see the impact of the measure on sales in China.[83] Yet, despite knowing what the reaction would be, the Chinese government has reintroduced similar "secure and controllable" provisions in the cybersecurity law.

The push for "secure and controllable" shows that China will push its mercantilist policies as far as it can, and if it provokes a strong enough reaction, it concedes some ground but keeps most of the restrictive policies or simply shifts them to another vehicle or venue through which to achieve the same policy. This also reveals the weakness in the strategy and response by the United States, Japan, European Union, and others to only episodically

and largely individually push back on the most egregious cases of Chinese innovation mercantilism. Foreign firms and key technology trading partners celebrate the limited win as a victory, but concede or ignore the broader and longer-term trend toward a market that is ever harder for foreign tech firms to compete in. Such a strategy is too reactive, narrowly focused, and short-sighted. As ITIF argues in *False Promises: The Yawning Gap Between China's WTO Commitments and Practices,* it's time for the United States and others to work closely together to adopt a policy of "constructive confrontation" to address China's and others' innovation mercantilist practices.[84]

CONCLUSION

As innovation and trade policy have become increasingly intertwined, openness to trade—characterized by open market access, protection of intellectual property, and receptivity to foreign direct investment—has become a bedrock pillar of an effective global innovation policy system. However, this report and prior year's reports show that many countries are still more than willing to pursue mercantilist, trade-distorting, beggar-thy-neighbor approaches instead of implementing across-the-board productivity and innovation-enhancing policies.[85]

The global trading system retains the potential to be the most innovation-empowering it has ever been. However, the threat posed by innovation mercantilism is not receding. If the global trade system is to maximize innovation, all nations should strongly advocate for the correct policies while pushing back equally strongly against mercantilist policies. Pro-innovation trade policies include eliminating all tariffs on trade in high-tech products, curtailing nontariff trade barriers, strengthening digital trade, encouraging market-based competition, and protecting intellectual property. By implementing these types of policies, countries can not only engender robust and innovation-enhancing trade and investment, they can also begin to form an alliance against mercantilist practices and to demonstrate continued commitment to the principles of free and fair trade.

ENDNOTES

1. Robert Atkinson, "Designing a Global Trading System to Maximize Innovation," *Global Policy Journal* 5, no. 1 (February 2014): 57–62, http://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12120/abstract; Stephen J. Ezell, Robert D. Atkinson, and Michelle Wein, "Localization Barriers to Trade: Threat to the Global Innovation Economy" (Information Technology and Innovation Foundation, 2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.
2. 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.
3. Atkinson, "Designing a Global Trading System to Maximize Innovation."
4. 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.
5. Josh China and Eva Dou, "China's New Cybersecurity Law Rattles Foreign Tech Firms," *The Wall Street Journal,* November 7, 2016, http://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064. "China Adopts Tough Cyber-Security Law," *The Economist,* November 12, 2106, http://www.economist.com/news/china/21710001-foreign-firms-are-worried-china-adopts-tough-cyber-security-law.
6. "China Passes Controversial Cyber Security Law," *Baker McKenzie*, November 15, 2016, http://www.lexology.com/library/detail.aspx?g=d23109be-661d-4e90-a92c-32b7330e3a49.
7. The specific scope of CII will be developed by the State Council. The cybersecurity law also makes CIIs subject to the Multi-Level Protection Scheme (MLPS) for network security, but it is unclear where this refers to an existing MLPS for information security (launched in 2007) or something else. It should be noted that the definition of levels three to five of information systems under MLPS for information security is substantially similar to that of CII in cybersecurity law. Karen Ip, Nanda Lau, and James Gong, "China's New Cyber-Security Law – Highlights," *Herbert Smith Freehills LLP,* November 29, 2016, http://www.lexology.com/library/detail.aspx?g=6d37cbb0-b341-4106-87b0-40b68f138bf1.
8. In 2007, the MLPS for information security was formally launched by the Ministry of Public Security (MPS), National Administration for Protection of State Secrets (NAPSS), and the Office of State Cipher Code Administration (OSCCA), led by the State Council.
9. This MLPS classifies information networks in China according to their relative impact on national security, social order, and economic interests if the system is damaged or attacked. The classification levels range from one to five, one being the least critical and five being the most critical. A level five ranking indicates extremely significant networks, such as for military and defense. According to MLPS regulations, systems classified at level three or above must procure IT security products containing only domestic IP. "China – Information and Communications Technology Equipment and Software" (Washington, DC: International Trade Administration, May 31, 2016), https://www.export.gov/article?id=China-Information-Communication-Technology.
10. Ibid., 6.
11. The definition of what is involved is being considered by China's National Information Security Standards Technical Committee (also known as Technical Committee 260) under the Cyberspace Administration of China, which is the cybersecurity standards maker, as part of its efforts to craft technical specifications for the new cybersecurity law. Eva Dou, "Microsoft, Intel, IBM Push Back on China Cybersecurity Rules," *The Wall Street Journal*, December 1, 2016, http://www.wsj.com/articles/microsoft-intel-ibm-push-back-on-china-cybersecurity-rules-1480587542.
12. This law required domestic and foreign banks to progressively increase their expenditure on "secure and controllable" IT to reach the level of 75 percent by 2019. Paul Mozur, "New Rules in China Upset

