The Worst Innovation Mercantilist Policies of 2017

BY NIGEL CORY | JANUARY 2018

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

Unfortunately, as the global race for market share in the digital economy and high-tech sectors intensifies, many countries continue to turn to "innovation mercantilism"—a strategy that uses trade-distorting policies to advantage local technology firms and production activities. While this modern protectionism typically relies on behind-the-border regulations, not tariffs, to protect local firms, the objective and impact remains the same—to either replace foreign goods and services with local ones or to unfairly promote exports, or both. These destructive, "beggar-thy-neighbor" tactics involve forcing companies to transfer the rights to their technology or to relocate their production, research and development (R&D), or data storage activities. Internet-based services, electric vehicles, biopharma products, and computers and electronics are common targets. In 2017, Brazil, China, Indonesia, Russia, and Vietnam headed the list of countries fielding the world's worst innovation mercantilist policies.

Innovation mercantilist practices do not just damage other economies and businesses; 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 such practices, particularly over the long run. Such policies lead countries to neglect the greater opportunity to spur greater sustainable growth over the long term by raising the productivity of all sectors of an economy, not just by spurring the growth of or creating more high-tech ones.

This fifth 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 2017. Policies were chosen based on their detrimental effects globally, so some nations have more than one policy included, due to the policy's widespread impact.

SUMMARY OF THE WORST INNOVATION MERCANTILIST POLICIES OF 2017

Data, Information Communication Technology Hardware, and Cybersecurity Policies

- **Brazil:** Brazil's Central Bank is considering a proposal to force all banks and financial firms to store financial data locally.

- **China:** Enacted a new cybersecurity law that is vague, intrusive, burdensome, and discriminatory against foreign tech firms and their goods and services. This includes extensive forced local data storage requirements, the exposure of sensitive intellectual property (IP), and discriminatory security reviews of information communication technology (ICT) hardware and software.

- **Colombia:** Enacted new data protection rules about the international transfer of Colombian citizens' personal data that will impede data flows, while the country pursues the misguided policy that countries should be responsible for enforcing the privacy regulations of foreign countries.

- **Vietnam:** Proposed a draft cybersecurity law that introduces intrusive and discriminatory "security reviews" of critical information infrastructure and a requirement for firms in these sectors to store data locally.

Internet-Based Services

- **Brazil:** Brazilian policymakers are considering a range of restrictive and discriminatory measures to over-the-top (OTT) services that distribute videos over the Internet, including discriminatory taxes and a local content requirement (for video).

- **Indonesia:** Enacted a broad, vague, and discriminatory regulatory framework for OTT Internet-based services, including forcing firms to set up a local office, hire local staff, produce local annual reports, and store data locally.

- **Russia:** Enacted a new law that includes stringent ownership restrictions that essentially precludes foreign firms from offering videos via Internet-based OTT services (or limits them to working as minor partners).

- **Thailand:** Considered burdensome, restrictive, and discriminatory regulations of OTT Services.

Electric Vehicles

- **China:** Enacted new rules that force foreign firms to transfer all the critical intellectual property needed for new energy vehicles (EV) to local partners as a condition for market access.

THE NATURE OF INNOVATION INDUSTRIES

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 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 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. 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.

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.

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.

Finally, innovation industries depend more than other industries on intellectual property, 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, both at the enterprise and 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 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 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's in this context that innovation mercantilist policies are so problematic, for relative to mercantilist policies affecting other industries (e.g., clothing, dairy, or lumber), the global economic damage from innovation mercantilist policies is 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 far worse adverse consequences. First, they can raise the cost of key capital goods, such as for information and communications technology products. This reduces capital-goods use by industries throughout an economy, thus 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; this undermines the global economic order. Seventh, and perhaps most importantly, they lead to unbalanced and unsustainable "dual economies," with weak productivity growth in non-favored sectors.[5]

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 countries' economic development strategies, which should include investments in education, research,

and physical and digital infrastructures, along with robust levels of 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 needs to do much more to push back against other nations' innovation mercantilist policies.

THE WORST INNOVATION MERCANTILIST POLICIES OF 2017

The following innovation mercantilist policies are just a sampling of unfair trade practices that nations proposed, drafted, or implemented in 2017 and that the global trading system needs to address as a top priority. The cases are grouped by key sector/topic.

Data, Information Communication Technology Hardware, and Cybersecurity Policies

Brazil: Cybersecurity Proposal Forces Firms to Only Store Financial Data Locally

The Central Bank of Brazil is considering a misguided and costly cybersecurity proposal that would force financial firms to store all data locally and to provide authorities with access to their datacenters. As ITIF outlined in a submission to the Central Bank of Brazil, the proposal raises a number of major concerns for both Brazil's (and the broader global) financial sector, not to mention Brazil's potential to develop into a data-driven economy.[6]

The Central Bank of Brazil is considering a misguided and costly cybersecurity proposal that would force financial firms to store all data locally and to provide authorities with access to their datacenters.

In September 2017, the Central Bank of Brazil released a proposal (57/2017) on cybersecurity policy and requirements for contracting processing, data storage, and cloud computing services for financial institutions and other institutions authorized to operate by the Central Bank of Brazil. The main issue is that the cybersecurity proposal would force firms to store their data locally (article 11). There are also concerns with its requirement for firms to indicate where the actual data centers are located (article 12:1); and regarding its requirement for cloud companies to provide the Brazilian Central Bank with physical access to the data centers (article 12:7).

At the heart of the proposal's focus on geography is the mistaken belief that data must be stored domestically to ensure that it remains secure, private, and accessible to government. This is false. With regard to security, while certain laws may impose minimum security standards, the commercial security of data does not depend on where data is stored, only on the measures used to store it securely. As ITIF writes in "The False Promise of Data Nationalism," data localization mandates do not increase commercial privacy or data security.[7] What matters are the technological and procedural methods of storing and transferring data when determining how safe data is, not the geographical location where data are stored.[8] A secure cloud server in Colombia is no different from a secure cloud server in Brazil.

The proposal's focus on locating data centers in Brazil and on providing the Central Bank with physical access to data centers is similarly mistaken. From a prudential oversight perspective, what should matter is how a firm or its cloud supplier manages its IT and data managements systems, how it provides the Central Bank with information on this as part of prudential reporting, and that it can provide timely access to data requested by the

Central Bank (as part of the latter's oversight activities). The proposal should focus solely on those provisions that provide the legal framework so that the Central Bank has confidence that financial firms are properly managing their data and that, if need be, they can provide data upon request.

The draft proposal's focus on geography would negatively affect Brazilian firm competitiveness and productivity, and would actually raise potential cybersecurity risks. Financial firms, and the sector as a whole, would become less competitive as the rules would potentially cut them off from accessing cheaper and better global cloud-service providers. This would ripple throughout the Brazilian economy by reducing productivity, as any increase in financial firms' IT costs would likely be passed onto users, whether these are individuals, companies, or the government. From a cybersecurity perspective, the local data storage requirement may force financial firms to use local cloud services that are not best-in-class in using the latest protective measures. Furthermore, forcing international firms to store data locally may also increase cybersecurity risk as it forces firms that operate across multiple countries to spread their data across more data centers—thus losing the benefits of centralized and more effective management oversight.

The provisions in the Central Bank's proposal could be particularly damaging as data, and the ability to move it freely, is critical to modern finance. Personal and corporate finance have been revolutionized by the Internet. Users can easily access online financial services to engage in e-commerce, such as to buy physical or digital goods and services. A tourist can use a credit card overseas and use the Internet to log onto their financial institution to check on the payment. In this way, financial services are a critical facilitator of the entire modern economy. At the international level, for international financial firms, the free flow of financial data is critical. They rely on the free flow of digital information to support customers and operations in virtually every sector of the economy in countries all around the world. For example, Citibank's global banking operations show the importance of the global free flow of data. More than 60 percent of Citibank's customers—it has over 200 million customer accounts—conduct banking online. These processes are facilitated through 20 regional data centers, which are purpose-built using servers, storage, and networks that are environmentally controlled and highly secured to provide the highest-possible resilience for the bank's services and customer support.[9]

Finally, the impact on financial data will negatively affect Brazil's broader digital economy.[10] While Brazil's digital economy is large, growing, and holds enormous promise, it has a long way to go to catch up to countries at the frontier of digitalization, and provisions in this proposal could hold it back further. There is an opportunity cost associated with countries that limit their participation in the global digital economy through policies such as the local data storage requirements in this proposal. A McKinsey study examined the size of this unrealized opportunity by calculating the value that countries realized by increasing participation across a range of data flows relative to the size of their economies from 2003 to 2013 (the latest year for which there are global data for all flows). Brazil could have added some $1.4 trillion to its GDP over the past ten years,

making its economy 60 percent bigger by 2014, by accelerating its participation in all types of global data flows.[11] Adding a local data storage requirement for financial data would only add to a lamentably long list of policies holding Brazil back.

China: Enacting a Wave of Discriminatory Digital Trade Barriers

In 2017, China ramped up its use of cybersecurity "reforms" to add further trade-distorting and discriminatory restrictions on how foreign firms, especially those in digital and other high-tech sectors, can compete in China.[12] While past versions of this report show that China is already a world leader in digital protectionism, what's different in this year's report is the scale, speed, and number of policies that affect digital and technology trade. This highlights the (largely unimpeded) momentum China has achieved in comingling trade-distorting and discriminatory industrial policy with cyber and national security policies (which also entail ancillary political and social goals). As a senior director of Microsoft's legal division noted at a recent Wilson Center event: "I have been working with international cybersecurity policy issues with various government[s] and I have never seen a country that took such [an] aggressive approach to really begin…rapid development of its legislation and policies in a very short amount of time."[13] To be sure, all nations have a right and responsibility to strengthen cybersecurity, but most nations do so in ways that are not trade-distorting and mercantilist in spirit and effect. But Chinese government officials are well aware that the growing concerns over cybersecurity allow them to advance their innovation mercantilism policies under this guise. The summaries below outline some of the trade-policy implications of these recent laws.

In 2017, China used cybersecurity reforms as a vehicle to add further trade-distorting and discriminatory restrictions on how foreign firms and their goods and services can compete in China.

