Before the
International Trade Administration
U.S. Department of Commerce
Washington, D.C.

In re:
Request for Comments on Energy,
Information and Communication Technology,
and Infrastructure in the Indo-Pacific Region

Docket Number 2018-25417
83 FR 58758

COMMENTS OF
INTERNET ASSOCIATION

On behalf of the world's leading internet companies, we are pleased to submit the following comments to the International Trade Administration as part of the request for public comments on energy, information and communication technology (ICT), and infrastructure in the Indo-Pacific region (83 FR 58758).

Internet Association (IA)[1] supports policies that promote and enable internet innovation, ensuring that information flows freely and safely across national borders, uninhibited by restrictions that are fundamentally inconsistent with the open and decentralized nature of the internet.

In the Indo-Pacific Region, internet businesses are facing increasing challenges that undermine the United States' (U.S.) leadership in the digital economy, making the International Trade Administration's work in understanding and addressing foreign digital restrictions in that region more critical than ever before. There are a number of current trends that are extremely concerning to the health of the digital economy. Countries, including Vietnam, Indonesia, and India, are adopting forced data localization policies that pose a fundamental threat to the free flow of information across borders and internet-driven trade. Moreover the recent push by some countries, notably India and Indonesia, to end the WTO moratorium on duties on electronic transmission would have a detrimental impact on how the internet connects and adds value to the world.

The U.S. is the global internet and digital content leader. Americans are enjoying a digital revolution that has led to amazing products, lower prices, and new jobs. We export all of this across the globe, with digital trade now accounting for more than 50 percent of all U.S. services exports. And every sector of the economy benefits from this leadership. That didn't just happen – existing U.S. law and policy are central to our digital success and leadership.

The administration should fight to see the adoption of America's digital framework across the world, including in our trade deals, and at the same time defend against attacks on U.S. technology leadership. There's a global race to set the rules for the digital economy. Other countries are actively pressuring their trading partners to adopt policies that will threaten the success of the U.S. digital economy both in the U.S. and abroad.

All industries — and businesses of all sizes — reap the rewards of our digital leadership. Small businesses and entrepreneurs in every American state and every community use the internet to sell and export across the globe. Internet-connected small businesses are three times as likely to export and create jobs, grow four times more quickly, and earn twice as much revenue per employee.

[1] A complete list of Internet Association's membership can be found at: https://internetassociation.org/our-members/.

The internet cuts the trade deficit in every sector of the economy. Each year, U.S. manufacturers export $86.5 billion of products and services through digital trade. Newly released figures from BEA show that the 2017 U.S. digital trade surplus increased 7.8 percent to $172.6 billion[2] from $160.2 in 2016.[3]

America rose to digital leadership thanks to our digital policies. Digital technologies are central to supporting American small business growth.

The internet is a borderless medium and the movement of electronic information enables virtually all global commerce. Every sector of the economy relies on information flows from manufacturing, to services, to agriculture. Requirements that force U.S. companies to store or process data locally hurt U.S. businesses and threaten the open nature of the internet.

Intermediary liability protections allow online platforms to function and facilitate massive volumes of U.S. exports, especially by small- and medium-sized businesses. They support 425,000 U.S. jobs and $44 billion in U.S. GDP annually.[4] If online platforms or other services are held liable for other people's materials, including customer reviews or other user-generated content, they would not be able to operate in such an open manner or, more importantly, innovate.

The U.S. has a strong and innovation-oriented copyright framework that protects creators' legitimate rights, enables new innovation, and allows consumers to benefit – including through safe harbors like those in the Digital Millennium Copyright Act (DMCA) and limitations and exceptions like fair use. This framework has been critical to the U.S. digital economy domestically and needs to be projected globally. Fair use laws underpin one in eight U.S. jobs, drive 16 percent of our economy, and generate $368 billion in exports annually.[5] They hold the key to future U.S. innovation, including in areas like artificial intelligence.

E-commerce is enabling millions of American small businesses to find customers and make sales throughout the Indo-Pacific Region in ways impossible a just a few of decades ago. The U.S. maintains streamlined and simplified trade facilitation and customs procedures, including an $800 de minimis and a $2,500 informal clearance threshold. Complex laws and policies at foreign borders, though, are putting e-commerce enabled American small businesses at a disadvantage, slowing the speed of delivery, increasing costs, and compromising U.S. competitiveness.

[2] This filing previously stated totals for "total digital service exports" and "digital service trade surplus" that summed together ICT-enabled service exports and potential ICT-enabled service exports. These figures should not have been summed together as potential ICT-enabled service exports includes ICT-enabled service exports. The correct totals are approximately $439 billion in digital service exports and a surplus of $172.6 billion for digital service trade balance. The previous, incorrect figures were $470 billion in digital service exports and $196.1 for for digital service trade balance.
[3] https://apps.bea.gov/iTable/iTable.cfm?ReqID=62&step=1#reqid=62&step=9&isuri=1&6210=4
[4]https://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf
[5] http://www.ccianet.org/wp-content/uploads/2017/06/Fair-Use-in-the-U.S.-Economy-2017.pdf

Key Issues Impacting Internet Companies in the Indo-Pacific Region

Broadly key issues impacting internet companies fall into the following areas.

- → Burdensome Or Discriminatory Data Protection Regimes
- → Customs Barriers To Growth In E-Commerce
- → Data Flow Restrictions And Service Blockages
- → Discriminatory Or Non-Objective Application Of Competition Regulations
- → Filtering, Censorship, And Service-Blocking
- → Non-IP Intermediary Liability Barriers
- → Restrictions On U.S. Cloud Service Providers
- → Overly Restrictive Regulation Of Online Services
- → Sharing Economy Barriers
- → Unbalanced Copyright And Liability Frameworks
- → Unilateral Or Discriminatory Tax Regimes

Burdensome Or Discriminatory Data Protection Regimes

Data has revolutionized every part of our economy and our lives, both online and offline. Businesses and nonprofits of all sizes, in all sectors, have integrated data into their products and services to the benefit of consumers. Countries throughout the Indo-Pacific Region are creating new privacy laws to regulate how companies handle data. This array of laws and regulations creates a "patchwork" effect that complicates compliance efforts and leads to inconsistent experiences for individuals.

IA companies believe trust is fundamental to their relationship with their users and customers.[6] IA member companies know that to be successful they must meet individuals' reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why IA member companies are committed to transparent data practices and to continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, IA member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

To give users and companies greater assurance that privacy will be protected on a cross-border basis, IA urges the administration to ensure that privacy protections are implemented in an objective and non-discriminatory way. In addition, it is important to encourage mechanisms that promote compatibility between different privacy regimes, as opposed to unilateral regulations that do not provide a basis for transferring data on a cross-border basis.

Customs Barriers To Growth In E-Commerce

Some countries have antiquated, complex, and costly customs procedures that make it difficult for U.S. small businesses to compete. In addition, some countries are reacting to the rise in American led e-commerce by implementing protectionist customs policies that will raise costs and slow delivery times, limiting U.S. companies' ability to serve customers in other markets. Governments across the globe have complex customs regimes and IA encourages the administration to work with foreign countries to modernize these antiquated systems and overly burdensome systems.

[6] https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/

Data Flow Restrictions And Service Blockages

Cross-border, global exchange of information – without censorship, content-based regulation, or filtering mandates – facilitates commerce and promotes economic inclusiveness. The internet ecosystem flourishes when users and content creators are empowered through an open architecture that promotes the unrestricted exchange of ideas and information. Internet services instantaneously connect users to goods and services, facilitate social interactions, and drive economic activity across borders. Consequently, support for the free flow of information is vital to eliminate trade barriers that restrict commerce or prevent U.S.-based internet services the freedom to operate in a foreign jurisdiction.

Unfortunately, data localization mandates and other limits on data transfers are increasingly restricting U.S. services from accessing overseas markets. While China has had data localization requirements in place, other countries are threatening to follow suit, particularly in the Asia-Pacific region. The most concerning developments in the past year have come from forced data localization efforts in India, Indonesia, and Vietnam.

