Internet Association

Submission For The 2021 USTR National Trade Estimate Report

Docket No. USTR-2020-0034

Contents

Introduction

On behalf of the world's leading internet companies, Internet Association (IA)[1] is pleased to submit the following comments to the Trade Policy Staff Committee (Docket Number USTR-2020-0034) for consideration as the Office of the United States Trade Representative (USTR) prepares the 2021 National Trade Estimate Report (NTE).

IA 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.

The pandemic has only underlined how important digital policy is, as more business is conducted online and information flows keep the economy going and all of connected while remaining socially distant. Yet internet businesses have continued to face significant challenges around the world that are undermining the United States' (U.S.'s) leadership in the digital economy and the global nature of the free and open internet. We see restrictions on digital trade growing – with an increasing number of governments pursuing 'beggar thy neighbor' digital economy policies that seek to exclude or restrict U.S. digital services or force value transfer from foreign to local businesses. Indeed, China's and Russia's past calls for "cyber sovereignty" and siloed digital economies are now surfacing, in different forms, elsewhere around the world.

Notably, since the European elections in 2019, European Union (EU) leaders have actively promoted an aggressive, multi-pronged approach towards "technology sovereignty" as one of the two main policy objectives for the current EU Commission. Under this new policy umbrella, the EU is proposing new regulatory 'ex ante' rules that would apply almost exclusively to U.S. platforms (under a new, sweeping Digital Services Act), as well as restrictions on cloud services, artificial intelligence, and data. EU officials have stated that the purpose of digital sovereignty is to create a "new empire" of European industrial powerhouses to resist American rivals. These unilateral regulations appear designed to discriminate against U.S. companies and to take aim at a slice of the $517 billion U.S. digital export market.

In the meantime, an increasing number of foreign trading partners have imposed unilateral digital services taxes (DSTs) over the past year, unfairly targeting U.S. digital companies while insulating domestic competitors from the scope of taxation. While previous DST proposals mostly emanated from the EU, governments outside of the EU including Kenya, Indonesia, and India have now jumped on the bandwagon, underscoring the risk of contagion if such discriminatory measures are not nipped in the bud. The budgetary pressures faced by many governments to fund economic recovery efforts from COVID-19 may inspire more unilateral measures that are designed to discriminate against and extract unfairly from U.S. companies.

Over the past year, some foreign governments have also devised new ways of targeting U.S. digital companies and reducing their space to operate in foreign markets while protecting their domestic industries. Australia's draft News Media and Digital Platforms Mandatory Bargaining Code requires U.S. digital companies to carry domestic Australian news content, transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms.

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

Meanwhile, barriers hindering U.S. digital trade in countries such as Vietnam, Indonesia, and India remain in place, notably in their adoption of forced data localization policies that pose a fundamental threat to the free flow of information across borders. The EU adopted a Copyright Directive that diverges sharply from the U.S. model, using copyright not to promote innovation, but instead to limit market access by online services. The continued push by some countries to abandon the WTO moratorium on duties on electronic transmission – notably India, Indonesia, and South Africa – would have a detrimental impact on how data and digital products flow and add value to the world.

In order to preserve and expand the internet's role as a driver of U.S. exports, economic development, and success, USTR must continue to defend the U.S. internet framework and push back on digital market access barriers that threaten the internet's growth and export-enabling potential. IA applauds the strong steps that USTR took on these issues in the U.S.-Mexico-Canada Agreement (USMCA) and Japan Trade Agreement as well as in its submissions to the WTO e-commerce talks, but there is more to be done. IA urges the USTR to act decisively and quickly in order to prevent the rapid expansion of harmful initiatives and measures such as the EU's digital sovereignty efforts that target U.S. digital companies. IA welcomes the USTR's initiation of investigations with respect to DSTs adopted or under consideration in 10 jurisdictions, and urges the USTR to continue to be on high alert for similar DST or other measures that specifically target the U.S. digital sector. Without a strong response from the USTR, U.S. digital leadership and the ability of U.S. businesses, including small businesses, to reach 95 percent of the world's customers through U.S. internet services could be in jeopardy.