Western Tech Companies," *The New York Times*, January 28, 2015, http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.

13. Ibid., 10.
14. The comments were made in a discussion log made public by Technical Committee 260, the national cybersecurity standards maker, as it released technical parameters of its omnibus cybersecurity law adopted on November 7. Ibid., 10.
15. Ibid.
16. Ibid.
17. "Final Cybersecurity Law Enacted in China," *Huntington and Williams*, November 8, 2016, https://www.huntonprivacyblog.com/2016/11/08/final-cybersecurity-law-enacted-china/.
18. Barbara Li, "China's New Telecom Catalogue Comes Into Force on March 1, 2016," *Norton Rose Fulbright*, February 2016, http://www.nortonrosefulbright.com/knowledge/publications/137503/chinas-new-telecom-catalogue-comes-into-force-on-march-1-2016; Jacob Parker, "US-China Business Council Comments on the Draft Cybersecurity Law" (The US-China Business Council, August 4, 2016), https://www.uschina.org/sites/default/files/USCBC%20Comments%20on%20Cybersecurity%20Law_EN.pdf; "China – Information and Communications Technology."
19. World Trade Organization Council for Trade in Services, "Computer and Related Services Background Note by the Secretariat S/C/W/45" (Geneva: World Trade Organization, July 14, 1998), https://www.wto.org/english/tratop_e/serv_e/w45.doc.
20. Stephen J. Ezell and Robert D. Atkinson, "False Promises: The Yawning Gap between China's WTO Commitments and Practices" (Information Technology and Innovation Foundation, September 2015), http://www2.itif.org/2015-false-promises-china.pdf.
21. United States Trade Representative, "2013 National Trade Estimate China" (Washington, DC: United States Trade Representative, 2014), https://ustr.gov/sites/default/files/2013%20NTE%20China%20Final.pdf; Hogan Lovells, "Third Party Payment Licenses in China - Are They Within the Grasp of Foreign Investors?" (London: Hogan Lovells, June 2014), http://www.hoganlovells.com/files/Uploads/Documents/14.06_Corporate_China_Alert_-_Third_Party_Payment_Licences_in_China_-_Are_They_within_The_Grasp_of_Foreign_Investors_SHALIB01_1093411.pdf.
22. IBM, "Made in IBM Labs: IBM to Build First Cloud Computing Center in China," news release, February 1, 2008, http://www-03.ibm.com/press/us/en/pressrelease/23426.wss; Rebecca Blumenstein, "Microsoft's Partner Strategy in China," *The Wall Street Journal,* June 8, 2016, http://www.wsj.com/articles/microsofts-partner-strategy-in-china-1465421401; SAP, "SAP and China Telecom Expand Strategic Partnership to Provide SAP Cloud Portfolio in China," news release, November 20, 2013, http://news.sap.com/sap-and-china-telecom-expand-strategic-partnership-to-provide-sap-cloud-portfolio-in-china/.
23. Leigh Ann Ragland et al., "Red Cloud Rising: Cloud Computing in China" (Washington, DC: U.S. Economic and Security Commission, September 5, 2013), http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising_2014.pdf; United States Information Technology Office (USITO), "USITO Brief: Ministry of Science and Technology 12th Five Year Plan" (Washington, DC: USITO, August 5, 2011), http://www.semiconductors.org/clientuploads/directory/DocumentSIA/USITO%20Brief%20Ministry%20of%20Science%20and%20Technology%2012th%20Five%20Year%20Plan.pdf.
24. Monika Kuschewsky, "Data Localization Requirements Through the Backdoor? Germany's 'Federal Cloud,' and New Criteria for the Use of Cloud Services by the German Federal Administration," *Inside Privacy,* September 15, 2016, https://www.insideprivacy.com/cloud-computing/germanys-criteria-for-federal-use-of-cloud-services/.