In May, Indonesia issued draft regulatory amendments to localize certain classes of data. In June, Vietnam passed a Cybersecurity Law with undefined and potentially broad localization requirements. In July, India released a draft personal data protection bill seeking to localize certain classes of personal data. In October, a regulation from the Reserve Bank of India came into force, requiring that data related to financial transactions be stored only in India.

These and other foreign governments frequently cite concerns about security, privacy, and law enforcement access to justify localization measures. However, as the U.S. responds to these measures, it is critical to convey that data localization requirements typically increase data security risks and costs – as well as privacy risks – by requiring storage of data in a single centralized location that is more vulnerable to natural disaster, intrusion, and surveillance. In practice, the primary impact of a data localization measure is not to safeguard data but instead to wall off local markets from U.S. competition, while hurting local businesses as well.

Non-IP Intermediary Liability Barriers

A fundamental reason that the internet has enabled trade is its open nature – online platforms can facilitate transactions and communications among millions of businesses and consumers, enabling buyers and sellers to connect directly on a global basis. This model works because platforms can host these transactions without automatically being held responsible for the vast amounts of content surrounding each transaction. In the U.S., Section 230 of the Communications Decency Act has enabled the development of digital platforms by ensuring that online services can host user content without being considered the ‘speaker’ of that content. This law enables features such as customer reviews, which have been essential to building customer trust for U.S. small businesses in foreign markets.

However, this core principle, which has allowed U.S. services to function as platforms for trade and communication, is increasingly under threat abroad. Foreign governments are exerting a heavier hand of control over speech on the internet and are subjecting online platforms to crippling liability or blockages for the actions of individual users for defamation, “dangerous” speech, political dissent, and other non-IP issues. At the same time, foreign governments are making it more difficult for platforms to evolve new approaches to dealing with problematic content.

Overly Restrictive Regulation Of Online Services

The proliferation of content, applications, and services available online has delivered enormous value directly to consumers and small businesses. This includes lower entry barriers; greater access to information, markets, banking, healthcare, and communities of common interest; and new forms of media and entertainment. So called "over-the-top" (OTT) services play key roles in the digital economy. Each 10 percent increase in the usage of these services adds approximately $5.6 trillion to U.S. GDP.[7]

Yet numerous foreign governments in the Indo-Pacific region are developing and implementing measures to regulate online communications and video services as traditional public utilities. Some regulators and telecommunications providers are applying sector-specific telecom regulations to online services on matters such as emergency calling, number portability, quality of service, interconnection, and tariffing. Similarly, regulators have sought to subject online video services to broadcasting-style obligations on local content quotas, local subsidies, and a variety of regulatory fees. Such special regulation is not necessary for online services, where there are few barriers to new market entrants and low switching costs. While often couched as "level playing field" proposals, these initiatives serve to protect incumbent businesses, impede trade in online services, and make it substantially more difficult for U.S. internet firms to export their services.

Unbalanced Copyright And Liability Frameworks

The U.S. copyright framework both ensures a high level of copyright protection and drives innovative internet and technology products and services. Internet services rely on balanced copyright protections such as Section 107 of the Copyright Act ('fair use') and Section 512 of the DMCA ('ISP safe harbors') to create jobs, foster innovation, and promote economic growth. The U.S. internet sector – as well as small businesses that rely on the internet to reach customers abroad – require balanced copyright rules to do business in foreign markets.

In countries that lack this two-sided model of copyright law, U.S. innovators are at a significant disadvantage. Increasingly, governments like Australia and India are proposing new onerous systems of copyright liability for internet services and several of these countries are out of compliance with commitments made under U.S. free trade agreements.

If the U.S. does not stand up for the U.S. copyright framework abroad, then U.S. innovators and exporters will suffer, and other countries will increasingly misuse copyright to limit market entry. For example, critical limitations and exceptions to copyright under U.S. law enable digital trade by providing the legal framework that allows nearly all internet services to function effectively. Web search, machine learning, computational analysis, text/data mining, and cloud-based technologies all, to some degree, involve making copies of copyrighted content. These types of innovative activities – areas where U.S. businesses lead the world – are possible under copyright law because of innovation-oriented limitations and exceptions. In the U.S., industries that benefit from fair use and other copyright limitations generate $4.5 trillion in annual revenue and employ 1in 8 U.S. workers.[8] Unfortunately, foreign trading partners lack these innovation-oriented rules, which limit the export opportunities for U.S. industries in those markets.

[7] "The Economic and Societal Value of Rich Interaction Applications (RIAs)." WIK, 2017. http://www.wik.org/fileadmin/Studien/2017/CCIA_RIA_Report.pdf
[8] Capital Trade. "Fair Use in the U.S. Economy." http://www.ccianet.org/wp-content/uploads/library/CCIA-FairUseintheUSEconomy-2011.pdf.

In addition, Section 512 of the DMCA is a foundational law of the U.S. internet economy. It provides a 'safe harbor' system that protects the interests of copyright holders, online service providers, and users, imposing responsibilities and rights on each. Safe harbors are critical to the functioning of cloud services, social media platforms, online marketplaces, search engines, internet access providers, and many other businesses. Weakening safe harbor protections would devastate the U.S. economy, costing nearly half a million U.S. jobs.[9] And yet key trading partners have failed to implement ISP safe harbors, including Australia which has expressed obligations to enact safe harbors under trade agreements with the U.S.

The administration has promoted copyright safe harbors in trade agreements for the last 15 years, including in the USMCA. Increasingly, however, jurisdictions have chipped away at the principles behind this safe harbor framework. For example, some countries have proposed or implemented requirements that internet companies monitor their platforms for potential copyright infringement or broadly block access to websites, rather than adhere to the U.S. model of taking down specific pieces of infringing content upon notice. Other countries have failed to adopt safe harbors at all. Such efforts threaten the ability of internet companies to expand globally by eliminating the certainty that copyright safe harbors provide.

Unilateral Or Discriminatory Tax Regimes

Some foreign trading partners are imposing taxation measures that single out digital platforms for special treatment, often with the intention of giving domestic companies an advantage over U.S. competitors. In many countries, these taxation measures run afoul of treaty obligations and are outside the agreed international framework for cross-border trade and investment. Unfortunately, these tax regimes are on the rise globally. The majority of such measures have three core problems from a trade perspective: they are discriminatory in design or effect towards U.S. companies, they effectively create tariffs on U.S. services, and they tax income that is already taxed by the United States.
Finally, with the rapid pace of internet-innovation, IA calls on the administration to intensify efforts to address emerging market access restrictions that impede U.S. digital trade. Foreign governments continue to propose or implement burdensome measures such as local presence requirements and forced transfers of technology, encryption keys, source code, and algorithms as conditions of market access. In addition, governments across the globe are considering measures that would assign liability for collecting customs duties and/or taxes directly to U.S. internet services.

[9] http://internetassociation.org/wp-content/uploads/2017/06/NERA-Intermediary-Liability-Two-Pager.pdf

Indo-Pacific Digital Trade Barriers

Australia

General

Australia's recently introduced Access and Assistance Bill stands as a significant barrier to trade for U.S. technology companies. The bill would impose obligations that are unprecedented and unworkable. If the bill became law, it would negatively affect the ability of businesses to safely and securely rely on any digital service, the internet, or technology more generally. Legally introduced security vulnerabilities, "backdoors," and other "secret access" capabilities designed to overcome encryption and other security features would have a material impact on any industry relying on technology. Given that the same technology can be sold and used globally, the introduction of such capabilities would not only put at risk the privacy and security of Australian citizens, businesses, and governments, it would undermine privacy and security globally. With this bill, Australia introduces significant risk that may compel foreign technology providers to cease operations in and exports to Australia.

Unbalanced Copyright And Liability Frameworks

Under the Australia-U.S. FTA (AUSFTA), Australia is obligated to provide safe harbors for a range of functions by online services providers. Australia has failed to comply with this commitment. Australia's Copyright Act of 1968's safe harbor provisions do not unambiguously cover all internet service providers, including the full range of internet services (cloud, social media, search, UGC platforms).[10] Instead, only a narrower subset of "service providers" are covered under Australian law,[11] rather than the broader definition of "internet service providers" in the Australia-U.S. FTA. The lack of full coverage under this safe harbor framework creates significant liability risks and market access barriers for internet services seeking access to the Australian market. IA urges the administration to engage with Australian counterparts to make necessary adjustments to Division 2AA of the Copyright Act to bring this safe harbor into compliance with AUSFTA requirements.