In the last half a decade, USTR has deepened its focus on digital trade barriers, with the understanding that digital trade represents a critical element of U.S. competitiveness and a key source of U.S. innovation and growth – not just for the tech sector but also for manufacturing, agriculture, and other industries.[2] In the 2020 NTE, USTR laid out the growing number of laws and regulations around the world that block the flow of data across borders, limit cloud computing, discriminatorily tax, and otherwise restrict the ability of American internet companies to compete globally. IA appreciates USTR's continued leadership and encourages the goal of preserving and expanding the internet's role as a key driver of U.S. exports, job creation, and economic development by making digital trade a top priority in the 2021 NTE Report and its trade agenda.

[2]https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2020/march/fact-sheet-2020-national-trade-estimate-strong-binding-rules-advance-digital-trade

American Digital Trade Leadership

The U.S. is the global internet and digital content leader. The digital economy has led to amazing products, lower prices, and new jobs, and American has spearheaded digitally driven export growth across borders, with digital trade now accounting for more than 59 percent of all U.S. services exports.

All industries — and businesses of all sizes — reap the rewards of the U.S.'s digital leadership. Small businesses and entrepreneurs in every U.S. 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. The internet cuts the trade deficit in every sector of the economy. Figures from BEA show that in 2019 the U.S.' overall digital exports were $517.5 billion and U.S. digital trade surplus increased to $219.9 billion from $179.6 billion in 2016.[3]

America's digital leadership didn't just happen – existing U.S. law and policy are central to the country's success and fostering the adoption and use of digital technologies here and around the world. They are also central to supporting American small business growth.

But the U.S.' digital leadership is at risk of being eroded and undermined. There's a global race to set the rules for the digital economy. USTR should use trade deals to fight for adoption of America's digital framework across the world and at the same time defend against attacks on U.S. technology leadership. Other countries are adopting policies that threaten the success of the U.S. digital economy both in the U.S. and abroad, and these countries are also actively pressuring their trading partners to adopt such policies. China's recent "Global Initiative on Data Security" is one example of China's desire to promulgate a vision of the internet and digital trade that runs contrary to U.S. interests and values.

USTR should focus on the inclusion of the free flow of information, intermediary liability protections, a strong and innovation oriented, copyright framework, and streamlined and simplified trade facilitation and customs procedures in future agreements.

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. As a result, online platforms support 425,000 U.S. jobs and $44 billion in U.S. GDP annually.[4] If online services are held liable for third-party content that they do not develop or create – or disincentivized from taking Good Samaritan actions to remove spam and abusive content – the services would not be able to operate in such an open manner. For example, if online services were held liable for consumer reviews, then they would not be able to serve as platforms for millions of American small businesses to build brand awareness in new markets and reach global customers.

[3]https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=6&isuri=1&tablelist=357&product=4
[4]https://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf

The U.S. has a strong and innovation-oriented copyright framework that protects creators' legitimate rights, enables new innovation, and generates massive consumer benefits – 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 the economy, and generate $368 billion in exports annually.[5] They hold the key to future U.S. innovation, including in areas like artificial intelligence that depend upon copyright exceptions to enable machine analysis of data. A safe harbor system that protects the interests of copyright holders, online service providers, and users by defining the responsibilities of each and the incentives for collaboration among them is an important part of U.S. trade policy.

E-commerce is enabling millions of American small businesses to find customers and make sales around the world in ways impossible just a few 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.

[5] http://www.ccianet.org/wp-content/uploads/2017/06/Fair-Use-in-the-U.S.-Economy-2017.pdf

Key Issues Impacting Internet Companies Around the World

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

- → Copyright-Related Barriers
- → Customs Barriers To Growth In E-Commerce
- → Data Flow Restrictions And Service Blockages
- → Discriminatory Or Opaque Application Of Competition Regulations
- → Divergence From Privacy Best Practices
- → Filtering, Censorship, And Service-Blocking
- → Infrastructure-Based Regulation Of Online Services
- → Non-IP Intermediary Liability Restrictions
- → Restrictions On Cloud Service Providers
- → Sharing Economy Barriers
- → Unilateral Or Discriminatory Digital Tax Measures

Copyright-Related Barriers

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 Copyright Act, as enacted by 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 – requires balanced copyright rules to do business in foreign markets.