25. "Law for the Introduction of a Storage Obligation and a Maximum Storage Period for Traffic Data," *Library of Germany's Parliament,* December 10, 2015, http://www.bundesgerichtshof.de/DE/Bibliothek/GesMat/WP18/V/Verkehrsdaten.html.
26. Lothar Determann and Michaela Weigl, "Data Residency Requirements Creeping Into German Law," *Bloomberg BNA,* April 11, 2016, http://www.bna.com/data-residency-requirements-n57982069680/.
27. In 2008, Sections 113a and 113b of the German Telecommunications Act stipulated that providers of publicly available telecommunication services must store traffic data for six months. On March 2, 2010, the German Federal Constitutional Court ruled that these provisions were unconstitutional and therefore void because they violated telecommunications secrecy and privacy rights (Article 10 of the German Constitution). Furthermore, on April 8, 2014, the Court of Justice of the European Union ruled that the underlying Data Retention Directive of the EU, which the 2008 version of the German Telecommunications Act sought to implement, was invalid.
28. Ibid., 26.
29. Ezell and Atkinson, "False Promises."
30. See also: Adam Klein, Michèle Flournoy, and Richard Fontaine, "Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond" (December 2016, Center for a New American Security), https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-Surveillance-Final.pdf.
31. Ibid.
32. In the United Kingdom, see Section 92 of the Investigatory Powers Act 2016.
33. On March 31, 2016, the Indonesian Ministry of Communication and Information Technology issued Circular Letter Number 3 on "over-the-top (OTT)" services, which replicates the data localization requirement in Regulation 82/2012. Regulation 82/2012, in effect since 2012, includes requirements for source code surrender as a condition for market access and a requirement for local storage of data. In mid-2015 MICT released additional draft implementation measures, which contain more detailed requirements for protecting personal data on electronic systems, including requirements to store personal data in primary and backup data centers in Indonesia. Information Technology Industry Council, "ITI Forced Localization Strategy Briefs" (brief, Information Technology Industry Council, July 2016), https://www.itic.org/public-policy/ITIForcedLocalizationStrategyBriefs.pdf.
34. "New Rules on OTT Services in the Offing," Assegaf Hamzah and Partners, accessed December 19, 2016, http://www.ahp.co.id/client-update-27-may-2016.
35. Grace D. Amianti, "BI Working on Integrated National Payment System," *The Jakarta Post,* December 14, 2015, http://www.thejakartapost.com/news/2015/12/14/bi-working-integrated-national-payment-system.html.
36. Nivell Rayda, "When It Comes to Innovation, Joko's Ministers Need a 'Mental Revolution,'" *Jakarta Globe*, December 18, 2015, http://jakartaglobe.id/opinion/commentary-comes-innovation-jokos-ministers-need-mental-revolution/.
37. "Indonesia Gives Netflix One Month to Get Permit, Office," *Jakarta Globe*, January 13, 2016, http://jakartaglobe.id/technology-features/indonesia-gives-netflix-one-month-get-permit-office/; Resty Woro Yuniar, "Netflix Blocked by Indonesia's Top Telecom Provider," *The Wall Street Journal,* January 27, 2016, http://www.wsj.com/articles/netflix-blocked-by-indonesias-top-telecom-provider-1453896220.
38. "Telkom to Bring Netflix Rival to Indonesia," *The Jakarta Post,* March 28, 2016, http://www.thejakartapost.com/news/2016/03/28/telkom-bring-netflix-rival-indonesia.html.
39. "Law of the Republic of Indonesia No. 13 of July 28, 2016, on Patents," World Intellectual Property Organization, accessed December 19, 2016, http://www.wipo.int/wipolex/en/details.jsp?id=16392.
40. Adolf Panggabean and Jonathan Loh, "Indonesia Update: Amendments to Indonesian Patent Law," news release, Spruson and Ferguson, August 25, 2016, http://www.spruson.com/amendments-to-indonesian-patent-law/.