China's Cybersecurity Law

On June 1, 2017, China enacted a new cybersecurity law that comingles new cybersecurity rules with discriminatory industrial policy. *The Economist* aptly described this overarching law as a "techno-nationalist Trojan horse."[14] The cybersecurity law provides a broad framework for China's government to discriminate against foreign tech firms and their products and otherwise distort the trade in IT hardware and the flow of data that underpins a broad range of trade and economic activity. This law and its many component regulations will have a major impact on China's digital economy and the increasingly restricted space for foreign firms, technology, services, and data flows.[15] During the public feedback process for this law, a Chinese government official made the protectionist intent clear in explaining how the Chinese government should use the cybersecurity law's requirement for "secure and controllable" technology as a disguise to discriminate against foreign technology products and thus help "domestic production."[16]

The cybersecurity law and its related policies show that China wants the local storage of data to become the default setting, and transfers the exception. The cybersecurity law requires a broad range of firms in sectors deemed "critical information infrastructure" (detailed below) to store personal information and "important data" only in China.[17]

China's efforts to explain what is "important data" has done little to allay concerns of foreign firms and policymakers that data so defined will be strictly national-security related. This is a tough ask as the law states that it applies to a range of commercial data (as the law

outlines that it covers data related to industry operations, business strategy, investment and development), as well as personal information (which includes private individuals' e-commerce account information, and financial and credit data).[18] Officials tried to explain that important data is "that concerning the state," not data related to businesses and individuals, except that the law also applies to data that is closely related to (vague and undefined) national security, economic development, and social and public interests.

Further evidence of the preference for local storage, the law requires firms that manage data in the context of this confusing array of data types to undergo a "security assessment" when they want to transfer relevant data overseas, which can only be done if it is "necessary for business needs." Officials tried to clarify that the security assessment is to determine if the transfer of data does not "endanger national security or social and public interests," the meaning of which, like many parts of this law and related policies, remains unclear. Draft guidelines on data transfers outline that the security assessment requires firms to assess the lawfulness and appropriateness of the data export and the level of risk involved in the transfer (given the type and sensitivity of data, how the recipient protects the data, and the political and legal environment of the recipient country).[19] Given China's track record in discriminating against foreign firms in order to support local technology firms, it's hard to see Chinese policymakers clarifying and revising these vague and burdensome rules so as to allow the free flow of data.

Draft Circular on Measures for the Assessment of Personal Information and Important Data Exit Security

On April 11, 2017, China released a draft circular on Measures for the Assessment of Personal Information and Important Data Exit Security that will expand the scope of data localization and inhibit the seamless collection, use, and transfer of data.[20] For example, the circular allows the transfer of relevant data overseas only if there is a business need to do so, whereas modern businesses transfer data as a matter of course. Regulations that unnecessarily impede data transfers will affect business competitiveness. Furthermore, the circular subjects any potential data transfers to a "self-security assessment." The circular requires companies to report on specific and technical details about the amount, scope, type, and sensitivity of the data and provide details about the specific recipient and the potential for such transfers (as mentioned above) to affect "national security, social, and public interests."[21]

The circular's focus on the location and control of data and not on outcomes (whether this is privacy- or cybersecurity-related) reinforces China's broader approach to using technology policy for mercantilist ends. However, by increasing the cost and complexity of data management and cross-border transfers of data, the circular will not only discriminate against foreign firms, it'll also undermine China's ability to benefit from data-driven innovation.

Draft Circular on Critical Information Infrastructure Security Protection Regulations

On July 10, 2017, China released a draft circular on critical information infrastructure (CII) that constitutes a broad, vague, and intrusive network and information security

regime with potentially major trade implications.[22] It potentially covers large parts of the economy, given that its definition of CII covers areas including finance, energy, transport, telecommunication networks, broadcasting networks, Internet and other information networks as well as organizations providing cloud computing, big data, and other large-scale public information network services. This list could grow even further as the draft circular provides each government department with discretionary authority to identify and list CII within their respective sectors.[23] It's clear that many of these sectors don't have direct connections to national security in the traditional sense, suggesting that China is advancing these policies less for security reasons and more out of political, social, and industrial interests.

Just as concerning are the potentially onerous, intrusive, and discriminatory security measures that firms in these sectors will need to follow. For example, the circular requires all firms to operate these functions in China, and should overseas support be needed, firms should notify Chinese regulatory and security agencies. This measure also uses the concept of a "multi-level protection scheme," which in past versions discriminated against foreign products and required forced intellectual property transfers.[24]

This draft measure on Critical Information Infrastructure reiterates the cybersecurity law's requirement for data localization of personal information or important data.

This measure reiterates the cybersecurity law's requirement that firms in CII sectors store personal information and important data generated during operations in China. Reinforcing the use of this policy to force the "localization" of data-related processes is the requirement for the "operation and maintenance" of CII to take place on Chinese territory. Furthermore, the draft circular's broad definition of network infrastructure and information systems is actually based on ownership, not geography, meaning it could be used to force a broad range of firms (such as ones doing research and development work related to chemistry, food, and pharmaceuticals, for instance) to relocate network and IT operations to China.[25]

China Enacts Security Review Measures for Network Products and Services

China's new cybersecurity law (re)introduces a range of intrusive and potentially discriminatory inspection measures—the concept of "secure and controllable"—for all important network products and services purchased for networks and information systems that are pertinent to "national security." China has not clearly defined many of these terms and processes, but we see from accompanying laws and know from past attempts at enacting similar provisions that they are likely to discriminate against foreign firms and their products and services.

Most critically, all firms in CII sectors will need to have their systems pass cybersecurity inspections to see if they are "secure and controllable." This concept, along with its analogous "independent 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.[26] Despite foreign pressure (which has to be continuously and consistently applied if it's too be effective) China is once again trying to apply these discriminatory "secure and controllable" concepts.

Since the cybersecurity law came into force, subsequent implementing documents have not narrowed the potential scope and severity of these security reviews, nor added much transparency to the criteria and process involved. On May 27, China released a draft guideline for these cybersecurity reviews, which outlined a few specific criteria for the review of goods and services, most of which remain undermined under the final catchall criterion: "other risks that may endanger national security."[27] This final criterion essentially provides China with the discretionary authority to pursue its broad definition of national security however it deigns to do so.

China's Draft Encryption Law

On April 13, 2017, China released a draft encryption law that opens up the potential for discriminatory and trade-distorting action in an area that is increasingly crucial to the competitive position of foreign tech firms.[28] It overlaps with the cybersecurity law in that it requires firms in CII sectors to get their encryption products run through a national security review if the use of these products affects China's already vague and broad definition of national security.[29]

The law allows Chinese government agencies to force foreign telecommunications companies and Internet service providers to provide "decryption technology support" for national security and law-enforcement purposes and maintains that such cooperation must be kept secret.[30] As Canada, the European Union, Japan, and the United States highlighted in comments about the draft law at the WTO, this broad, vague, and intrusive draft law could be highly trade-restrictive on ICT products as it gives the Chinese government the arbitrary ability to discriminate against foreign IT goods and services (e.g., simply because they're foreign).[31]

Furthermore, the draft law could be used to force foreign firms to expose sensitive and protected intellectual property as part of any security review; such property could then be passed on to Chinese competitors.[32] This is a major problem for leading tech firms in China as encryption stands at the forefront of competition in IT goods and services. Encryption underpins the security of digital financial processes, mobile devices, and connections over the Internet. However, the source code at the heart of software is susceptible to theft and replication, explaining why firms are so concerned given China's track record in actively or tacitly supporting the theft of cutting-edge intellectual property and passing it on to Chinese firms (in order to support industrial-development goals).

This draft law is the most recent in a long line of Chinese policies that demonstrate the country's use of encryption policy as an industrial- policy tool, much as it does elsewhere in using differential standards to support Chinese technology firms and products.[33] Indeed, the law builds on already-existing policies that allow unannounced inspections and access

to encryption keys and source code.[34] China has attempted to deflect criticism of its policies by claiming that they are in accordance with "international common practices," such as those in the United States and United Kingdom.[35] Yet that's manifestly nowhere near the case.

Tying It All Together–Industrial, Cyber/National Security, and Foreign Policy

China's cybersecurity policies will have a wide-ranging impact on trade. China knows this, and despite commitments it made in its WTO accession, China's overt use of discriminatory and trade-distorting policies continues nonetheless.[36] These policies also breach commitments China made at the 2016 U.S.-China Strategic and Economic Dialogue, where it agreed to make cybersecurity policy for commercial tech sectors narrowly tailored, non-discriminatory, and WTO-consistent, while also taking into account international norms and not imposing nationality-based conditions or restrictions on the purchase, sale, or use of ICT products for commercial purposes.[37]

The trade policy implications of these policies dovetail with China's strategic, well-financed, and advanced efforts to dominate a range of high-tech sectors and to develop "local champions" in each of them.

The trade policy implications of these cybersecurity plans dovetail with China's strategic, well-financed, and advanced efforts to dominate a range of high-tech sectors and to develop "local champions" in each of them. Chinese products may lag slightly behind those of their Western competitors, but there are now close approximations in the domestic market—Huawei for Cisco; Inspur for IBM; Xiaomi for Apple; and Kylin for Microsoft, for example.[38] China has made its drive for local production clear in its Made in China 2025 Strategy, which provides a roadmap to achieve specific targets for domestic production by Chinese firms in everything from semiconductors, ICT equipment, software, robotics, aerospace, and electric vehicles, to advanced manufacturing.[39]

Even if China releases revised drafts and implementing regulations—that clarify some rules and processes and address some of the more-severe provisions—it will still leave intact a vast policy framework that disadvantages foreign firms and allows the Chinese government to control data and the technology used in many parts of the economy. China could misuse these cybersecurity (and other similarly intrusive laws) in a number of ways: to access and copy valuable intellectual property as part of certification audits or inspections; to use the threat of punishment under these laws to coerce foreign companies to transfer intellectual property to their Chinese JV partners; and to leverage the rules' vagueness to exclude foreign tech products from many sectors of the economy on account of their alleged "insecure and uncontrollable" status.[40]

Fears that China will use the law in these and other ways are well founded given China's track record of restricting market access to suit industrial-policy aims. Indeed, foreign companies are rightly worried. A 2017 U.S.-China Business Council survey of its members found 82 percent were concerned about China's cybersecurity and IT security policies, especially the loss of sales due to national security and protectionism (31 percent), the inability to use global IT solutions in China (55 percent), and restrictions on cross-border data flows (65 percent).[41] Furthermore, a EuroCham survey showed that 13 percent of

respondents had recently deferred R&D investment in China or had become unwilling to set up R&D operations after Internet restrictions increased in early 2015.[42]

What we haven't yet seen is an equally strategic, comprehensive, and consistent effort by the United States in concert with others, such as the Europe Union, Japan, and South Korea, to push back against China's ongoing efforts to ignore or undermine key rules and principles of the world trading system. However, there are signs that a more coordinated approach may be finally emerging.[43] While China is very good at disguising trade-distorting policies, it should be clear for others to see where it's going and how it's planning on getting there—China continues to publish its strategic aims, as it has for many years. It's just that China's trading partners haven't devoted similar attention, resources, and prioritization to ensure that China's tech policy rules are non-discriminatory and non- or least-trade-distorting and that its economy is driven by market, not state, dynamics. The Trump administration would do well to prioritize this issue and change course from the, frankly, failed approaches of past U.S. administrations.