On 28 June 2018, the Australian Parliament amended the Copyright Act's provisions on safe harbors. The amendments expand the intermediary protections to some service providers including organizations assisting persons with a disability, public libraries, archives, educational institutions and key cultural institutions — effectively acknowledging that the scope of the current safe harbor is too narrow. However, the amendments pointedly left out commercial service providers including online platforms.[12] The amendments do not put Australian copyright law into compliance with the AUSFTA. In fact, it is clear that the amendments were framed in such a way as to specifically exclude U.S. digital services and platforms from the operation of the scheme, with members of the Australian Parliament referencing the importance of their exclusion in the parliamentary debate.[13] Further amendments to these provisions are required to make sure that limitations on liability for commercial service providers are extended to all functions provided for under Article 17.11.29(b)(i)(A-D). The failure to include online services such as

[10] Copyright Act 1968, Part V Div. 2AA.

[11] Section 116ABA of the Copyright Amendment (Service Providers) Act 2018.
[12] Copyright Amendment (Service Providers) Act 2018 https://www.legislation.gov.au/Details/C2018A00071.
[13] Copyright Amendment (Service Providers) Bill 2017, Second Reading https://parlinfo.aph.gov.au/parlInfo/download/chamber/hansards/4a4f29d6-cec4-4a55-97d8-b11f23b85dd4/toc_pdf/Senate_2018_05_10_6092_Official.pdf;fileType=application%2Fpdf#search=%22chamber/hansards/4a4f29d6-cec4-4a55-97d8-b11f23b85dd4/0258%22

search engines and commercial content distribution services disadvantages U.S. digital services in Australia and serves as a deterrent for investment in the Australian market.

Australia has also proposed amendments to the scope of the online copyright infringement scheme in section 115A of the Copyright Act 1968, including to allow injunctions to be obtained against online search providers.[14] The Australian Government has indicated that it anticipates these changes will only affect two U.S. companies.[15] In circumstances where the scheme already applies to carriage service providers, thus disabling access to Australian users to offending sites, there is no utility in the extension of these laws to other providers.

In addition, IA urges the administration to work with Australia to develop a clearer fair use exception in order to resolve uncertainty under the existing fair dealing regime. The Australian Law Reform Commission and the Australian Productivity Commission have both made positive recommendations on fair use that would enable Australia to achieve an appropriate balance in its copyright system and increase market certainty for both Australian and U.S. providers of digital services. The government should adopt these recommendations and implement "a broad, principles-based fair use exception."[16]

Unilateral Or Discriminatory Tax Regimes

In 2016, Australia's Multinationals Anti-Avoidance Law entered into force. This law appears to be outside the scope of the OECD BEPS recommendations and may impede market access for businesses seeking to serve the Australian market. In 2017, Australia passed another unilateral tax measure, the Diverted Profits Tax. Finally, in 2018, Australia has released a discussion draft which suggests it is actively considering a third unilateral tax measure, targeted exclusively at digital technology, a major US export sector. This measure is designed to circumvent the multilateral tax system and would undermine the OECD's attempts to create a globally agreed approach to taxation in the digital age. We urge the U.S. government to engage with counterparts in Australia to develop taxation principles that are consistent with international best practices.[17]

China

Data Flow Restrictions And Service Blockages

China imposes numerous requirements on internet services to host, process, and manage data locally within China, and places significant restrictions on data flows entering and leaving the country.[18]

Discriminatory Or Non-Objective Application Of Competition Regulations

Chinese competition regulators continue to use the Anti-Monopoly Law (AML) to intervene in the market to advance industrial policy goals. In many cases involving foreign companies, China's enforcement agencies have implemented the AML to advance industrial policy goals and reduce China's perceived

---

[14] The Copyright Amendment (Online Infringement) Bill 2018 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6209

[15] Explanatory Memorandum https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6209_ems_b5e338b6-e85c-4cf7-8037-35f13166ebd4/upload_pdf/687468.pdf;fileType=application/pdf.

[16] Australian Productivity Commission, April 2016 report.

[17] *Combating Multinational Tax Avoidance – A Targeted Anti-Avoidance Law*, Australian Tax Office, https://www.ato.gov.au/Business/International-tax-for-business/In-detail/Doing-business-in-Australia/Combating-multinational-tax-avoidance--a-targeted-anti-avoidance-law/.

[18] *Data localization,* AmChamChina, http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization

dependence upon foreign companies, including in cases where there is no evidence of abuse of market power or anti-competitive harm.

The Chinese companies that benefit from these policies are often national champions in industries that China considers strategic, such as commodities and high-technology. Through its AML enforcement, China seeks to strengthen such companies and, in apparent disregard of the AML, encourages them to consolidate market power, contrary to the normal purpose of competition law. By contrast, the companies that suffer are disproportionately foreign.

We urge continued U.S. government engagement on this issue to ensure that competition laws in China are not enforced in a discriminatory manner.

Electronic Payments

The People's Bank of China (PBOC) released Notification No. 7 in March 2018 that restricted foreign institutions that intend to provide electronic payment services for domestic or cross-border transactions. Notification No. 7 mandates service providers set up a Chinese entity and obtain a payments license. The PBOC has subsequently blocked foreign entities from obtaining payment license by restricting the ability to acquire existing licensed entities and by stopping foreign entities from applying for licenses, and by not approving new foreign entity applications, including for those already in the pipeline. The inconsistent interpretation has resulted in the blocking or delaying the launch and operation of new electronic payment services provided by U.S. companies.

Filtering, Censorship, And Service-Blocking

In the world's biggest market, China, the services of many U.S. internet platforms are either blocked or severely restricted. Barriers to digital trade in China continue to present significant challenges to U.S. exporters.

China imposes numerous requirements on internet services to host, process, and manage data locally within China, and places significant restrictions on data flows entering and leaving the country.[19] China actively censors – and often totally blocks – cross border internet traffic. It has been estimated that approximately 3,000 internet sites are totally blocked from the Chinese marketplace, including many of the most popular websites in the world. High-profile examples of targeted blocking of whole services include China's blocking of Facebook, Picasa, Twitter, Tumblr, Google search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare. This blocking has cost U.S. services billions of dollars, with a vast majority of U.S. companies describing Chinese internet restrictions as either "somewhat negatively" or "negatively" impacting their capacity to do business in the country.

At the same time, Chinese-based internet firms such as Baidu and Tencent are not blocked in China, nor are they blocked in the U.S. This gives Chinese firms an unfair commercial advantage over U.S.-based internet companies.

Restrictions on U.S. Cloud Service Providers

U.S. cloud services providers (CSPs) are among the strongest American exporters, supporting tens of thousands of high-paying American jobs and making a strong contribution toward a positive balance of trade. While U.S. CSPs have been at the forefront of the movement to the cloud in virtually every country in the world, China has blocked them. Draft Chinese regulations combined with existing Chinese laws are poised to force U.S. CSPs to transfer valuable U.S. intellectual property, surrender use of their brand

[19] *Data localization,* AmChamChina, http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization

names, and hand over operation and control of their business to a Chinese company in order to operate in the Chinese market. Without immediate U.S. government intervention, China is poised to implement fully these restrictions, effectively barring U.S. CSPs from operating or competing fairly in China.

Recently, China's Ministry of Industry and Information Technology (MIIT) has proposed two draft notices – Regulating Business Operation in Cloud Services Market (2016) and Cleaning up and Regulating the Internet Access Service Market (2017). These measures, together with existing licensing and foreign direct investment restrictions on foreign CSPs operating in China under the Classification Catalogue of Telecommunications Services (2015) and the Cybersecurity Law (2016), would require foreign CSPs to turn over essentially all ownership and operations to a Chinese company, forcing the transfer of incredibly valuable U.S. intellectual property and know-how to China.