41. Michelle A. Wein, "Let's Clear a Few Things Up: On the Subject of Compulsory Licensing in TRIPS," *The Innovation Files*, June 27, 2013, http://www.innovationfiles.org/lets-clear-a-few-things-up-on-the-subject-of-compulsory-licensing-in-trips/.
42. Decree 1010.
43. Indonesia also assessed whether to grant these compulsory licenses in groups, and not on their individual merits, as required under TRIPS. The Pharmaceutical Research and Manufacturers of America (PhRMA), *2017 National Trade Estimate Report on Foreign Trade Barriers* (PhMRA, October 2016), http://phrmacdn.connectionsmedia.com/files/dmfile/PhRMA-2017-NTE-Comments.pdf.
44. The proposed applicant for the license tried to apply for a voluntary license first, but this was not successful within a reasonable amount of time. Applying for a voluntary license can be bypassed if there is a national emergency, other circumstances of extreme urgency, or the patent is intended for public noncommercial use.
45. Ibid., 42.
46. World Trade Organization, "Trips: Agreement on Trade-Related Aspects of Intellectual Property Rights Part II—Standards Concerning the Availability, Scope and Use of Intellectual Property Rights," available on World Trade Organization website, accessed December 19, 2016, https://www.wto.org/english/tratop_e/trips_e/t_agm3c_e.htm.
47. "Healthcare Indonesia: Boosting Local Production of Medicines' Raw Materials," *Indonesia Investments*, January 11, 2016, http://www.indonesia-investments.com/news/todays-headlines/healthcare-indonesia-boosting-local-production-of-medicines-raw-materials/item6362.
48. Marcell Sihombing, "President Demands Accelerated Development of Indonesia's Pharmaceutical and Medical-Equipment Industries," *Hukumonline.com,* July 20, 2016, http://en.hukumonline.com/pages/lt578f4f3443c34/president-demands-accelerated-development-of-indonesia-s-pharmaceutical-and-medical-equipment-industries.
49. Ksenia Koroleva, "'Yarovaya' Law—New Data Retention Obligations for Telecom Providers and Arrangers in Russia," *Latham and Watkins Global Privacy and Security Compliance Law Blog,* July 29, 2016, http://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.
50. "New Russian Legislation on Massive Telecoms Surveillance," *Jones Day Publications,* July 2016, http://www.jonesday.com/new-russian-legislation-on-massive-telecoms-surveillance-07-12-2016/.
51. Nigel Cory, "The Worst Innovation Mercantilist Policies of 2015" (Information Technology and Innovation Foundation, January 2016), http://www2.itif.org/2016-worst-innovation-mercantilists.pdf.
52. Laura Mills, "New Russian Data Laws Worry Rights Activists, Telecom Companies," *The Wall Street Journal,* July 7, 2016, http://www.wsj.com/articles/new-russian-data-laws-worry-rights-activists-telecom-companies-1467905452.
53. Ibid.
54. Ernst & Young (EY), "Tax Alert: Restrictions on Foreign Software for State Procurements" (London: EY, July 7, 2015), http://www.ey.com/Publication/vwLUAssets/EY-Tax-Alert-06-July-2015-ENG/$FILE/EY-Tax-Alert-06-July-2015-ENG.pdf.
55. Ibid., 50.
56. Maria Tsvetkova and Andrew Osborn, "Russia Starts Blocking LinkedIn Website After Court Ruling," *Reuters,* November 17, 2016, http://www.reuters.com/article/us-russia-linkedin-idUSKBN13C0RN.
57. BSA The Software Alliance, "Special 301 Submission" (industry report, BSA The Software Alliance, Washington, DC, February 5, 2016), http://www.bsa.org/~/media/Files/Policy/Trade/BSA2016Special301.pdf.
58. Ibid., 50.

59. World Trade Organization, "Continuing Solid Progress on Pending Accessions to Government Procurement Pact," news release, October 19, 2016, https://www.wto.org/english/news_e/news16_e/gpro_19oct16_e.htm.

60. Organisation for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2015* (Paris: OECD, 2015), http://dx.doi.org/10.1787/9789264232440-en.

61. Ezell and Atkinson, "False Promises."

62. "Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries," European Commission website, accessed January 5, 2017, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

63. Courtney M. Bowman, "An Overview of Turkey's New Data Protection Law," *Proskauer Privacy Law Blog,* April 15, 2016, http://privacylaw.proskauer.com/2016/04/articles/international/an-overview-of-turkeys-new-data-protection-law/.

64. Paul de Hert and Vagelis Papakonstantinou, "The Data Protection Regime in China" (analytical report for the Directorate General for Internal Affairs, European Parliament, Brussels, October 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

65. Ibid., 50.

66. Information Technology Industry Council, "ITI Forced Localization Strategy Briefs"; Banking Regulation and Supervision Agency (BDDK), "Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions," *Official Gazette*, no. 28690, June 27, 2013, https://www.bddk.org.tr/websitesi/english/Legislation/129166493kanun_ing.pdf.