Colombia's new data privacy rules will impede data flows, while pursuing the misguided policy that countries should be responsible for enforcing the privacy regulations of foreign countries.

Colombia: Follows Europe's Misguided Approach to Global Data Flows and Privacy Protections

In August 2017, the Superintendency of Industry and Commerce (SIC)—the agency responsible for setting and enforcing data protection regulations in Colombia— issued new rules about the international transfer of Colombian citizens' personal data that will impede data flows, while pursuing the misguided policy that countries should be responsible for enforcing the privacy regulations of foreign countries.[44]

In general, Colombia's data privacy laws prevent businesses from transferring personal data outside the country without the permission of users. However, the exception to this rule is that businesses can transfer data without the permission of users to countries found to provide an "adequate level" of protection, which can never be lower than those established by Colombian privacy law.[45] This adequacy requirement copies the European Union's flawed approach to data protection in that it tries to make foreign countries enforce Colombian data privacy standards, instead of using domestic regulators to hold companies responsible for any breaches of Colombian data privacy laws—regardless of where the company stores the data.

The list of countries that SIC has deemed adequate included Costa Rica, Iceland, Mexico, Norway, Peru, Serbia, South Korea, the United States, the European Union member states, and the countries granted adequacy by the European Commission.[46] An earlier draft of the regulation released in February 2017 had omitted the United States from the list of countries providing an adequate level of protection.

By copying the European Union's approach, Colombia has signed up to an untenable and impractical approach to governing data privacy and global data flows. The EU's own process and criteria for assessing "adequacy" is not clear, nor is it comprehensive, covering a disparate collection of 11 countries—from Israel to the Faeroe Islands, Guernsey to the Isle

of Man. (Data transfers to the United States are covered separately by the EU-U.S. Privacy Shield, although this remains threatened by legal challenges in the European Union.)

Both Colombia and the European Union's approach are misguided in thinking that this country-by-country assessment is effective in promoting better data privacy and protections in companies that manage the personal data of the country's citizens.[47] This top-down approach is ultimately untenable, as not every country considers privacy in the same way due to differences in social, cultural, and political values, norms, and institutions. For example, it's inconceivable that China would ever be deemed "adequate" from a European perspective given the country's approach to data protection and privacy.[48]

The reality is that data can be safely stored almost anywhere and that inadequately secured data is not safe anywhere, at home or abroad. This goes without even mentioning that the most likely primary destination of much of this data is the United States, where, irrespective of legal differences, de facto privacy protections "on the ground" are arguably stronger than in much of the world, including in Europe.[49]

The "adequacy" standard in Colombia should instead be replaced with a duty-of-care provision. When it comes to handling data, companies doing business in Colombia 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 stating that companies that do business in Colombia (and thereby have a legal nexus there) are legally responsible for any failure to protect the personal data of Colombian citizens, regardless of whether that failure is the fault of the company in Colombia, or of an affiliate or business partner in another nation. In other words, Colombian protection would travel with the data, regardless of where that data travels. Companies doing business in Colombia would then have a strong incentive to insist that their business partners outside of Colombia adhere to the country's privacy protections, because Colombian citizens and the government could seek remedies from companies in Colombia for any privacy violations.

This is what most nations do, after all. For example, the United States does not have an "adequacy"-based system, but companies in the United States need to enact proper data-protection measures and safeguards when processing data outside the United States, 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. For example, Colombian 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 Bogota. And, if a company's affiliate in Bogota violates HIPAA, then U.S. data authorities can bring legal action against the Colombian company operating in America.

Ironically, the new data protection rules, and parts of existing law, align with this view that protection should travel with the data and that companies in Colombia remain legally responsible for that data's protection. A 2015 SIC decree on accountability holds that a data exporter owns the risks to others associated with all data-processing phases, including

movements of data across borders.[50] These companies thereby need to undertake due diligence to mitigate risk when moving data—which is ultimately what should matter to data-protection authorities.

Vietnam: New Cybersecurity Law Introduces Vague, Broad, and Burdensome Restrictions on Data, the Internet, and ICT Hardware

On June 6, Vietnam released a draft "Law on Cybersecurity" that outlines a vague and potentially burdensome and discriminatory framework that affects the role of data, ICT hardware, and the Internet in Vietnam. If enacted, these new cybersecurity requirements will make it harder for foreign technology companies to operate in Vietnam's digital economy.[51] Like China's cybersecurity law, Vietnam's draft law goes well beyond technical cybersecurity issues in mixing digital protectionism with other social/political goals.

Vietnam's new cybersecurity law goes well beyond technical cybersecurity issues, much like China's does, in mixing digital protectionism with social/political goals.

Vietnam's conceptualization of cybersecurity uses a broad definition to set out a burdensome set of responsibilities for firms that manage data and information services. The provisions cover information systems deemed to be "critical to the national security," including those that are used in state-sponsored industries, those "affecting the national sovereignty, interests, and security," and those "seriously affecting the social order and safety," among others (referred to herein as "Critical Systems").

At the heart of this cybersecurity bill is a broad, vague, potentially intrusive, discriminatory, and trade-distorting security review regime for ICT hardware. It allows Vietnam's Ministry of Public Security (MPS) to establish cybersecurity standards for critical systems and to audit them, including by analyzing data derived from the system and to implement "technical solutions and professional operations" for any perceived deficiencies.[52] Local and foreign firms don't yet know the extent of the law's impact—in terms of it acting as a technical barrier to trade—as the draft law doesn't outline the criteria and steps involved in this review, only that the goods and services used in critical systems be reviewed by MPS or by an organization authorized by MPS.

Vietnam uses the draft cybersecurity law to introduce several new localization requirements for firms involved in information, the Internet, and telecommunications services. Under the law, firms in this broad range of sectors need to obtain a license and to set up local offices in order to be allowed to operate.[53] Foreign tech firms are most affected by this rule given they tend to use the Internet and other business units and third-party services based outside of Vietnam as part of daily operations in the country as this allows them to avoid the cost and complexity of setting up a physical office in the country. This potentially means that all Internet-based services, such as Skype, Facebook, Amazon, and others that target the Vietnamese market will need to set up a local office, otherwise face the threat of criminal charges.

Vietnam's already extensive list of data-flow restrictions grows longer still under the draft law as it requires local data storage for all data used in the vague and broad "information systems critical to the national security" category.[54] In relation to data localization, the two key provisions of the cybersecurity law are:

- Article 34 (4) states that "Foreign enterprises, when providing telecommunication and/or internet services in Vietnam shall … locate their representative offices and services in which Vietnamese users' data are administered in the territory of the Socialist Republic of Vietnam, secure user information and users account information and sanction violations stringently under legislation."
- Article 48 (4) states "When collecting or creating personal information and critical data, to store the same within the country. Where it is obligatory to provide any information out of the country, to assess security levels as regulated by the Ministry of Public Security or in accordance with legislation where it provides for this."

Foreign firms and business associations have highlighted the negative impact the draft law will have on Vietnam's economy, yet revised drafts of the law retain the key measures outlined above.[55] The draft cybersecurity law shows that mercantilist, political, and national security interests in Vietnam's government have trumped those that recognize the importance of data flows and an open, dynamic, and competitive tech sector and digital economy. Similar to China, Vietnam's new cybersecurity law expands upon existing information and content control laws by outlining a vague, and onerous framework to identify and remove a broad range of illegal content online, including for political and social reasons.[56]

The overriding emphasis on censorship and state control of data and ICT systems shows that MPS has prevailed in Vietnam's internal debate with reform-minded officials from economic and trade agencies (like those involved in the Trans-Pacific Partnership (TPP) trade agreement). Furthermore, the spirit and many provisions of the draft law run directly counter to those of the e-commerce chapter in the revised TPP trade agreement (relabeled the Comprehensive and Progressive Agreement for TPP), which prohibits data localization. The irony is that Vietnam positioned itself (through the TPP and other policies) as a global ICT manufacturing hub, in part as an attractive alternative to China, where rising costs and similar discriminatory policies have changed many firms' calculus about being in China. Yet these provisions may have the same effect in Vietnam. Vietnam should reconsider its approach to cybersecurity as this draft law takes the country's digital policies in the entirely wrong direction.

Internet-Based Services

Brazil: Targeting Online Video Services

Brazil is moving to enact a range of restrictive measures to over-the-top (OTT) services that distribute videos over the Internet. On May 18, 2017, Brazil's National Agency of Cinema (known as Ancine) proposed regulations for all OTT platforms that offer videos on demand (VODs), regardless of where they are based, including periodic reports on content, users, and revenue; a 20 percent local cultural content requirement (specifying that half of this should be independently produced); and a requirement that companies make an annual investment in local production (up to 4 percent of revenue).[57] Ancine also flagged that future regulation should include other online video platforms, such as YouTube.[58]

Ancine's proposals are partly in response to the arrival of major streaming services in Brazil, such as Netflix in 2011, which has provoked a reaction from pay-TV operators who want a "level playing field" with OTT service providers.

Ancine's director bases the need for mandatory national quotas, established across Brazil's film sector in 2011, on having to counter the fact that international productions are cheaper as they're able to spread their costs over many markets.[59] Highlighting the focus on local content, Ancine's director has stated that regulations should be used to drive private investment in local production and distribution of Brazilian content.[60] On November 2, 2017, Ancine's director said that the agency will push ahead with plans to ask Brazil's Congress to approve a platform-specific law for VODs that would include a minimum local content requirement and a tax for OTT services.[61]

Ancine's misguided efforts to target VOD platforms are partly based on efforts to extend a pre-OTT tax that exists for films in Brazil. Ancine charges a tax on the production, licensing, and distribution of videos in Brazil (regardless of economic results). The tax differs depending on the film's runtime and the type of video (it's a lower tax for local films and TV shows).[62] Ancine wants to extend this tax to VOD content, which would see the government charge VOD platforms a fee for each product in their Brazil catalogue lasting more than 50 minutes. The tax would also be discriminatory as the rate would be higher for foreign vs. local productions.[63]

The regulations will negatively affect the many Brazilian consumers who have flocked to VOD services, which together form a large and growing market that could incentivize OTT firms to invest in more service innovations and local content. In 2016, nearly half of Internet users in Brazil watched VOD.[64] In August 2016, a survey of Brazilians showed that over 80 percent had used YouTube to watch movies or TV shows, while 71 percent had used Netflix, followed by local players Globo and SBT.[65] The popularity of VODs in Brazil is clear, with the revenue generated by the sector growing from $74.6 million in 2010 to $398 million in 2015. This makes Brazil the largest VOD market in Latin America and the eighth-largest in the world.[66]

Brazilian policymakers should avoid hasty, unnecessary, and misguided taxes and regulations lest they undermine Brazil's growing VOD market, where an increasing number of firms compete on the basis of price, offerings (both local and foreign), and services. Extending the film industry tax to OTT services would undermine the business model for all VOD OTTs. First, it would encourage them to significantly reduce the number and variety of titles to reduce their taxes. Second, it would affect consumers as any tax and cost increases would inevitability be passed on, which would likely undermine this growing sector.[67] This in turn would reduce overall rates of broadband adoption in Brazil (a key reason people adopt broadband is for access to VOD).