More specifically, these measures 1) prohibit licensing foreign CSPs for operations; 2) actively restrict direct foreign equity participation of foreign CSPs in Chinese companies; 3) prohibit foreign CSPs from signing contracts directly with Chinese customers; 4) prohibit foreign CSPs from independently using their brands and logos to market their services; 5) prohibit foreign CSPs from contracting with Chinese telecommunication carriers for Internet connectivity; 6) restrict foreign CSPs from broadcasting IP addresses within China; 7) prohibit foreign CSPs from providing customer support to Chinese customers; and 8) require any cooperation between foreign CSPs and Chinese companies be disclosed in detail to regulators. These measures are fundamentally protectionist and anti-competitive.

Further, China's draft notices are inconsistent with its WTO commitments as well as specific commitments China has made to the U.S. Government in the past. In both September 2015 and June 2016, China agreed that measures it took to enhance cybersecurity in commercial sectors would be non-discriminatory and would not impose nationality-based conditions or restrictions.

Given this very serious situation, it is critical that the U.S. secure a Chinese commitment to allow U.S. CSPs to compete in China under their own brand names, without foreign equity restrictions or licensing limitations, and to maintain control and ownership over their technology and services. Chinese CSPs are free to operate and compete in the U.S. market, and U.S. CSPs should benefit from the same opportunity in China.

Overly Restrictive Regulation Of Online Services

China's revised Telecommunications Services Catalog released in 2015 expands regulatory oversight of new services not typically regulated as telecom services. China's classification of Cloud Computing, online platforms, and content delivery networks as Value Added Telecom Services (VATS) not only has far-reaching consequences for market access and the development of online services in China, but also runs counter to China's WTO commitments. For example, cloud computing is traditionally classified as a Computer and Related Service, not a Telecommunications Service. Applying licensing obligations to online platforms imposes a number of market access limitations and regulatory hurdles, making it more difficult for online companies to participate in the Chinese market. The Catalog subjects a broad set of services to cumbersome, unreasonable, and unnecessary licensing restrictions, imposes new conditions on Telecommunications Service suppliers with longstanding business in that country, and impedes market access to foreign suppliers of computer and related services by classifying certain computer and related services such as cloud computing as VATS.

Hong Kong

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services outside of the traditional taxi industry must be licensed under the for-hire vehicle category. In addition, for-hire vehicles face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of for-hire vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- → *License cap*: For-hire vehicle licenses (Hire Car Permit - HCP) are capped under a 1981 ordinance at 1,500.

- → *Vehicle requirement:* For-hire vehicles must have a minimum taxable value of HKD $300,000 (if the applicant can show a contract for future services, typically with a corporate client) or HKD $400,000 (if the applicant cannot show a contract for future services).

- → *Physical location requirement*: The passenger's name and trip details must be recorded at the registered physical address of the vehicle operator. Proof of demand: Operators must demonstrate the necessity of the service to the satisfaction of the regulator.

Unbalanced Copyright And Liability Frameworks

In the past years, Hong Kong had considered measures to bring its copyright law in line with the realities of digital age: including safe harbor provisions for internet intermediaries and exceptions for parody which would form a strong foundation for future reforms and further discussion of flexible exceptions and limitations. Since the draft bill in question did not pass, Hong Kong has never reactivated a discussion on amending its copyright framework. The administration should urge Hong Kong counterparts to adopt reforms introducing a safe harbor regime in line with the international practice and a broad set of limitations and exceptions which would remove market access barriers for numerous U.S. businesses by establishing a more balanced copyright framework and support the growth of national digital economy.

India

Burdensome or Discriminatory Data Protection Regimes

India's draft Data Protection bill seeks to define principles and parameters for the Indian data economy. However, in a number of respects, the Bill is far more restrictive than the EU's recently enacted GDPR, which is widely considered to be the most comprehensive regulation in the data protection sphere. Along with data localization requirements, other excessive restrictions in the Bill include:

- → New discretionary powers to local data protection authorities (DPAs), including the ability to impose draconian penalties on foreign companies, unilaterally suspend data transfers, engage in search and seizure activities, cancel the registration of 'data fiduciaries,' and order the discontinuation of certain businesses or activities;

- → Onerous obligations on 'significant data fiduciaries,' including data audits and impact assessments by DPAs; the assignment of 'data trust scores' to companies and the publication of

ratings on the DPA's website; and mandatory registration and record-keeping requirements;

→ Potentially destructive monetary penalties linked to global turnover, uncapped compensation, and inclusion of criminal penalties and non-bailable offences;

→ Definition of 'sensitive personal data' to include financial data and passwords (in conflict with global best practices on privacy), and definition of a 'child' to include anyone under 18 years old;

→ An unduly tight timeline for companies (and the government itself) to implement this new law;

→ Imposition of an EU-style 'right to be forgotten' to be adjudicated by DPAs.

IA strongly encourages the administration to engage with Indian counterparts to address these concerns and develop a privacy framework that is more consistent with global norms, as recently articulated in Art. 19.8 of the USMCA.

Data Flow Restrictions And Service Blockages

The government of India has taken several recent steps that are in deep conflict with global best practices on data governance and data localization, and which present severe market access barriers to U.S. firms.

Among other recent developments on data localization, IA is deeply concerned with the Reserve Bank of India's directive (RBI/2017-18/153, dated April 6, 2018) requiring data related to payment transactions be stored only in India. The directive, which is now in force, requires "storage of data in a system in India" without clarifying whether the data can be accessed from or transferred outside the country, even if a copy is kept in India. Other proposed measures with prescriptive requirements on data localization include a draft cloud computing policy requiring local storage of data, the draft national e-commerce policy framework, and the draft Data Protection Bill. These would harm a wide range of U.S. exporters to India and damage India's domestic digital economy.

For example, the Data Protection Bill would require companies to store a copy of all "personal data" in India, while subjecting "sensitive" personal data to even stricter requirements and mandating that "critical" personal data can only be processed within India. These definitions of personal data all remain very unclear and, if not addressed, will create significant market access barriers for U.S. firms doing business in India.

India is using data localization requirements to address concerns about security and law enforcement access to data. But these requirements will be counterproductive to India's security objectives. Data localization has been shown to increase security risks and costs by requiring storage of data in a single, centralized location, making companies more vulnerable to natural disaster, intrusion, and surveillance. In addition, localization requirements make it more difficult to implement best practices in data security, including redundant or shared storage and distributed security solutions.

Mandating local storage of data locally will not facilitate access to data by law enforcement. The U.S. and India can engage through bilateral and multilateral instruments to make data sharing work in the cloud era without resorting to data localization measures. For example, the CLOUD Act provides a path for governments that honor baseline principles of privacy, human rights, and due process to seek bilateral agreements with the U.S. on law enforcement requests. We encourage dialogue between the Department of Justice and Indian counterparts on this issue.

Data localization requirements are also deeply problematic from an economic perspective. Forced localization significantly dilutes the benefits of cloud computing and cross-border data flows, which have previously brought great benefits to India and have driven the development of India's IT industry. This approach fails to address India's economic priorities, including the government's vision of making India a trillion dollar digital economy, creating jobs, and using emerging technologies like artificial intelligence and the Internet of Things to solve the country's pressing problems.

Ultimately, forced data localization will decrease foreign direct investment, harm India's 'ease of doing business' goals, make it more difficult for local startups to access state-of-the-art technologies and global markets, and hurt Indian consumers seeking to access information and innovative products online.

IA strongly urges the administration to request the removal of data localization requirements in the RBI directive, the data protection bill, the e-commerce policy, the cloud computing policy, and other recent proposals.

Discriminatory Or Non-Objective Application Of Competition Regulations

We are aware that several Competition Commission of India (CCI) decisions have been overturned by the Competition Appellate Tribunal on procedural grounds. One way to avoid this situation is through improving CCI interaction with parties during the course of an investigation. It is important for due process and for efficiency of investigations to ensure that parties under investigation have an understanding of the issues for which they are being investigated, and have the opportunity to comment on emerging thinking and provide relevant evidence before allegations are formalized in a DG Report or finalized in an Order.