67. Lance Whitney, "PayPal to Shutter Operations in Turkey Over Licensing Hurdle," *CNET,* May 31, 2016, https://www.cnet.com/news/paypal-to-close-operations-in-turkey-over-licensing-hurdle/.

68. "PayPal Is Shutting Down in Turkey," *Business Insider Intelligence,* June 1, 2016, http://www.businessinsider.com/paypal-is-shutting-down-in-turkey-2016-6.

69. US-ASEAN Business Council and Informational Technology Industry Council, joint letter to Vietnamese Minister Son, Minister of Information and Communication, January 6, 2016, http://cloud.chambermaster.com/userfiles/UserFiles/chambers/9078/File/ICT/2015/VietnamOTTCircular-USABC-ITILetterFINAL.pdf.

70. Van Ly, "Ministry Protects OTT Services," *The Saigon Times Daily,* October 25, 2016, https://www.vietnambreakingnews.com/2016/10/ministry-protects-ott-services/.

71. Van Oanh, "OTT Users Likely to Be Forced to Pay Fee," *The Saigon Times Daily,* October 25, 2016, https://www.vietnambreakingnews.com/2016/10/ott-users-likely-to-be-forced-to-pay-fee/.

72. Hoang Phuong Bui, "Vietnam ICT Market and Regulatory View on OTT Services" (presentation, Ministry of Information and Communications of Vietnam, Ha Noi, December 2015), https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/Dec-OTT/Presentations/Vietnam%20ICT%20Market%20and%20Regulatory%20view%20on%20OTT%20services%20-%20Vietnam%20PHUONG.pdf.

73. Ibid., 68.

74. Asia Internet Coalition, "Formal Comments on the Draft Decree Amending Decree 72 on the Management, Provision and Use of Internet Services and Information Content Online (Decree 72/2013-ND-CP)," letter to Vietnam's Chamber of Commerce and Industry, October 17, 2016, http://www.asiainternetcoalition.org/wp-content/uploads/2016/11/AIC-Comments-on-Decree-Amending-Decree-72-2016_10_17.pdf.

75. U.S. Department of State, *2015 Country Reports on Human Rights Practices: Vietnam* (Washington, DC: U.S. Department of State, April 13, 2016), http://www.state.gov/j/drl/rls/hrrpt/2015/eap/252813.htm.

76. Stephen Ezell, "Vietnam's Proposed Law on Information Network Security Threatens to Imperil Its ICT Economy," *The Innovation Files,* July 27, 2016, https://itif.org/publications/2016/07/27/vietnam%E2%80%99s-proposed-law-information-network-security-threatens-imperil-its.
77. Vietnam's National Assembly, Law on Network Information Security, Article 32.2.d and Article 36.2 (Hanoi: Vietnam's National Assembly, May 15, 2015), http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf.
78. Ibid.
79. For example, China's Securities Regulatory Commission regulations on information security management requests access to source code for review and testing (Article 14). Also see U.S.-China Economic and Security Review Commission, *2015 Report to Congress* (Washington, DC: U.S.-China Economic and Security Review Commission, November 2015), https://news.usni.org/wp-content/uploads/2015/11/2015-Annual-Report-to-Congress.pdf.
80. First, Vietnam could expand the Ministry of Defense's exemption from the law's business license requirement to also cover the import-export permitting requirements and second by the Ministry of Information and Communications adopting the same exemption in its own decree. Ezell, "Vietnam's Proposed Law on Information Network Security."
81. 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.
82. Gillian Wong, "China Halts Implementation of Banking-Technology Rules," *The Wall Street Journal,* April 16, 2015, http://www.wsj.com/articles/china-halts-implementation-of-banking-tech-guidelines-1429181094.
83. Eva Dou and Rachel King, "China Sets New Tone in Drafting Cybersecurity Rules," *The Wall Street Journal,* August 26, 2016, http://www.wsj.com/articles/china-moves-to-ease-foreign-concerns-on-cybersecurity-controls-1472132575.
84. Ezell and Atkinson, "False Promises."
85. Ezell, Atkinson, and Wein, "Localization Barriers to Trade."

ACKNOWLEDGMENTS

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

ABOUT THE AUTHOR

Nigel Cory is a trade policy analyst 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 one of the world's leading science and technology think tanks, 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.