The new law's focus on a minimum content mandate also threatens to undermine the price and services available to Brazilian consumers by driving up the cost of market entry, especially for smaller platforms. Netflix's experience in Brazil provides some insights into

how quickly this sector has changed and how hasty regulations pose a problem. By coincidence, in 2011, Brazil became a testing ground for Netflix's subsequent global expansion, being its first international market at the time. Between 2013 and 2016, Netflix doubled its offering of national titles in Brazil. Furthermore, Netflix become a platform to showcase content from the region: in 2016, more than 45 percent of Netflix users outside Latin America consumed content from the region.[68] Furthermore, in March 2017, HBO Brazil (which has a regional production center in Brazil) announced 14 original Brazilian productions—its largest set of productions for a single year in Brazil.[69]

Indonesia wants to use discriminatory and trade-distorting regulations to "level the playing field" between traditional telecommunications operators and new Internet-based services.

These developments highlight the opportunity global platforms like Netflix and HBO present and show why Brazilian policymakers should look to incentivize, not mandate, local investments (such as through co-production measures), which can then use these local, regional, and global platforms to access broader international markets. Brazil's VOD market is rapidly growing, and if Brazilian consumers really want to view more Brazilian-oriented content, then Brazilian content producers (or even international providers) should recognize this and provide this content. If that's not sufficient for Brazilian policymakers, then they could consider subsidizing the production of additional Brazilian-produced and oriented-content, but they should not resort to a policy of mandating showing certain percentages of local content.

Indonesia: Adds Further Discriminatory and Restrictive OTT Regulations

On October 15, 2017, Indonesia enacted regulations for over-the-top (OTT) Internet services that expand the range of burdensome and discriminatory policies considered in 2016.[70] As initially outlined in last year's report, Indonesia wants to use discriminatory and trade-distorting regulations to "level the playing field" between traditional telecommunications operators and new Internet-based services.[71] Indicative of this, the revised draft calls for the protection of telecommunications operators as an explicit objective and implements "fair distribution" for telecommunications.

There are many vague and potentially troubling parts of these revised provisions. For example:[72]

- The provisions will introduce a burdensome regulatory regime over a potentially vast section of the Internet given it defines OTT providers as those in two broad categories: providers of Internet-based application services and those of Internet-based content services. This presumably covers both free and subscription/fee-based services. Previous versions of this regulation elaborate on the broad range of services covered: communications (video calls, emails, instant messaging services), financial transactions, data storage, search engines, social networks, and platforms that deliver content (such as for music videos and games). This means it would apply to Google search and Gmail, PayPal, Skype, Amazon Web Services, Facebook, Spotify, and local variants of these services. The potential application of new regulations to millions of phone apps alone (never mind other services) shows the impractical reach of these new regulations.

- The regulation then adds the impractical goal of trying to force foreign firms within this vast range of sectors to set up a permanent physical presence in Indonesia, including a local office and employees, as a condition of market entry.
- The regulation effectively tries to install the Indonesian government as a gatekeeper of the Internet by including the requirement that foreign OTT firms apply for a license to offer services in Indonesia. This application would include details about their local presence, such as their local tax identification number, the details of their information contact center, and their business license. This impractical (and nearly impossible) requirement effectively tries to pre-empt the launch of new Internet-based being offered in Indonesia.
- The regulation intervenes in how OTT firms operate by forcing them to use Indonesia's national payment "gateway" for processing electronic payments (such as ATMs, credit cards, and electronic money), which includes only using a "switching agency" that is at least 80 percent Indonesian-owned. Besides being discriminatory, this provision raises concerns about whether these local switching agencies have the expertise and capability to ensure secure and timely transactions.
- Foreign OTT firms must provide user guides in Bahasa Indonesian.
- OTT firms must set up a local bank account to manage all services in Indonesia.
- OTT firms must have an information contact center to manage questions and complaints from customers, which must be responded to within 48 hours. The details for this contact center must be provided with a firm's application for a license.
- OTT firms must submit an annual report to the Ministry of Information and Communications, including providing information on their number of subscribers in Indonesia.
- OTT firms that do not comply will be blocked by Indonesian telecommunications companies. Full and effective enforcement would have an extensive impact. Given the broad range of sectors covered and the need for OTT firms to get pre-approval from the government before offering services, enforcement would effectively require the Indonesian government to exert control over the country's Internet.

Furthermore, these rules will affect Indonesia's broader digital economy in how they categorize and treat certain types of data. The Indonesian government defines three categories of data:

- Strategic (intended for security, intelligence, national IDs, and military data).
- Important (data must be accessible to law-enforcement agencies within a few days when requested).
- Low (no requirements).

However, there is potential for significant uncertainty as to how OTT firms should manage certain types of data and whether different government agencies will take different and

conflicting approaches to certain types of data. Which category data falls into is significant. Strategic data refers to data intended for the government. Strategic data must be stored only locally, while important data can be stored and processed outside of Indonesia. While commercial data will likely fall in the important or low data categories, the new rules will allow individual regulators to follow their own categorization of data, meaning that government agencies may differ in how they categorize and treat categories of commercial data. While Indonesia's national police have reportedly not pushed for local data storage (simply that data be available upon request), there is uncertainty about this and whether other government agencies (such as the Financial Services Authority of Indonesia) will push for local data storage in their respective areas of responsibility. Likewise, there is uncertainty as to how agencies classify "Indonesian ID" data (which is strategic data) and whether this covers Indonesia's electronic identity card (known locally as the e-KTP). Furthermore, it is unclear whether this also includes broader personally identifiable information, which companies collect and use on a daily basis, such as for social media and online banking.

On top of this new regulation, Indonesia is enacting a new fiscal policy to target OTT firms in an effort to extract excess taxes from the digital economy. In April 2017, Indonesia's Director General of Tax released a new law (Circular Letter No. SE-04/PJ/2017) that forces OTT firms to create a "taxable" physical presence in the country.[73] In this way, forcing a foreign OTT firm to set up a local presence just because it has users in Indonesia is much the same as forcing a foreign manufacturer to set up an office if it happens to have customers in Indonesia who import its products. In doing so, Indonesia's efforts to force Internet-based firms to establish a physical presence runs counter to the emerging international consensus on how to tax the digital economy, such as reflected in the OECD's Base Erosion and Profit Shifting (BEPS) project.

For example, a key takeaway from the OECD/G20 report "Addressing the Tax Challenges of the Digital Economy" (prepared for BEPS) is that because the digital economy is becoming an economy in and of itself, it would be difficult, if not impossible, to ring fence the digital economy from the rest of the economy for tax purposes.[74] Yet, this is exactly what Indonesia is trying to do. As the OECD/G20 BEPS Taskforce on the Digital Economy outlined, a better approach would be for countries to subject cross-border business-to-consumer digital services to national value-added taxes (VATs).

Together, Indonesia's OTT policies would essentially fragment a central feature of the Internet and potentially limit Indonesian firms and citizens from using global Internet services. The impact will be especially hard on small firms as they don't have the time, expertise, and resources to deal with such vague, expansive, and expensive regulations. Indonesia's policies create a number of unnecessary local requirements (for data, offices, staff, languages, reporting, payment gateways, and bank accounts) that will likely preclude many foreign firms, especially small and medium-sized firms, from providing services to Indonesian residents. In the future, the absence of a physical office could provide reason for Indonesian authorities to target (with tax bills) or cut off access (digitally) to foreign firms.

As a consequence, Indonesian users will likely be left with having access to fewer, more expensive, and less-innovative services.

Russia: New Rules Target and Squeeze Out Foreign Internet-based Video Providers

On July 1, 2017, a new Russian law came into force that severely restricts foreign ownership of OTT video services.[75] The law was largely motivated by Netflix's launch in Russia in 2016, which led to local online video services complaining that Netflix, as a global player, would present "unfair competition" to local firms.[76] The largely government-owned and controlled Russian media supported the law, under the guise that it equalizes regulatory burdens between traditional media and OTT services. Despite opposition from OTT firms and Internet companies and an expert government council, the bill was approved by Russia's parliament almost without any amendments.[77]

Russia's new restrictions on OTT video services was motivated by Netflix's launch in 2016, as local companies complained that Netflix, as a global player, would present "unfair competition" to local firms.

The measure requires that only a Russian legal entity or a Russian citizen (and moreover an individual who does not hold any other citizenship) can be the majority owner of such services. The new law applies to owners of Internet websites, website pages, information systems, and computer software that are used for online distribution of videos that target Russian consumers, and that are accessed by more than 100,000 users per day in Russia (as measured by a government agency). It covers both subscription-based and free advertising-supported services. Firms that have less than 50 percent of their users in Russia have to apply for government approval to own more than 20 percent of any such Russian legal entities. The law will not apply to Internet search systems or information resources that primarily distribute user-generated content. All providers who meet the criteria will need to register with the Federal Service for Oversight in the Sphere of Communications, Information Technologies and Mass Media, which has the ability to fine or block those services that do not comply with these requirements.

The impact these restrictions have had on foreign operators is clear as per a report prepared for the Council of Europe's European Audiovisual Observatory: "to expect foreign investments in the Russian VOD market in such terms is not realistic. It is also impossible to make full launches of [a] foreign service."[78]

Some examples:

- In the middle of 2016, LeEco, a Chinese company, wanted to launch in Russia by purchasing a local firm or by using its own platform. LeEco's representatives held several meetings with a variety of large companies and headhunted leading experts, announcing large investments in content and devices. However, by the end of the year, the company closed most of its operation in Russia due to risks associated with this new law.[79]
- Media analysts predict that the new law will force Amazon Prime and Netflix to abandon their stand-alone streaming services and instead exit the market and license content to third parties (as Netflix does in China).[80] These firms' experiences show how hard the Russian market is for foreign digital firms.