In addition, there may be more that the CCI can do to protect the confidential information of investigated parties and third parties. The improper disclosure of information, and information leaks more generally, can have a detrimental impact on the investigatory process and the standing of the agency. Providing adequate protections for this information can increase the quality of investigations by encouraging cooperation and voluntary submission of confidential information.

Barriers to Mobile Payments

In March 2017, the Reserve Bank of India released new guidelines that require mobile payment product providers to establish a local entity in order to access the market. This requirement isn't limited to financially regulated entities, and applies even to companies that are serving as a platform for licensed partners.

Blocking Foreign Direct Investment

The Ministry of Commerce, Government of India formed a think tank (or committee) to frame the E-Commerce Policy for India, a draft of which was released in July 2018. The think tank that drafted the policy did not have any representation of foreign companies. Indian promoted companies (comprising largely of companies which were Indian startups but now have substantial foreign equity invested in them) such as Snapdeal, Paytm, and Ola Cabs are represented on this think tank and aim to make the policy favorable to Indian companies in order to protect their interests. Some of the proposed clauses in the policy included provisions to enable founders to retain control of companies they have minority stakes in, mandatory disclosure of source codes to the government under domestic law, discouraging FDI in the sector through over-regulation, among others.

> E-commerce firms are globally classified under different models such as marketplace, inventory, and hybrid. While most developed countries do not distinguish between them, India continues to treat these models differently, due to pressure exerted by trader associations and Indian e-commerce firms who are looking to undermine foreign companies. India is the only country to define the marketplace model and currently, FDI is not permitted in the inventory model and is permitted only in the marketplace model, with the exception of food retail. The draft New Economic Policy recommended that limited inventory model be allowed for 100 percent made in India goods sold through platforms whose founder/promoter would be a resident Indian, where the company would be controlled by an Indian management and foreign equity would not exceed 49 percent. Despite receiving much flak for such a proposal, it is being reported that the revised draft policy is likely to keep this unchanged. India currently does not allow a hybrid model in e-commerce and has issued multiple regulations which have sought to restrict the inventory model in India, including effecting a 25 percent cap on sales from a single seller or its group companies on e-commerce platforms. The draft NEP proposed to allow Indian companies to follow an inventory model for made in India products, a provision which wasn't extended to companies with foreign equity. This was aimed at protecting the interests of companies promoted by Indian entrepreneurs over foreign equity-held companies.

Duties on Electronic Transmissions

India wants to do away with the ongoing moratorium on customs duty on electronic transmissions which goes against its current WTO obligations. Levying customs duties on electronic transmissions will hurt e-commerce companies as it will be a deterrent for buyers and sellers to transact on online platforms. It will also create barriers for India in the global e-commerce market thus adversely impacting the country's economy as well. Due to India adopting different standardization norms, smaller players may find it difficult to enter the market.

Filtering, Censorship, And Service-Blocking

Indian regional and local governments engage in a regular pattern of shutting down mobile networks in response to localized unrest, disrupting access to internet-based services.[20]

Non-IP Intermediary Liability Barriers

The United States Trade Representative correctly highlighted numerous problems with India's non-IP liability framework in the 2017 National Trade Estimate:

> India's 2011 Information Technology Rules fail to provide a robust safe harbor framework to shield online intermediaries from liability for third-party user content. Any citizen can complain that certain content is "disparaging" or "harmful," and intermediaries must respond by removing that content within 36 hours. Failure to act, even in the absence of a court order, can lead to liability for the intermediary. The absence of a safe harbor framework discourages investment to internet services that depend on user generated content.

---

[20] *India Shuts Down Kashmir Newspapers Amid Unrest*, Al Jazeera (July 17, 2016), http://www.aljazeera.com/news/2016/07/india-shuts-kashmir-newspapers-unrest-160717134759320.htmlhttp://www.aljazeera.com/news/2016/07/india-shuts-kashmir-newspapers-unrest-160717134759320.html; Betwa Sharma & Pamposh Raina, *YouTube and Facebook Remain Blocked in Kashmir*, New York Times India Ink Blog (Oct. 3, 2012), http://india.blogs.nytimes.com/2012/10/03/youtube-and-facebook-remain-blocked-in-kashmir/?_r=0http://india.blogs.nytimes.com/2012/10/03/youtube-and-facebook-remain-blocked-in-kashmir/?_r=0 (reporting on the practices of the Jammu and Kashmir governments to "increasingly [use] a communication blackout to prevent unrest in the valley.").

Safe harbors from intermediary liability are not just critical elements of balanced intellectual property enforcement frameworks; they also power digital trade and enable companies that are dependent upon intellectual property to access new markets. Where such safe harbors are incomplete or nonexistent, stakeholders in the internet sector face greater difficulty and risk in accessing these markets.

Overly Restrictive Regulation Of Online Services

In March 2015, India's telecom regulator, TRAI, issued a consultation paper on "Regulatory Framework for Over-the-Top (OTT) services."[21] There has been no response from the regulator on this paper after comments were submitted, yet it appears that the matter is still under consideration. In 2016, there have been additional consultation papers on issues including net neutrality,[22] VoIP,[23] and cloud service.[24] Many of these consultations have sought feedback on whether there is a need for regulation of OTT providers that offer such services. However, again, regulators have provided little feedback or response to industry submissions. Finally, the Ministry of Telecommunications recently released draft registration guidelines for machine-to-machine (M2M) service providers in India, with a focus on increasing regulation of M2M service providers.[25]

Restrictions on U.S. Cloud Service Providers

Cloud computing services require a highly reliable, low latency underlying network. Cloud service providers face significant regulatory challenges in operating and managing data centres in India including 1) inability to buy dark fibre in order to construct and configure their own networks, 2) a prohibition on the purchase of dual-use equipment used to manage and run those networks, 3) inability to own and manage a network to cross-connect data centers and connect directly to an Internet Exchange Point (IXP), and 4) high submarine cable landing station charges. These restrictions significantly impact the ability of cloud service providers to configure and manage its own network to optimize access by customers, to minimize latency and downtime by choosing ideal routing options, and to reduce the capex and opex costs incurred in offering cloud services in India.

Unbalanced Copyright And Liability Frameworks

India's intermediary liability framework continues to pose a significant risk to U.S. internet services. In particular, India does not have a clear safe harbor framework for online intermediaries,[26] meaning that internet services are not necessarily protected from liability in India for user actions in case of copyright infringements.

[21] TRAI, *Consultation Paper on Regulatory Framework for Over-the-Top (OTT) Services* (Mar. 27, 2015), http://www.trai.gov.in/Content/ConDis/10743_23.aspx.http://www.trai.gov.in/Content/ConDis/10743_23.aspx.

[22] TRAI, *Consultation Paper on Net Neutrality* (May 30, 2016), http://www.trai.gov.in/Content/ConDis/20775_0.aspx.

[23] TRAI, *Consultation Paper on Internet Telephony (VoIP)* (June 22, 2016), http://www.trai.gov.in/Content/ConDis/20779_0.aspx.http://www.trai.gov.in/Content/ConDis/20779_0.aspx.

[24] TRAI, *Consultation Paper on Cloud Computing* (Oct. 6, 2016), http://www.trai.gov.in/Content/ConDis/20777_0.aspx.http://www.trai.gov.in/Content/ConDis/20777_0.aspx.

[25] TRAI, *Consultation Paper on Spectrum, Roaming, and QoS related requirements in Machine-to-Machine (M2M) Communications* (Oct. 18, 2016), http://www.trai.gov.in/Content/ConDis/20798_0.aspx.http://www.trai.gov.in/Content/ConDis/20798_0.aspx.

[26] The Copyright (Amendment) Act, 2012, Section 52(1)(b)-(c) (allowing infringement exceptions for "transient or incidental storage" in transmission and, in part, "transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration . . .").

Unilateral Or Discriminatory Tax Regimes

We are deeply concerned about India's adoption of an "equalization levy," which imposes an additional 6 percent withholding tax on outbound payments to nonresident companies for digital advertising services.[27] These provisions do not provide credit for tax paid in other countries for the service provided in India. In addition, the levy targets business income even when a foreign resident does not have a permanent establishment in India, and even when underlying activities are not carried out in India, in violation of Articles 5 and 7 of the U.S.-India tax treaty. And it does this by singling out one particular activity provided through one particular mode of supply: online advertising.