In countries that lack a balanced model of copyright law, U.S. innovators are at a significant disadvantage. Increasingly, governments like the EU (including Spain, Germany, and France), Australia, Brazil, Colombia, India, and Ukraine 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. The EU's Copyright Directive directly conflicts with U.S. law and requires a broad range of U.S. consumer and enterprise firms to install filtering technologies, pay European organizations for activities that are entirely lawful under the U.S. copyright framework, and face direct liability for third-party content. Critically, such "must carry and must pay laws" are not only antithetical to U.S. copyright theory, but are in effect measures designed to subsidise and protect domestic industries at the expense of U.S. digital innovators and exporters.

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 1 in 8 U.S. workers.[6] Unfortunately, foreign trading partners lack these innovation-oriented rules, which limit the export opportunities for U.S. industries in those markets.

In addition, Section 512 of the Copyright Act, as enacted by 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.[7] And yet key trading partners have failed to implement ISP safe harbors, including three countries (Australia, Colombia, and Peru) that have express obligations to enact safe harbors under trade agreements with the U.S.

USTR has promoted copyright safe harbors in trade agreements for the last 15 years, including in the USMCA, with the recent legal reform in Mexico to implement these policies as an example for other regions. 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.

IA urges USTR to step up enforcement of copyright safe harbors in existing trade agreements and use upcoming trade negotiations to promote a strong and balanced copyright framework that benefits all U.S. stakeholders. Companies, especially startup platforms, need consistent and clear legal frameworks to compete globally. A patchwork of copyright liability frameworks would not only impose new risk and cost on startups, but would be confusing to navigate and put startups at a disadvantage that could hinder their growth. USTR should adopt an even-handed approach to copyright enforcement and work to advance the interests of all U.S. industries and not just that of rights holders. Without the promotion and enforcement of these business-critical protections, internet services – and the industries they enable – face troubling legal risks, even when they follow U.S. law.

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 USTR to identify these issues as key impediments to digital trade in the 2021 NTE and work with foreign countries to modernize these

[6] Capital Trade. "Fair Use in the U.S. Economy." http://www.ccianet.org/wp-content/uploads/library/CCIA-FairUseintheUSEconomy-2011.pdf.
[7] http://internetassociation.org/wp-content/uploads/2017/06/NERA-Intermediary-Liability-Two-Pager.pdf

antiquated systems and overly burdensome systems. When it comes to USMCA, IA urges USTR to undertake intensive work with Mexico to fully implement the agreement. In particular, IA encourages the parties to work to ensure that the provisions related to tax and duty collection and procedures for low value shipments do not lead to additional obstacles for small businesses exporting to Canada and Mexico.[8]

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 in order to eliminate trade barriers that restrict commerce or deny U.S.-based internet services the freedom to operate in a foreign jurisdiction.

Data localization mandates are increasingly inhibiting U.S. companies from serving foreign markets on a cross-border basis and undermining their competitiveness within foreign countries, cutting into U.S. job and export growth while damaging U.S. security. China and Russia have led the way in implementing data localization requirements, but other countries including India, Indonesia, Saudi Arabia, South Korea, and Vietnam are following suit, often at the behest of local firms. It is important for the U.S. government to take a strong stance against these measures, which harm U.S. exports and threaten U.S. jobs linked to digital trade.

In 2018, Indonesia issued draft regulatory amendments to localize certain classes of data, Vietnam passed a Cybersecurity Law with undefined and potentially broad localization requirements, India released a draft personal data protection bill that seeks to localize certain classes of personal data, and 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 their 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 disasters, intrusion, and surveillance. Other countries have numerous other less trade-restrictive options available to them that more effectively accomplish these policy objectives. 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.

Divergence From Privacy Best Practices

Data has revolutionized every part of the economy and people's 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 around the world are creating new privacy laws and other measures to regulate how companies handle data. While many of these privacy measures are

[8] https://internetassociation.org/us-mexico-canada-agreement/

appropriate, some are clearly out of sync with global privacy norms and best practices. In addition, this emerging array of laws and regulations risks creating a "patchwork" effect that complicates compliance efforts and leads to inconsistent experiences for consumers and businesses.