- Amazon Prime launched on December 14, 2016; however, programming is only in English, only a few movies have Russian subtitles, and payment is in U.S. dollars.
- Netflix launched in Russia in the beginning of 2016. Perhaps indicative of the struggle to establish operations, Netflix only purchased one Russian movie in the first year.[81] Netflix may be able to avoid many of the new law's restrictions (at least in the short term) if it has less than 100,000 Russian users, which it would need to prove to Russian government agencies.[82] However, implying that Netflix is beyond this threshold, in April, 2017, the head of Russia's communications agency said that Netflix would have to partner with a Russian company to continue operating in the country.[83]

Thailand: Considers Burdensome, Restrictive, and Discriminatory Regulations of OTT Services

In Thailand, regulators are considering range of burdensome, restrictive, and discriminatory proposals for OTT content providers. These measures, introduced by the National Broadcasting and Telecommunications Commission (NBTC), are being pursued in part to protect traditional telecommunication operators struggling to compete with OTT services. While the proposals are still being developed (including key points like how to define and categorize OTT services), it's clear that the NBTC's initial ideas would undermine a growing part of Thailand's digital economy.

OTT services in Thailand, as in many other countries, are growing in popularity due to changes in technology (e.g., wireless broadband and smart phones) and consumer behavior (e.g., preferring to access video and music via smart phones). Traditional telecommunications and broadcast companies have struggled to adapt to these changes, seeing a drop in advertising revenue and subscribers/viewers for traditional services (such as voice and text and cable subscriptions). Thai companies in these sectors have called for government regulation to "level the playing field" claiming that Internet-based services have an unfair advantage as they don't pay a license fee (like traditional Thai companies in these sectors often have to), don't pay specific charges for the use of infrastructure (which is facing capacity constraints, especially broadband), and that foreign OTT providers are not subject to similar taxes.[84]

As in other nations pursuing similar regulations, the NBTC is trying to regulate OTTs as part of an outdated view that they are the same as traditional telecommunications and content delivery providers.[85] In April, the NBTC indicated in a draft proposal that OTT video services should be categorized like traditional broadcast businesses, be registered with the government, be required to set up a local office as a condition of market entry, and be required to pay a bandwidth fee on the consumption of OTT services. Subsequently, the NBTC tried to pressure both local and foreign OTT service providers, such as Facebook, Netflix, YouTube, and others to register with the government by July 22 (which none did), with the threat that failure to do so would lead the agency to undermine their services in

Thailand.[86] However, in July, the NTBC decided to delay these changes after receiving criticism from foreign firms and business groups, such as the U.S.-ASEAN Business Council, that the policy would undermine Thailand's digital economy and that the drafting process did not allow enough time for feedback.[87] However, the Thai government and NBTC have not ruled out that the final policy will include any and/or all parts of this initial proposal.[88]

By and large, the NBTC's approach to OTT services is misplaced and misguided. Technological displacement is not a new phenomenon, nor is the political reaction against it. Those who lose out to market competition, especially by new entrants who may not face the same regulatory burdens, often feel that the latter benefit from an unfair advantage. Thai regulators should not be trying to saddle new entrants with regulations simply because incumbent firms are unable to compete with the new technologies and business models at the heart of these new services. There is no reason to expect that the tremendous value created by these OTT services should go to incumbent providers. Instead, it is meant for the consumers that use them, which is why OTT services have grown in popularity around the world.

Furthermore, the NBTC should not be trying to apply traditional regulations to OTT services, such as licensing, to simply "level the playing field." OTT services do not fit the same regulatory model as legacy providers. Nor should the NBTC be trying to apply discriminatory charges, such as a bandwidth fee, against data associated with OTT services, whether the data is related to emails, voice, search, or video. Such an approach is both unrealistic and untenable. Instead, the NBTC should see the value that consumers and businesses derive from free and easy data flows and the services that rely on them.

The NBTC's proposal was developed with little notice and with little or no engagement with stakeholders. This partly explains why it is overly vague, expansive, discriminatory, and trade distorting. This approach to policymaking has raised a number of issues about regulation in Thailand's digital economy. Similar to the short-notice effort to get OTT services to register with the government, in May, the NBTC released a proposal whereby the agency considered setting up a "control list" of the top 100 content creators for OTT platforms. The head of the NBTC's broadcasting committee, Colonel Natee Sukonrat, stated that the rule was needed as "the top 100 most popular content providers or users on social media who influence public opinion will have to be reined in (such as on Netflix, YouTube, and Facebook)."[89] For Thailand's digital economy to thrive, it needs to avoid these types of burdensome, vague, and potentially arbitrary and discriminatory approaches to regulations.

Electric Vehicles

China: Undermines IP by Forcing Tech Transfers for Electric Vehicles

China introduced new rules that force foreign electric vehicle (EV) makers to transfer intellectual property (IP) into the country as a condition of market entry, despite World Trade Organization (WTO) laws that prohibit such practices as well as repeated claims that

it hasn't used similar rules in this or a range of other sectors. On January 7, 2017, China released the Administrative Regulations on Market Access of New-energy Automobile Manufacturers and Products, which introduces new restrictions on how foreign automakers operate in China, including forcing them to disclose and transfer critical know-how to their joint venture (JV) partner (given rules that restrict foreign ownership to 50 percent in the sector) as a condition for market entry into China's large and fast-growing EV market. It should be noted that Chinese automakers face no such restrictions if they want to sell or produce in most other nations.

China has used the regulation to introduce significant additional requirements that foreign EV makers need to fulfil to qualify as a government-authorized EV manufacturer in China.[90] Foreign firms are already forced to sell their vehicles under a new brand name (instead of foreign companies' existing one) and allow their Chinese JV partner to control at least one of three key EV technologies (electric motors, complex electronic controls, and power storage devices). The new rules require, that if the foreign automaker is to be allowed to compete in China's market, then its domestic-EV JV partner must have (been taught and) mastered the development and manufacturing technology for a complete EV (including with regard to all facets of the three core EV technologies) and have also developed EV-specific research and development capabilities.

China is using this rule with EVs as one part of a familiar playbook—lock down the market, set up a Faustian bargain for foreign firms, pump up local companies, encourage global expansion, and squeeze out foreign firms once dominance has been achieved.

In reality, this means that foreign EV makers will need to disclose all their cutting-edge technology to their local JV partner. This complete "mastery" requirement precludes foreign firms from manufacturing most of a vehicle in country and importing the most sensitive components in order to protect their technological advantage from the real threat that their local partner will use it for their own operations (separate from the JV). This targeted approach is not surprising given that batteries and their electronic components have been identified as the key technological challenge to be overcome in the successful development of an EV industry.[91]

China is using this rule with EVs as one part of a familiar playbook that it has used across a range of other strategic tech sectors—lock down the local market, set up a Faustian bargain for foreign firms (in terms of restrictive market access), support local companies, encourage global expansion, and squeeze out foreign firms once local dominance has been achieved. Foreign EV makers, like leading foreign firms in other tech sectors, are finding it hard not to agree to this bargain given the size and growth of the Chinese market. China became the world's largest car producer in 2009.[92] In 2016, China represented by far the largest electric car market, accounting for more than 40 percent of electric cars sold in the world (336,000 new electric cars were registered in 2016), more than double the number sold in the United States.[93]

Chinese policymakers view EVs as a strategic sector, explaining why the country has pumped the equivalent of billions of dollars in subsidies into developing local champions. For instance, China's Made in China 2025 plan calls for China to become a world leader in 10 future industries, including EV production.[94] Made in China 2025's goal is to

localize research and development and core segments of global supply chains, to reduce the country's dependence on foreign technology—by developing it indigenously or acquiring it from overseas—and to then capture international market share in these key industries. For example, regarding EVs, the plan sets a goal of 70 percent local production by 2020, rising to 80 percent by 2025.[95]

This new law comes despite China's WTO accession agreement containing rules forbidding the country from tying foreign direct investment or market access to requirements to transfer technology to the country. Indeed, it remains commonplace for China to require that firms transfer technology in exchange for being granted the ability to invest, operate, or sell in China.[96] In its 2017 survey of members, the U.S.-China Business Council showed that 20 percent of members had been asked to transfer technology to China during the past three years.[97] The new rule also breaches WTO rules that afford a 60-day period for stakeholders to submit feedback on new policies affecting its trade commitments.[98] It also comes after China made explicit commitments at the 2011 U.S.-China Joint Commission on Commerce and Trade that it would not do the exact things that this new law does.[99]

Foreign firms and national trading partners are justifiably skeptical of China's response to concerns raised after the law's release—that China wields no forced technology transfer requirements—given their past experience in dealing with Chinese authorities.[100] One of the most recent cases of this involved General Motors, which looked to start selling its electric hybrid vehicle, the Volt, in China. The Chinese government began placing "heavy pressure on the company to share some of the car's core technology."[101] Specifically, the Chinese government precluded the Volt from qualifying for purchase subsidies totaling up to $19,300 a car—subsidies which are available for alternative fuel vehicles (but only if manufactured in China; again yet another violation of WTO rules)—unless General Motors agreed to transfer the engineering secrets for one of the Volt's three main technologies to a JV in China with a Chinese automaker.[102] For its part, the Ford Motor Company, which is currently conducting demonstration projects of electric cars in China (and plans to launch commercial sales there), has already acceded to China's technology transfer demand.[103] In addition to these forced technology transfer requirements and production and purchase subsidies, China's proposal to establish a carbon credit trading system also tilts the market in favor of local companies.[104]

China is using the new law to help its firms catch up to the technological frontier in EVs, as the majority of these EVs in China are not particularly sophisticated at the moment, and have a limited battery range.[105] That the new rules, along with other policies, target battery technology is clear.[106] Take the case of Samsung SDI and LG Chem. These Korean companies are the world's leading producers of lithium-ion EV batteries, which are the only type of battery eligible for subsidies in China. In October 2015, both firms established plants in China, yet in July 2016, both were left off a list of 31 companies that had been certified as approved battery suppliers.[107] China tried to explain their omission based on the previously undisclosed requirement that a factory had to have been in operation for over a

year.[108] As if the intention wasn't clear, in November 2016, China released a draft law that stipulated a minimum production requirement for EV battery makers (of eight gigawatt hours) that is well above the capacity of both firms (despite them producing tens of thousands of units a year in China).[109]

Another case, this related to EVs in Beijing, showcases other tools that China uses to disadvantage foreign EV firms.[110] In February 2017, in an effort to fight Beijing's air pollution problem, the city government announced a plan to replace some 70,000 petrol-powered taxis with EVs.[111] The Beijing government is likely to benefit directly from this policy as it also happens to own the Beijing Automotive Industry Corporation (BAIC), which makes one of China's top-selling electric cars, the EU 260. In a further twist, Hyundai (which has been a 50-50 JV partner with BAIC since the early 2000s) received approval to start producing an electric version of its Elantra model car in 2018. However, Hyundai received approval only after BAIC-Hyundai "agreed" to switch its use of batteries made by Samsung and LG Chem (which suddenly did not meet Chinese standards) to those from Chinese firm Contemporary Amperex Technology Limited (CATL)—a "national champion" that China wants to become a world leader in batteries.[112]

There are enough similarities in the policies in this and prior years' reports to show that countries watch what others are doing (and getting away with) before deciding to do it themselves.