This measure deviates from international agreements and is deliberately designed to circumvent double tax agreements, exposing multinationals operating in India to double taxation, essentially creating a tariff on U.S. services. This levy impedes foreign trade and increases the risk of retaliation from other countries where Indian companies are doing business.

Separately, in February 2018, India's Finance Minister introduced a measure to enact a "substantial economic presence" tax measure as of April 2019. The measure seeks to unilaterally change the definition of Permanent Establishment. It is effectively targeted at the digital sector, but may also impact other transactions outside the digital economy. This measure preempts the outcomes of the multilateral OECD process and may expose US companies to double taxation.

Indonesia

General

Indonesia's "Draft Regulation Regarding the Provision of Application and/or Content Services through the Internet" targets online services and would require platforms to take responsibility for a very broad list of content types, including content that "ruins reputation," "is contradictory to the Indonesian constitution," and "threatens the unity of Indonesia."[28] This regulation, which is part of the broader package of OTT regulations discussed below, will present significant market access barriers to U.S. providers in Indonesia.

Data Flow Restrictions And Service Blockages

The government of Indonesia has introduced a series of forced data localization measures through Ministry of Communication and Informatics Regulation 82/2012 and the more recent Draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet. These measures contain numerous market access barriers, including requirements for foreign services to "place a part of its servers at data centers within the territory of the Republic of Indonesia."[29]

Indonesia's GR82 data localization policy continues to be a significant barrier to digital trade, and is

[27] Madhav Chanchani et al., *Equalisation Levy of 6% On Digital Ad: Government Finds a Way to Tax Companies Like Google, Facebook,* The Economic Times (Mar. 2, 2016), http://economictimes.indiatimes.com/news/economy/policy/equalisation-levy-of-6-on-digital-ad-government-finds-a-way-to-tax-companies-like-google-facebook/articleshow/51216310.cms.

[28] https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/

[29] Alexander Plaum, *The Impact of Forced Data Localisation on Fundamental Rights*, Access Now (June 4, 2014), https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/.

inhibiting foreign firms' participation in Indonesian e-commerce. Indeed, U.S. firms have lost, and continue to lose, business in Indonesia from customers being told they must store their data locally. Indonesia is planning to take important steps to reform its data localization policy, including by replacing it with a data classification policy whereby only national security and intelligence data must remain onshore. This approach would be a positive step for Indonesia. However, we are concerned that there are no clear commitments to finalizing this revision, creating tremendous business uncertainty and increased compliance risks. We urge you to strongly encourage Indonesia to move swiftly in finalizing this revision.

Discriminatory Or Non-Objective Application Of Competition Regulations

Indonesia currently imposes restrictions on foreign direct investment related to e-commerce. This impairs the ability of U.S. firms to invest in Indonesia and provide local e-commerce offering. Non-Indonesian firms are prevented from directly retailing many products through electronic systems and limited to 67 percent of ownership for warehousing, logistics or physical distribution services provided that each of these services is not ancillary to the main business line. Indonesia should liberalize its FDI restrictions related to e-commerce, which limit the ability of Indonesia to grow its digital economy.

Duties On Electronic Transmissions

Indonesia has taken an unprecedented step to impose customs barriers and potentially duties on electronic transmissions. Indonesia recently issued Regulation No.17/PMK.010/2018 (Regulation 17), which amended Indonesia's Harmonized Tariff Schedule (HTS) Chapter 99 to add: "Software and other digital products transmitted electronically." Chapter 99 effectively treats an electronic transmission as a customs "import," which triggers a number of negative implications including: the imposition of customs import requirements (including declaration and other formalities) that will be impossible to meet for certain intangible products, the imposition of import duty and taxes on each electronic transmission, the creation of U.S. technology and security risks, and constraint of the free-flow of communication into Indonesia. These extremely onerous customs reporting requirements are likely to restrict international trade and may expose U.S.-originated digital transmissions to a variety of customs measures, including seizure. The inclusion of "[s]oftware and other digital products transmitted electronically" in Indonesia's HTS skirts Indonesia's commitment under the World Trade Organization (WTO) Moratorium on Customs Duties on Electronic Transmissions, a commitment that Indonesia reaffirmed as recently December 2017.

Indonesia appears to be the only country in the world that has added electronic transmissions to its HTS. Imposing customs requirements on purely digital transactions will impose significant and unnecessary compliance burdens on nearly every enterprise, including many SMEs. Indonesia's actions will establish a dangerous precedent, and will likely have the effect of encouraging other countries to violate the WTO Moratorium. In order to eliminate this barrier, Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

Overly Restrictive Regulation of Online Services

Indonesia introduced a draft law in April 2016 focused on online services ("Draft Regulation Regarding the Provision of Application and/or Content Services through the Internet") that would require data localization, creation of a local entity or permanent establishment, forced cooperation with local telecom operators offering similar services, new intermediary liability and monitoring requirements, exclusive use of a national payment gateway, and numerous other barriers that would severely impact or

cripple the ability of many internet services to do business in Indonesia.[30] The compliance and enforcement provisions of these regulations would impose significant costs on both companies and on the government, ultimately hampering the development of Indonesia's digital economy.

Unilateral Or Discriminatory Tax Regimes

Indonesia has taken steps on taxation that significantly deviate from global norms, bilateral tax treaties, and WTO commitments. These steps include proposed requirements that would compel foreign services to create a permanent establishment in order to do business in Indonesia.[31] This process would require significant resources from online service providers, many of which are small companies that lack the necessary legal and technical resources to comply with such processes, and could have significant tax consequences that conflict with OECD multilateral principles. Furthermore, this requirement would likely violate Indonesia's WTO commitments to allow computer and other services to be provided on a cross-border basis.

Japan

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services, whether as a taxi or one of the two for-hire vehicle categories ("city hire" and "other hire"), faces market access and operational restrictions that serve no public interest but are instead intended to protect incumbents.

- → *License cap:* Japanese law has capped the number of taxi and other hire licenses. Only in some jurisdictions may taxi and for-hire vehicle companies petition for additional licenses to be issued, although in practice such petitions are rarely ever successful.
- → *Minimum trip duration.* While the number of city hire licenses is not capped, city hire cars must be booked for a minimum of 2 hours.
- → *Price controls*: Regulations set a minimum price floor and a maximum price ceiling for both taxis and hire cars.
- → *"Return-to-garage" rule:* Hire car drivers must return to their registered place of business after completing every trip.
- → *Barriers to independent taxi operators*: In order to receive a license to work as an independent taxi driver—as opposed to an affiliate of a larger taxi firm—a driver must first have 10 years of experience driving for the same taxi firm and be at least 35 years old.

[30] *MCIT Issues Draft Regulation on OTT In Indonesia,* TeleGeography (May 5, 2016), https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/.

[31] Victoria Ho, *Indonesia Tells Google and Other Internet Firms to Pay Tax or Risk Getting Blocked*, Mashable (Mar. 1, 2016), http://mashable.com/2016/03/01/indonesia-tax-google/#bmvYs96AfsqF.

Unbalanced Copyright And Liability Frameworks

Despite limited exceptions for search engines[32] and some data mining activities,[33] Japanese law today does not clearly provide for the full range of limitations and exceptions necessary for the digital environment[34] – which creates significant liability risks and market access barriers for U.S. and other foreign services engaged in caching, machine learning, and other transformative uses of content.

Malaysia

Overly Restrictive Regulation Of Online Services

In Malaysia, there has been a proposal to include regulation of online services within the ambit of communications regulators. In addition, last year, the Malaysian Communications and Multimedia Commission (MCMC) decided to assess the need for improvements to the Communications and Multimedia Act (CMA).[35] The U.S. government should monitor the development of these regulatory frameworks and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach. In particular, Malaysia should avoid creating market access barriers by subjecting foreign internet services and applications to telecom-specific or public utility regulations.

New Zealand

Unbalanced Copyright And Liability Frameworks

New Zealand has made commitments to promote balance in its copyright system through exceptions and limitations to copyright for legitimate purposes, such as criticism, comment, news reporting, teaching, scholarship, and research – including limitations and exceptions for the digital environment.