These policies highlight how there is a complete lack of reciprocity in automobile trade and market access between China and the United States—something emblematic of the state of affairs across a wide range of advanced-technology industries. China maintains tariffs and highly restrictive conditions for autos while the United States imposes few or no barriers on foreign automobile manufacturers. As outlined, U.S. and other foreign car makers face tariffs up to 25 percent, highly restrictive JV requirements, and caps on foreign ownership. Meanwhile, the United States applies tariffs of 2.5 percent and operates no foreign ownership caps.[113] As it relates to subsidies, U.S. tax credits for the purchase of energy-efficient alternative fuel vehicles are not restricted to domestic-headquartered auto producers, nor are foreign auto manufacturers barred from enjoying them unless they transfer technology to the United States.

CONCLUSION

Trade policy has assumed an unusual prominence in policy debates around the world over the last year. In terms of addressing innovation mercantilism, there were setbacks in efforts to set new rules to address some of the modern trade barriers outlined in this and past years' ITIF reports (e.g., the United States' withdrawal from the TPP and the failure of WTO members to make any real progress on e-commerce issues). However, there were also some bright spots that point toward progress in the year ahead, most notably the United States stepping up efforts to confront Chinese innovation mercantilism. But in the absence of more action and new rules and stricter enforcement, more and more countries will consider following China, Russia, Vietnam, and others' leads in pursuing a strategy of innovation mercantilism. There are enough similarities in the policies in this and prior years' reports to show that countries watch what others are doing (and getting away with) before deciding to go down such a mercantilist path. If this trend continues, the broader global trading system will be put at systemic risk.

This is why the United States, European Union, Japan, South Korea, and other leading innovation countries need to do more in terms of pushing back against these policies and negotiating new rules. As innovation and trade policy have become increasingly intertwined, openness to trade has become a bedrock pillar of an effective global innovation policy system. These countries will need a renewed push for an update to the global trading system if the damage from mercantilist policies is to be stopped and rolled back, ensuring that the global trading system will be better placed to maximize innovation in the years ahead.

ENDNOTES

1. Robert Atkinson, "Designing a Global Trading System to Maximize Innovation," Global Policy Journal 5, no. 1 (February 2014): 57–62.
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. 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.
6. Nigel Cory and Robert Atkinson, "ITIF Filing to the Central Bank of Brazil on Cybersecurity and Data Processing Requirements" (Information Technology and Innovation Foundation, November, 2017), https://itif.org/publications/2017/11/14/itif-filing-central-bank-brazil-cybersecurity-and-data-processing.
7. 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.
8. Castro, "The False Promise of Data Nationalism."
9. Ibid., 6; Charles Johnston, "Investigation Number 332-531, Digital Trade in the U.S. and Global Economies, Part 1" (submission by Citi to a United States International Trade Commission investigation, March 14, 2013), http://www.uscib.org/docs/Citi_TC_030713.pdf.
10. As can be attested by the growing size of associated subscriptions, value added, output, and employment Organisation for Economic Co-operation and Development (OECD), *OECD Digital Economy Outlook 2015* (Paris: OECD, 2015), http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm.
11. OECD Digital Economy Outlook 2015; James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute report, February, 2016), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
12. This wave of cyber-related digital trade barriers builds on China's restrictive policies in this domain reported in past years of this report. See: Nigel Cory, "The Worst Innovation Mercantilist Policies of 2016" (The Information Technology and Innovation Foundation, January 9, 2017), https://itif.org/publications/2017/01/09/worst-innovation-mercantilist-policies-2016; Nigel Cory, "The Worst Innovation Mercantilist Policies of 2015" (The Information Technology and Innovation Foundation, January 11, 2017), https://itif.org/publications/2016/01/11/worst-innovation-mercantilist-policies-2015.
13. Jing de Jong-Chen, Senior Director, Global Security Strategy and Diplomacy Group in the Corporate, External and Legal Affairs Division at Microsoft Corp, "Event: Policy and Politics: the Impact of China's New Cybersecurity Law" (event transcript, June 23, 2017), https://www.wilsoncenter.org/event/policy-and-politics-the-impact-chinas-new-cybersecurity-law.
14. "China adopts a tough cyber-security law," *The Economist,* November 10, 2016, https://www.economist.com/news/china/21710001-foreign-firms-are-worried-china-adopts-tough-cyber-security-law.
15. "Understanding the Impact of China's Far-Reaching New Cybersecurity Law," Cleary Gottlieb law firm website, accessed December 14, 2017, https://www.clearygottlieb.com/~/media/organize-

archive/cgsh/files/2017/publications/alert-memos/understanding-the-impact-of-chinas-far-reaching-new-cybersecurity-law-10-5-17.pdf.

16. Eva Dou, "Microsoft, Intel, IBM Push Back on China Cybersecurity Rules," *WSJ,* December 1, 2016, https://www.wsj.com/articles/microsoft-intel-ibm-push-back-on-china-cybersecurity-rules-1480587542.
17. Article 37.
18. As set out by the Draft Guidelines on Security Assessment for Data Export published by the National Information Security Standardisation Technical Committee on May 27, 2017
19. Clarice Yue, Michelle Chan, Sven-Michael Werner, and John Shi, "China Cybersecurity Law Update - Any Further Guidance on Data Localisation and Data Export," Bird and Bird law firm website, accessed December 14, 2017, https://www.twobirds.com/en/news/articles/2017/china/any-further-guidance-on-data-localisation-and-data-export.
20. Nigel Cory and Robert Atkinson, "Comments to Chinese State Internet Information Office on Handling Data," (The Information Technology and Innovation Foundation, May 11, 2017), https://itif.org/publications/2017/05/11/comments-chinese-state-internet-information-office-handling-data.
21. Translation: "Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security (Draft for Soliciting Opinions)," translation by Paul Triolo, China Copyright and Media website, accessed December 14, 2017, https://chinacopyrightandmedia.wordpress.com/2017/04/11/circular-of-the-state-internet-information-office-on-the-public-consultation-on-the-measures-for-the-assessment-of-personal-information-and-important-data-exit-security-draft-for-soliciting-opinions/.
22. Translation: "Critical Information Infrastructure Security Protection Regulations," translation by Graham Webster, Paul Triolo and Rogier Creemers, China Copyright and Media website, accessed December 14, 2017, https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/.
23. Paul Triolo, Rogier Creemers and Graham Webster, "China's Ambitious Rules to Secure 'Critical Information Infrastructure' New Draft Regulations Suggest Expansive Scope, Detail Responsibilities for Network Operators" (New America, July 14, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.
24. Cory, "Worst Innovation Mercantilist Policies of 2016."
25. Article 18 defines the scope of CII as: The network infrastructure and information systems operated or managed by the following work units, which whenever destroyed, cease functioning or leak data may gravely harm national security, the national economy, the people's livelihood and the public interest, shall be brought into the scope of CII protection…" Article 18:3 states that CII includes: research and production work units in sectors and areas such as national defense science and industry, large-scale equipment, chemistry, food, drugs, etc." Translation: "Critical Information Infrastructure Security Protection Regulations."
26. Paul Mozur, "New Rules in China Upset Western Tech Companies," *New York Times,* January 28, 2017, https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html.
27. Translation: "Interim Security Review Measures for Network Products and Services," translation by Paul Triolo, China Copyright and Media website, accessed December 14, 2017, https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/; Nick Beckett and Amanda Ge, "China publishes security review measures for network products and services," *Lexology,* May 9, 2017, https://www.lexology.com/library/detail.aspx?g=2b23010c-3b62-4236-9e47-32cbbac9a89c.
28. Translation: "Encryption Law of the People's Republic of China (Opinion-seeking Draft)," translation by Paul Triolo and Joh Costello, China Copyright and Media website, accessed December 14, 2017,

https://chinacopyrightandmedia.wordpress.com/2017/04/13/encryption-law-of-the-peoples-republic-of-china-opinion-seeking-draft/; "China Releases Draft Encryption Law for Public Comment," Covington and Burling law firm website, accessed December 14, 2017, https://www.cov.com/-/media/files/corporate/publications/2017/05/china_releases_draft_encryption_law_for_public_comment.pdf.

29. China Releases Draft Encryption Law for Public Comment," Covington and Burling law firm website.
30. "China Releases Draft Encryption Law for Public Comment," Covington and Burling law firm website.
31. "Members debate cyber security and chemicals at technical barriers to trade committee," World Trade Organization website, accessed January 11, 2018, https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm.
32. "Members debate cyber security and chemicals at technical barriers to trade committee," World Trade Organization website, accessed January 11, 2018, https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm.
33. For a full review see: Adam Segal, "China, Encryption Policy, and International Influence" (Hoover Institution Essay, Series paper No. 1610, 2016), https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf; On Chinese tech standards see: Stephen Ezell and Robert Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (The Information Technology and Innovation Foundation, December, 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.
34. Dieter Ernst and Sheri Martin, "The Common Criteria for Information Technology Security Evaluation— Implications for China's Policy on Information Security Standards" (East-West Center Working Papers, No. 108, January 2010), www.files.ethz.ch/isn/134351/econwp108.pdf.
35. Gerry Shih and Paul Carsten, "China Says Tech Firms Have Nothing to Fear from Anti-Terror Law," *Reuters*, March 4, 2015, https://www.reuters.com/article/us-china-security-usa/china-says-tech-firms-have-nothing-to-fear-from-anti-terror-law-idUSKBN0U60QG20151223.
36. Including on transparency and the reporting of policies that affect WTO trade commitments. See: Robert Atkinson, Nigel Cory, and Stephen Ezell, "Stopping China's Mercantilism: A Doctrine of Constructive, Alliance-Backed Confrontation" (The Information Technology and Innovation Foundation, March, 2017), https://itif.org/publications/2017/03/16/stopping-chinas-mercantilism-doctrine-constructive-alliance-backed.
37. "2016 U.S.-China Strategic and Economic Dialogue Joint U.S.-China Fact Sheet – Economic Track," U.S. Department of Treasury website, accessed December 14, 2017, https://www.treasury.gov/press-center/press-releases/Pages/jl0484.aspx.
38. Adam Segal, "China, Encryption Policy, and International Influence."
39. The U.S.-China Business Council (USCBC), "Unofficial USCBC Chart of Localization Targets by Sector Set in the MIIT Made in China 2025 Key Technology Roadmap" (report, 2017), https://www.uschina.org/sites/default/files/2-2-16%20Sector%20and%20Localization%20Targets%20for%20Made%20in%20China%202025.pdf; Keithe Bradsher and Paul Mozer, " China's Plan to Build Its Own High-Tech Industries Worries Western Businesses," *New York Times,* March 7, 2017, https://www.nytimes.com/2017/03/07/business/china-trade-manufacturing-europe.html.
40. Such as China's new National Intelligence Law, which requires firms to provide assistance to intelligence officials, access to facilities, and to keep such cooperation secret. What this means is that officials from China's national security and intelligence agencies could show up at a firm's China offices, show their badges, and demand technical support. The scope of the law may include allow the government to insert devices into data centers, monitor data traffic, and access IT products. While this has not been clearly detailed, it gives an idea of what "technical assistance" may imply in China. Jing de Jong-Chen, Senior

Director, Global Security Strategy and Diplomacy Group in the Corporate, External and Legal Affairs Division at Microsoft Corp, "Event: Policy and Politics: the Impact of China's New Cybersecurity Law."

41. The U.S.-China Business Council (USCBC), "USCBC 2017 Membership Survey: The Business Environment in China" (survey, 2017), https://www.uschina.org/sites/default/files/2017_uscbc_member_survey_1.pdf.
42. "Internet Restrictions Increasingly Harmful to Businesses, Say European Companies in China," EU Chamber of Commerce in China press release, February 12, 2015, http://www.europeanchamber.com.cn/en/press-releases/2235.
43. Shawn Donnan, "EU, Japan and US to ramp up trade pressure on China," *Financial Times,* December 13, 2017, https://www.ft.com/content/5f0aad90-deae-11e7-a8a4-0a1e63a52f9c.
44. "Adicionar un Capítulo Terecero al Tíitulo V de la Circular Única," Industria y Comercio Superintendencia, August 10, 2017, http://www.sic.gov.co/sites/default/files/normatividad/082017/Circular_Externa_005_de_2017.pdf.
45. The criteria for SIC's assessment include: the existence of rules for lawful data processing; the recognition of data subjects' rights and obligations for data controllers and data processors; and the presence of a supervisory authority tasked with overseeing compliance with data protection legislation. However, even if a country has not received an adequacy determination, businesses can still transfer data to these countries if they can establish a legal agreement ensuring compliance with Colombia's data protection standards. Under Article 26 of Statutory Law 1581 of 2012, Luz Helena Adarve, Juanita Acosta and Lina Cala, "Data protection in Colombia: overview," Thomas Reuters Practical law website, August 1, 2017, https://uk.practicallaw.thomsonreuters.com/2-619-4326.
46. David Haskel, "Colombia Adds U.S. to List of Data-Transfer-Safe Nations," *Bloomberg Law: Privacy and Data Security,* August 14, 2017, https://www.bna.com/colombia-adds-us-n73014463125/.
47. 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/.
48. For example, a report done for the European Parliament on data protection in China states that there is "no common grounds…found between two fundamentally different systems both in their wording and in their raison d'etre." The report takes a relativist approach by saying that China's culture and approach to human rights means that 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 done 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.
49. Kenneth Bamberger and Deirdre Mulligan, "Privacy on the Books and on the Ground." *Stan. L. Rev.* 63 (2010): 247, http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2011/01/Bamberger-Mulligan-63-Stan-L-Rev-247.pdf; Kenneth Bamberger and Deirdre Mulligan, *Privacy on the Ground Driving Corporate Behavior in the United States and Europe* (Boston: MIT Press, 2015), https://mitpress.mit.edu/privacy.
50. Julie Seaman, "Latin American Data Export Governance," (The Information Accountability Foundation, August 2, 2017), http://informationaccountability.org/latin-american-data-export-governance/.
51. Yee Chung Seck, Thanh Son Dang and Troy Taylor, "New Draft Cybersecurity Law 2017," *Lexology,* July 31, 2017, https://www.lexology.com/library/detail.aspx?g=b3fd124e-e230-4859-84a4-e7fe623e57df.
52. Articles 20-21.
53. Article 34 (4).
54. Article 9. Other barriers to data flows: 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.

55. This includes the US-ASEAN Business Council, AMCham Hanoi, BSA, CompTIA, the Asia Internet Coalition, DIGITALEUROPE, the Information Technology Industry Council, JEITA, SIA, and the U.S. Chamber of Commerce. See: Alexander Feldman, "August 2017 update" (U.S.-ASEAN Business Council, August update), https://www.usasean.org/presidents-newsletter/2017/08; Asian Internet Coalition, "Comments on Draft Law on Cybersecurity" (trade association comments on a draft law, August 4, 2017), https://www.aicasia.org/wp-content/uploads/2017/08/Draft-Law-on-Cyber-Security.pdf; Asian Internet Coalition, "Comments on amendments to the Draft Law on Cybersecurity," (trade association comments on amendments, November 13, 2017), https://www.aicasia.org/wp-content/uploads/2017/11/November-comments-on-v14-Draft-Law-on-Cybersecurity.pdf; Asian Internet Coalition, "Comments on amendments to the Draft Law on Cybersecurity" (trade association comments on amendments, September 5, 2017), https://www.aicasia.org/wp-content/uploads/2017/09/5-Sept-comments-on-amended-Draft-Law-on-Cybersecurity.pdf.

56. For example: Sections 8, 22, 34: " The use of cyberspace to oppose the State of the Socialist Republic of Vietnam; prejudice national security or social order and safety, sabotage great national unity, propagate an aggressive war or terrorism, cause enmities or conflicts between nations or religions; incite sex or racial discrimination; propagate or instigate violence, cause violent disturbances, disrupt security to disturb public order; post embarrassing slanderous obscene depraved or felony information; practise prostitution or social evils or traffic in human; sabotage the fine customs and practices of the nation, social morality of public health."

57. Anabelia Horbuz, "ANCINE issues VOD regulation recommendations," *Nextv News,* May 19, 2017, http://nextvnews.com/ancine-issues-vod-regulation-recommendations/; Juan Fernandez Gonzalez, "Brazil Continues VOD regulation debate," *RAPIDTVNews,* May 18, 2017, https://www.rapidtvnews.com/2017051847250/brazil-continues-vod-regulation-debate.html#axzz50bWz5ovC; ANCINE, (Portuguese) "Report of Public Consultations from the Regulatory Notice on Audiovisual Communications on Demand and Recommendations of ANCINE" (regulatory report, ANCINE, 2017), http://convergecom.com.br/wp-content/uploads/2017/05/Relatorio_Ancine_VoD.pdf.

58. Juan Fernandez Gonzalez, "Brazil Continues VOD regulation debate."

59. Paulo Higa, (from Portuguese) "ANCINE to create a tax for Netflix and quota for national films," *technoblog,* December, 2015, https://tecnoblog.net/192787/netflix-imposto-cota-producao-nacional-ancine/; "LAW Nº 12.485, OF SEPTEMBER 12, 2011," website of the Presidency of Brazil's Civil House, Sub-Office for Legal Affairs, accessed December 14, 2017, http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12485.htm.

60. Juan Fernande Gonzalez, "Brazil's creators demand VOD regulation," *RAPIDTVNews,* July 5, 2016, https://www.rapidtvnews.com/2016070543482/brazil-s-creators-demand-vod-regulation.html#axzz4lPHvvBsY.

61. "Brazilian cinema agency suggests VoD regulation," *telecompaper,* November 2, 2017, https://www.telecompaper.com/news/brazilian-cinema-agency-suggests-vod-regulation--1218709.

62. "Taxation on OTT in Brazil," *TechinBrazil,* June 10, 2015, https://techinbrazil.com/taxation-on-ott-in-brazil.

63. Ricardo Feltrin, (from Portugese) "Government plans to charge R$300 million in fees from Netflix Brazil until 2022," *UOL,* March 3, 2017, https://tvefamosos.uol.com.br/noticias/ooops/2017/03/01/governo-cogita-cobrar-r-300-milhoes-em-taxas-da-netflix-brasil-em-5-anos.htm.

64. "Half of Internet Users in Brazil Watch VOD," *eMarketer,* August 23, 2016, https://www.emarketer.com/Article/Half-of-Internet-Users-Brazil-Watch-VOD/1014384.

65. "YouTube, Netflix Find Massive VOD Success in Brazil," *eMarketer,* September 2, 2016, https://www.emarketer.com/Article/YouTube-Netflix-Find-Massive-VOD-Success-Brazil/1014435.

66. Tendências Consultoria Integrada, "The Economic Impact of Brazil's Audiovisual Industry" (report prepared by consultants, October 2016), http://www.mpaamericalatina.org/wp-content/uploads/2015/12/MPAAL_10_04_2016-english-fv.pdf.

67. Tendências Consultoria Integrada, "The Economic Impact of Brazil's Audiovisual Industry."

68. Nelson de Sa, (from Portugese) "Netflix President remembers stumbling blocks and comments on competition with channels," *Folha de Sao Paulo,* January 10, 2016, http://www1.folha.uol.com.br/ilustrada/2016/10/1818877-presidente-da-netflix-lembra-tropecos-e-comenta-concorrencia-com-canais.shtml.

69. Juan Fernandez Gonzalez, "HBO ramps up Brazilian production," *RAPIDTVNews, March 11, 2017,* https://www.rapidtvnews.com/2017031146475/hbo-ramps-up-brazilian-production.html. #axzz50bWz5ovC.

70. "Government Regulation No. 82 of 2012 on Electronic Transactions and Systems Operators (GR 82)," website accessed December 14, 2017, https://chambermaster.blob.core.windows.net/userfiles/UserFiles/chambers/9078/File/ICT/2017/OTT_Public_Hearing/ApplicationandContentServiceMinisterRegulationDraftFinal002.pdf; Nigel Cory, "Worst Innovation Mercantilist Policies of 2016."

71. Nigel Cory, "Worst Innovation Mercantilist Policies of 2016."

72. "Government Regulation No. 82 of 2012 on Electronic Transactions and Systems Operators (GR 82)."

73. Nick Redfearn, "Online Businesses and tax in Indonesia," Rouse the Magazine website, June 19, 2017, https://www.rouse.com/magazine/news/online-businesses-and-tax-in-indonesia/.

74. Organization for Economic Cooperation and Development (OECD), *Tax Challenges of Digitalisation* (Paris: OECD, October 25, 2017), https://www.oecd.org/tax/beps/tax-challenges-digitalisation-part-2-comments-on-request-for-input-2017.pdf.

75. Federal Law No. 87-FZ of May 1, 2017. "New Regulation of Online Cinemas in Russia," Debevoise and Plimpton law firm website, accessed December 14, 2017, https://www.debevoise.com/~/media/files/insights/publications/2017/05/20170531en_new_regulation_of_online_cinemas_in_russia.pdf.

76. Vladimir Kozlov, "Netflix Continues Operating in Russia Despite Foreign Ownership Restrictions," *Hollywood Reporter,* July 3, 2017, https://www.hollywoodreporter.com/news/netflix-continues-operating-russia-foreign-ownership-restrictions-1015525.