New Zealand relies on a static list of purpose-based exceptions to copyright. In practice, this means that digital technologies that use copyright in ways that do not fall within the technical confines of one of the existing exceptions (such as new data mining research technologies, machine learning, or innovative cloud-based technologies) are automatically ruled out, no matter how strong the public interest in enabling that new use may be. For example, there is a fair dealing exception for news in New Zealand, but it is more restrictive than comparable exceptions in Australia and elsewhere, and does not apply to photographs – which limits its broader applicability in the digital environment.

---

[32] Copyright Law of Japan, Section 5 Art. 47-6, http://www.cric.or.jp/english/clj/cl2.html (narrowly defining the exception for search engine indexing as "for a person who engages in the business of retrieving a transmitter identification code of information which has been made transmittable . . . and of offering the result thereof, in response to a request from the public").

[33] Copyright Law of Japan, Section 5 Art. 47-7, http://www.cric.or.jp/english/clj/cl2.html (limiting the application of this data mining exception to "information analysis" done (1) on a computer, and (2) not including databases made to be used for data analysis).

[34] Approximately a decade ago, there was legislative discussion intended to facilitate the development of internet services in Japan by explicitly allowing copyright exceptions for activities such as crawling, indexing, and snippeting that are critical to the digital environment. This discussion resulted in a 2009 amendment to Japanese copyright law – however, the resulting amendment only provided narrowly defined exceptions for specific functions of web search engines, not for other digital activities and internet services. Japan continues to lack either a fair use exception or a more flexible set of limitations and exceptions appropriate to the digital environment.

[35] *Amendment to Communications and Multimedia Act 1998 in March*, Astro Awani (Feb. 22, 2016), http://english.astroawani.com/malaysia-news/amendment-communications-and-multimedia-act-1998-march-95481.

As a result, New Zealand's approach to devising purpose-based exceptions is no longer fit for purpose in a digital environment. This approach creates a market access barrier for foreign services insofar as it is unable to accommodate fair uses of content by internet services and technology companies that do not fall within the technical confines of existing exceptions. To eliminate this barrier and comply with the U.S. standard and prevailing international norms, New Zealand should adopt a flexible fair use exception modeled on the multi-factor balancing tests found in countries such as Singapore and the U.S.

Intermediary Liability

New Zealand's Copyright Act 1994 limits safe harbor caching to "temporary storage" while U.S. law and other similar provisions in U.S. FTAs include no such limitation. The definition of caching in Section 92E of the Copyright Act should be amended to remove the requirement of the storage being "temporary." This amendment would allow for greater technological flexibility and remove uncertainty surrounding the definition of "temporary." In addition, the government should clarify that under this caching exception, there is no underlying liability for the provision of referring, linking, or indexing services.

Pakistan

Overly Restrictive Regulation Of Online Services

The Pakistan Telecommunications Authority is working on a regulatory framework draft for online services, which may include licensing. Licensing could carry government access requirements, which would pose significant market access barriers for U.S. companies.[36] IA encourages the administration to monitor the development of this policy and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach, and that encourages innovation and investment.

Unilateral Or Discriminatory Tax Regimes

In May 2018, Pakistan's National Assembly passed its Finance Bill 2018 into law and created a new 5 percent withholding category for "fees for offshore digital services" on a gross basis. This unilateral law, effective as of July 2018, is a significant deviation from international tax agreements. It discriminates against US companies providing digital services to Pakistan and gives rise to double taxation.

South Korea

Burdensome or Discriminatory Data Protection Regimes

Several South Korean regulators have threatened a number of U.S. tech firms with investigations and fines for not complying with prescriptive South Korean privacy law, even though these firms do not maintain data controllers on South Korean territory. As a result, services have been forced to modify the way they do business in South Korea.

[36] *See PTA To Regulate Mobile Apps and OTT Services in Pakistan*, More News Pakistan (Aug. 20, 2016), http://www.morenews.pk/2016/08/20/pta-regulate-mobile-apps-ott-services-pakistan/.

Data Flow Restrictions And Service Blockages

Localization barriers regarding geospatial data continue to impede foreign internet services from offering online maps, navigational tools, and related applications in Korea.

Separately, a new proposed bill would require online service providers to establish local servers in order to ensure user protection from deliberate diversion of traffic and slowed service. Penalties for not complying with this requirement would include up to a 3 percent fine based on revenue.

Discriminatory Or Non-Objective Application Of Competition Regulations

In investigating U.S. companies, the Korea Fair Trade Commission (KFTC) routinely fails to provide subjects a fair opportunity to defend themselves. Lack of transparency is an issue throughout the investigative process, during which the KFTC often denies U.S. companies access to third-party and exculpatory evidence in its possession, which is excluded from their investigative report or recommendation. Respondents only get access to documents the KFTC chooses to release, which are frequently heavily redacted. It is also important to ensure that Korea is meeting the standards of Article 16.1.3 of the U.S.-Korea Free Trade Agreement, which requires that respondents have a reasonable opportunity to cross-examine any witnesses.

Korea also does not recognize the attorney-client privilege, which makes it difficult for a company to receive frank advice from counsel about the merits of an investigation and ways to comply. In addition, Korea does not respect the status of documents that are subject to attorney-client privilege in other countries, which may lead to the loss of that privilege in some contexts.

Overly Restrictive Regulation of Online Services

Congress members have proposed an OTT bill to regulate online video platforms, targeting overseas service providers.

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services must be licensed as a taxi driver. These new entrants face operational restrictions that serve no public interest but are instead intended to protect incumbents by needlessly raising the cost of the services that these new entrants can provide.

- → *Minimum/maximum price restrictions:* Prices for regular taxis are regulated. Although prices for premium taxis are—in regulation—flexible, apps cannot—in practice—set premium taxi prices below a certain floor. This de facto rule is intended to protect incumbent regular taxis.

Unbalanced Copyright And Liability Frameworks

IA has concerns with private copyright levies on smartphones/tablets.

Singapore

Sharing Economy Barriers

Any new entrant seeking to provide app-based transportation services outside of the traditional taxi industry must be licensed under the for-hire vehicle category. In addition, for-hire vehicles face market access restrictions that protect the taxi industry by limiting the number of for-hire vehicles.

→ *Exams:* In 2017, the Singapore Government introduced a new training regime for for-hire vehicle drivers that includes a 10-hour training course and challenging test. The course is delivered by a single provider—the Singapore Taxi Academy—and taught by taxi drivers. Coupled with administrative delays in the processing of background checks and applications, the driver accreditation process amounts to a significant barrier to entry for drivers, taking upwards of four months to complete.

Taiwan

Discriminatory Of Non-Objective Application Of Competition Regulations

The Taiwan Fair Trade Commission's (TFTC) investigations of U.S. companies often provide little to no insight into what issues are under investigation, as well as limited and inconsistent ability for a company to present its defense to decision-makers prior to a ruling. These procedural deficiencies are compounded by the fact that TFTC decisions are not stayed on appeal.

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services must either be licensed as a taxi driver or operate as a rental car driver (following convoluted regulatory requirements, the rider is technically renting the car from a car rental company which has sourced the driver, who then independently provides the driving service to rider/renter of the car). These new entrants face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect incumbents by limiting the number of new competing service providers, raising the price consumers must pay for those new services, and lowering the quality of the new service.

→ *License cap:* Taxi licenses are capped for taxi companies and taxi fleets and the growth in their number is pegged to the growth of each city/county's population or road expansion. (There is no license cap for individual taxi operators' licenses or for rental car licenses.)

→ *Minimum/maximum price restrictions:* Prices for taxis are regulated by local governments and constrained within a minimum price floor and maximum price ceiling. While taxis operating under the new Multi-Purpose Taxi scheme face only a price floor and not a price ceiling, access to the scheme is limited to only those taxi drivers who have an exclusive affiliation with a single taxi dispatch company and not those who operate independently or as members of a co-operative—forming a taxi dispatch company requires meeting a NTD $5 million capital requirement.