77. J'son & Partners Consulting, "The Russian Legal On-Demand Video Services Market" (report done for the European Audiovisual Observatory, 2017), http://www.obs.coe.int/documents/205595/552774/RU+2017+The_Russian_Legal_On-Demand_Video_Services_Market-Report_J_sonAndPartners_EN.pdf. /f0f0705f-4bf3-48b3-bd64-ce9d79d63235.

78. J'son & Partners Consulting, "The Russian Legal On-Demand Video Services Market."

79. J'son & Partners Consulting, "The Russian Legal On-Demand Video Services Market."

80. Erik Gruenwedel, "Report: Netflix, Amazon Prime Video Projected to Leave Russia," *Home Media Magazine,* September 11, 2017, http://www.homemediamagazine.com/streaming/report-netflix-amazon-prime-video-projected-leave-russia-40763.

81. J'son & Partners Consulting, "The Russian Legal On-Demand Video Services Market."

82. Vladimir Kozlov, "Why Russia's Foreign Ownership Restrictions on Streamers Do Not Affect Netflix," *Hollywood Reporter,* August 31, 2017, https://www.hollywoodreporter.com/news/netflix-exempt-russias-foreign-ownership-restrictions-1034219.

83. Vladimir Kozlov, "Netflix Continues Operating in Russia Despite Foreign Ownership Restrictions."

84. Komsan Tortermvasana, "NBTC mulls bandwidth fees, licensing for OTT," *Bangkok Post,* April 4, 2017, https://www.bangkokpost.com/tech/local-news/1226600/nbtc-mulls-bandwidth-fees-licensing-for-ott.

85. Komsan Tortermvasana, "NBTC considers OTT control options," *Bangkok Post,* May 31, 2017, https://www.bangkokpost.com/tech/local-news/1259538/nbtc-considers-ott-control-options.

86. "Facebook, Netflix get OTT ultimatum," *Bangkok Post,* June 23, 2017, https://www.bangkokpost.com/archive/facebook-netflix-get-ott-ultimatum/1273743.

87. "NBTC makes volte-face on OTT plan," *Bangkok Post, July 6, 2017,* https://www.bangkokpost.com/archive/nbtc-makes-volte-face-on-ott-plan/1281779; Alexander Feldman, "Letter: OTT regulations in Thailand" (letter from the President and CEO of the U.S-ASEAN Business Countil to the Thai Deputy Prime Minister and the Chairman of the National Broadcasting and Telecommunications Commission, June 12, 2017), https://chambermaster.blob.core.windows.net/userfiles/UserFiles/chambers/9078/File/Thailand-OTT-letter---6.12.17.pdf; Alexander Feldman, "September 2017 update" (U.S.-ASEAN Business Council, September update), https://www.usasean.org/presidents-newsletter/2017/09.

88. Alexander Feldman, "September 2017 update"

89. Komsan Tortermvasana, "NBTC considers OTT control options."

90. (translated from Chinese) "Administrative Regulations on Market Access of New-energy Automobile Manufacturers and Products, MIIT," January 17, 2017, viewed December 14, 2017, http://www.miit.gov.cn/newweb/n1146295/n1146557/n1146624/c5462995/content.html.

91. Guy Fournier, Henning Hinderer, Daniel Schmid, René Seign, and Manuel Baumann, "The new mobility paradigm: Transformation of value chain and business models," *Enterprise and Work Innovation Studies,* 8 (2012): 9-40.

92. Gilmar Masiero, Mario Henrique Ogasavara, Ailton Conde Jussani, and Marcelo Luiz Risso, "Electric vehicles in China: BYD strategies and government subsidies," *RAI Revista de Administração e Inovação* 13, no. 1 (2016): 3-11.

93. International Energy Agency (IEA), *Global EV Outlook 2017* (Paris: IEA, 2017), https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf.

94. Trefor Moss, "China, With Methodical Discipline, Conjures a Market for Electric Cars,: *WSJ,* October 2, 2017, https://www.wsj.com/articles/china-with-methodical-discipline-takes-global-lead-in-electric-cars-1506954248.

95. U.S. Chamber of Commerce, "Made in China 2025: Global Ambitions Built on Local Protections" (report, 2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

96. "The representative of China confirmed that China would only impose, apply or enforce laws, regulations or measures relating to the transfer of technology, production processes, or other proprietary knowledge to an individual or enterprise in its territory that were not inconsistent with the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) and the Agreement on Trade-Related Investment Measures (TRIMs Agreement)." Congressional-Executive Commission on China, "China's Working Party Report," (November 2011), 49, http://www.cecc.gov/pages/selectLaws/WTOimpact/wkptrptPRCWTO.php.

97. "2017 USCBC Annual Member Survey Released," U.S.-China Business Council website, accessed January 9, 2018, http://www2.itif.org/2016-unlocking-encryption.pdf.

98. The law was adopted on January 6, less than a month after the draft was released. Given the law came into force on July 1, 2017, it's difficult to believe that China was open to receiving comments from foreign firms and trading partners.

99. At the 2011 U.S.-China Joint Commission on Commerce and Trade (JCCT), China confirmed: that it does not and will not maintain measures that mandate the transfer of technology. China clarified that

"mastery of core technology" does not require technology transfer for NEVs; that the establishment of brands is a corporate decision and that the Chinese government does not and will not impose any requirements for foreign-invested companies to establish domestic brands in China; and confirmed that foreign-invested enterprises are eligible on an equal basis for subsidies or other preferential policies for NEVs with Chinese enterprises, and that these subsidies and preference programs will be implemented in a manner consistent with WTO rules. "22nd U.S.-China Joint Commission on Commerce and Trade Fact Sheet," U.S. Department of Commerce website, accessed December 14, 2017, https://2010-2014.commerce.gov/news/fact-sheets/2011/11/21/22nd-us-china-joint-commission-commerce-and-trade-fact-sheet.html.

100. Charles Clover, "Foreign carmakers on edge despite China tech transfer assurances," *Financial Times,* March 30, 2017, https://www.ft.com/content/adb80896-1462-11e7-80f4-13e067d5072c.

101. Keith Bradsher, "Hybrid in a Trade Squeeze," *New York Times*, September 5, 2011, http://www.nytimes.com/2011/09/06/business/global/gm-aims-the-volt-at-china-but-chinese-want-itssecrets.html.

102. Keith Bradsher, "Hybrid in a Trade Squeeze." This purchase-subsidy program will be superseded by a new mandated manufacturing quota, which again discriminates against foreign EV makers. See: Marika Heller, "Chinese Government Support for New Energy Vehicles as a Trade Battleground," The National Bureau of Asian Research, September 27, 2017, http://www.nbr.org/research/activity.aspx?id=805.

103. Keith Bradsher, "Hybrid in a Trade Squeeze."

104. European Union Chamber of Commerce in China, "China Manufacturing 2025: Putting Industrial Policy Ahead of Market Forces," (report, 2017), http://www.europeanchamber.com.cn/en/china-manufacturing-2025.

105. Michael Dunne, "The Beginning of the End For American Automakers in China," *The New Cartographer,* April, 2017, http://newcartographer.com/combustion/endchina.html; Hua Wang and Chris Kimble "Innovation and leapfrogging in the Chinese automobile industry: Examples from Geely, BYD, and Shifeng," *Global Business and Organizational Excellence* 32, no. 6 (2013): 6-17. https://halshs.archives-ouvertes.fr/halshs-00859483/document; Oliver Kaberry, "Can China Successfully leapfrog into Electrical Vehicle Dominance," (Master's thesis, Lund University, 2015), http://lup.lub.lu.se/student-papers/record/7854737/file/7854739.pdf; World Bank and PRTM Management Consultants, *The China New Energy Vehicles Program Challenges and Opportunities* (Washington D.C., the World Bank and PRTM Management Consultants, April, 2011), http://documents.worldbank.org/curated/en/333531468216944327/The-China-new-energy-vehicles-program-challenges-and-opportunities; "The Kandi EV is a good example. The best-selling electric car in China in 2015 (16,736 units), the Kandi EV looks like a cheap knock-off of a Mercedes Smart For Two mini-car with a range of 75 miles and a top speed of 50mph," Dr. Crystal Chang, "China's 13th Five-Year Plan: Implications for the Automobile Industry" (testimony before the U.S.-China Economic and Security Review Commission, April 27, 2016), https://www.uscc.gov/sites/default/files/Crystal%20Chang_Written%20Testimony%20042716.pdf.

106. European Union Chamber of Commerce in China, China Manufacturing 2025: Putting Industrial Policy Ahead of Market Forces."

107. Jin-young Cho, "The Real Reason Samsung SDI, LG Chem Failed to Get EV Certification Due to Short Period of Operation," *Business Korea*, June 23, 2016, http://www.businesskorea.co.kr/english/news/industry/15067-real-reason-samsung-sdi-lg-chem-failed-get-ev-battery-certification-due-short; Jason Deign, "South Korean Battery Makers Face a Surprising Challenge in China," *Green Tech Media*, June 30, 2016, https://www.greentechmedia.com/articles/read/south-korean-battery-makers-face-a-surprise-challenge-in-china#gs.Jdm5dVk.

108. Jin-young Cho, "The Real Reason Samsung SDI, LG Chem Failed to Get EV Certification Due to Short Period of Operation."

109. "Call for comments on Regulations on Auto Power Battery Industry (2017)," Ministry of Industry and Information Technology, November 22, 2016, accessed December 14, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057585/n3057589/c5375253/content.html.

110. Michael Dunne, "China Deploys Aggressive Mandates To Take Lead In Electric Vehicles," *Forbes,* February 28, 2017, https://www.forbes.com/sites/michaeldunne/2017/02/28/china-deploys-aggressive-mandates-to-stay-no-1-in-electric-vehicles.

111. Yuvetta Tan, "China's capital is replacing tens of thousands of taxis with electric cars to fight pollution," *Mashable,* February 27, 2017, http://mashable.com/2017/02/27/china-electric-taxis.

112. Steve Hanley, "China Is Playing Politics With Hyundai EV Production," *CleanTechnica,* February 16, 2017, https://cleantechnica.com/2017/02/16/china-playing-politics-hyundai-ev-production/; Henry Sanderson, Tom Hancock and Leo Lewis, "Electric cars: China's battle for the battery market," *Financial Times,* March 5, 2017, https://www.ft.com/content/8c94a2f6-fdcd-11e6-8d8e-a5e3738f9ae4.

113. Michael Dunne, "The Beginning of the End for American Automakers in China."

ACKNOWLEDGMENTS

The author wishes to thank the following individuals for providing input to this report: Robert Atkinson, Daniel Castro, and Stephen Ezell. 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 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.