→ *Identification requirement:* Although a rider being driven by a rental car driver is not renting the car in the sense contemplated by legacy car rental regulations, the service is nevertheless governed by those regulations. As a result, the rider/renter must provide the rental car company

with her/his national identification number, as if in fact renting the car to drive herself/himself. The national identification number is a very sensitive piece of personal information, akin to the Social Security number in the U.S. Requiring riders to turn it over has a severe deterrent effect on use of rental car driver services.

Unilateral Or Discriminatory Tax Regimes

Since 2017, Taiwan's Ministry of Finance has required nonresident suppliers to collect and remit a direct tax on cross-border B2C supplies of digital goods and services, requiring suppliers to remit 20 percent of the local source component of their "deemed profit." The "deemed profit" can be as much as 30 percent of revenue. This approach, implemented unilaterally, will expose US companies to double taxation.

Thailand

Data Flow Restrictions And Service Blockages

Thailand's Personal Data Protection Bill includes a number of concerning data localization requirements.

Non-IP Intermediary Liability Barriers

Internet service providers who "assist or facilitate" the commission of defamation by another person can be liable as supporters of the defamatory offenses, even if the actor does not realize such they are assisting or facilitating the offense.[37] One webmaster faced a sentence of up to 32 years in jail under the "Lèse Majesté" law for allowing comments on an interview with a Thai man known for refusing to stand at attention during the Thai Royal Anthem.[38] Such rules have resulted in the blockage of U.S. online services in Thailand.

Vietnam

Cybersecurity Law

Vietnam's Ministry of Public Security introduced a first draft of the Law on Cyber Security (LOCS) in mid-2017. It underwent multiple revisions until it was passed by the National Assembly (NA) on June 12, 2018, and will take effect on January 1, 2019.

On October 11, the Ministry of Public Security (MOPS) introduced a new version of the draft Guiding Decree for the LOCS. The draft decree subjects almost all online services to a requirement to store a broad range of user data in Vietnam, and requires online services to disclose that data in unencrypted form to the Ministry of Public Security. Article 59.1 requires a provider of these services to store "personal data" of users in Vietnam. Personal data is also defined broadly to include name, contact details, ID number, occupation, financial details, medical records, hobbies, political views, biometrics, and other information. Under Article 59.2, the MOPS may request access to personal data as well as other data generated while using a service, and the service provider must disclose such data in a decrypted format. In addition, the draft provides broadly designed criteria to identify "critical information systems," which may enable the MOPS to extend the scope of regulation to privately-owned systems.

[37] https://www.law.uw.edu/media/1423/thailand-intermediary-liability-of-isps-defamation.pdf

[38] https://www.eff.org/deeplinks/2012/05/suspended-sentence-good-news-thai-webmaster-jiew-threat-freedom-expression-remains

These data localization, licensing, and representative office requirements would affect U.S. business quite broadly, forcing companies to adjust their investment strategies or abandon their business in the country. The U.S. should strongly encourage Vietnam to take certain steps to minimize the commercial impact of this bill.

Data Flow Restrictions And Service Blockages

Under the Decree on Information Technology Services (Decree No. 72/2013/ND-CP), Vietnam requires a wide range of internet and digital services to locate a server within Vietnam. In addition, Vietnam's Ministry of Information and Communications recently introduced a new draft decree (Draft Decree Amending Decree 72/2013-ND-CP) that would implement new data retention requirements, local presence requirements, interconnection requirements, and additional server localization requirements. Finally, Vietnam's Law on Cyber Security includes significant data localization requirements.

Non-IP Intermediary Liability

Vietnam's Ministry of Information and Communications has introduced a new decree on the use of Internet Services and Online Information that includes an excessively short 3-hour window for compliance with content takedown requests, as well as numerous other market access barriers [39]

Unfortunately, the requirements in this decree deviate from international standards on intermediary liability frameworks, and would present significant barriers to companies seeking to do business in Vietnam. Online services often require more than 3 hours to process, evaluate, and address takedown requests, particularly in situations where there are translation difficulties, different potential interpretations of content, or ambiguities in the governing legal framework.

A similar intermediary liability provision in India has forced U.S. services "to choose between needlessly censoring their customers and subjecting themselves to the possibility of legal action." IA urges the administration to take similar action on this Vietnamese decree and to highlight that this decree would serve as a market access barrier. In addition, we encourage the administration to work with Vietnam and other countries to develop intermediary liability protections that are consistent with U.S. law and relevant provisions in trade agreements, including Section 230 of the Communications Decency Act and Section 512 of the Digital Millennium Copyright Act.[40]

This draft decree also includes long and inflexible data retention requirements, a requirement for all companies to maintain local servers in Vietnam, local presence requirements for foreign game service providers, requirements to interconnect with local payment support service providers, and other market access barriers that will harm both U.S. and Vietnamese firms.

Finally, IA urges the administration to press Vietnam for greater transparency and public input into the development of internet-related proposals. This recent decree was publicized on a Friday, and comments on the decree were due on the following Monday. Such short windows do not provide sufficient time for expert input into the development of complex regulations, and are inconsistent with

[39] Draft Decree Amending Decree 72/2013-ND-CP on the Management, Provision and Use of Internet Services and Information Content Online.

[40] In particular, Vietnam must at a minimum include express and unambiguous limitations on liability covering the transmitting, caching, storing, and linking functions for its ISP safe harbors; revise Article 5(1) of Joint Circular No. 07/2012 to provide a safe harbor for storage rather than just "temporary" storage; and clarify that it's safe harbor framework does not include any requirements to monitor content and communications.

Vietnam's obligations under Chapter 26 of the TPP ("Transparency and Anti-Corruption") to provide for notice-and-comment processes when developing new regulations.

Overly Restrictive Regulation Of Online Services

In 2014 and 2015, Vietnam's government released two draft regulations appearing to target foreign providers of internet services. In October 2014, the Ministry of Information and Communications released a draft "Circular on Managing the Provision and Use of Internet-based Voice and Text Services," proposing unreasonable regulatory restrictions on online voice and video services. These restrictions would require foreign service providers to either:

- → Install a local server to store data or
- → Enter into a commercial agreement with a Vietnam-licensed telecommunications company.[41]

The government of Vietnam also promulgated a draft IT Services Decree that would have included additional data localization requirements as well as restrictions on cross-border data flows.

While the government of Vietnam has apparently not taken any additional action on these measures, the administration should monitor this or any similar requirements. In particular, the administration should continue to resist any efforts that would prevent foreign providers from supplying internet services in Vietnam unless they enter into a commercial agreement with local telecommunications companies.

Sharing Economy Barriers

Vietnam has established a specific regulatory framework for for-hire vehicles working through apps ("e-contract"). License cap: Cities across Vietnam, including Hanoi and Ho Chi Minh City, have announced their intent to impose a cap on the number of e-contract vehicles. While such caps already exist in certain cities for taxis and traditional for-hire vehicles not working through smartphone apps, these caps are not enforced.

- → *Independent operation restriction:* Vietnam currently requires that all e-contract drivers affiliate with a transport company or transport cooperative, limiting the flexibility and autonomy that attracts drivers to work via apps. This requirement does not apply to traditional for-hire vehicle vehicles not working through apps, which can operate on an independent operator basis.

Unbalanced Copyright And Liability Frameworks

Vietnam does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Vietnamese law provides a short list of exceptions that do not clearly cover core digital economy activities such as text and data mining, machine learning, and indexing of content. IA urges the administration to work with Vietnam to implement a flexible fair use exception modeled on the multi-factor balancing tests found in countries such as Singapore and the U.S. [42]

Vietnam also inhibits U.S. digital trade by failing to provide for adequate and effective ISP safe harbors. IA encourages the administration to work with Vietnam to implement safe harbors that are consistent with Section 512 of the Digital Millennium Copyright Act.

---

[41] *Circular Regulates OTT Services*, Vietnam News (Nov. 15, 2014), http://vietnamnews.vn/economy/262825/circular-regulates-ott-services.html#qvpySzIcYMz25vCl.http://vietnamnews.vn/economy/262825/circular-regulates-ott-services.html#qvpySzIcYMz25vCl.97 97.

[42] Law on Intellectual Property (as amended, 2009), Art. 25, 26.