IA's member companies believe trust is fundamental to their relationship with their users and customers.[9] They 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's 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, they 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 USTR to ensure that privacy protections are implemented in an objective and non-discriminatory way. A good example on this matter is the reference of the APEC Privacy Framework in the USMCA, to ensure that the parties will take these privacy principles into account when facilitating the cross-border free flow of data in an informed (to the data subjects) and secure way. A number of countries have started moving forward with laws that are problematic in this respect, such as the adhesion of some Latin American countries to treaties such as the European Convention 108 and 108+ which hinder the free flow of data across borders.

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. Where regulations fall short of this standard, IA encourages USTR to identify these issues in the 2021 NTE as key impediments to digital trade.

Non-IP Intermediary Liability Restrictions

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 when platforms are able to 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 allows U.S. services to function as platforms for trade and communication, is increasingly under threat abroad. USTR has rightly identified "unreasonable burdens on internet platforms for non-IP-related liability for user-generated content and activity" as a barrier to digital trade in the last two NTE reports. Yet this state of affairs has not improved. 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, political dissent, and

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

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.

IA encourages USTR to identify the increasing number of non-IP liability trade barriers abroad and use upcoming trade negotiations and additional engagements to set clear rules that would prohibit governments from making online services liable for third-party content.

Infrastructure-Based 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 barriers to entry; 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.[10]

Yet numerous foreign governments – Brazil, Colombia, the EU (as well as several Member States including Italy, Germany, France, and Spain), Ghana, India, Indonesia, Japan, Kenya, Thailand, Vietnam, and Zimbabwe, among others – 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.

To maintain and capitalize on the clear U.S. competitive advantage in this area, IA urges USTR to identify legal or regulatory measures that are harming the deployment of online services to consumers and businesses and to engage with foreign counterparts to address these market access barriers. IA also encourages USTR to continue working to introduce disciplines on OTT regulations into ongoing trade negotiations.

Unilateral Or Discriminatory Digital Tax Measures

An increasing number of foreign trading partners are proposing discriminatory 1.5 to 7.5 percent revenue taxes on digital services provided by U.S. technology firms. These digital services taxes are narrow in scope and are specifically designed to target U.S. digital companies while insulating foreign competitors from the scope of taxation. In many cases, these taxation measures contradict longstanding global consensus-based practices (e.g., by taxing gross revenues instead of income) and would result in double taxation on American businesses. Unfortunately, these tax regimes are on the rise globally. The majority of DSTs have three core problems from a trade perspective: they discriminate against U.S.

[10] "The Economic and Societal Value of Rich Interaction Applications (RIAs)." WIK, 2017. http://www.wik.org/fileadmin/Studien/2017/CCIA_RIA_Report.pdf

companies by design; they undermine the competitiveness of the impacted U.S. companies relative to domestic suppliers of the same services; and, in some cases, they have retroactive application. In addition, by taxing gross revenue instead of profits, DSTs do not account for real costs of doing business, such as R&D or capital expenditures. This feature increases the cost of capital and discourages investment and innovation for all companies in scope and particularly for companies in loss positions or those with low margins. The DSTs are often arbitrary not just in their scope and rate but also their taxable base, as many DSTs focus on user participation which results in taxation of activity that does not generate any actual realized or recognized income. Such a departure from fundamental concepts like taxing net profit or realized income is a concerning precedent that further supports the need for international consensus.

IA believes that global tax rules should be updated for the digital age, but discriminatory go-it-alone taxes targeted against U.S. firms are not the right approach. IA urges countries to withdraw discriminatory digital tax measures and to continue working within the Organisation for Economic Co-operation and Development (OECD) process, including re-engaging on Pillar I, as the OECD remains the best venue for resolving global taxation.[11] It is positive that over 135 members of the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting agreed to a road map for resolving these tax challenges and committed to working toward a consensus-based long-term solution.[12] If re-engagement at the OECD is not currently feasible due to the global pandemic, it is important for countries to create an updated plan for when the Pillar I process can continue and not resort to creating or expanding unilateral measures during this time. Throughout the process, it is critical that the U.S. emphasizes the value of reaching a compromise that results in the taxation of net income, not gross revenue. The final product must be fair to the U.S., the American digital industry, and the countless small businesses that depend on information flows and digital services to engage in commerce around the world.

The internet industry applauds USTR initiating investigations with respect to DSTs adopted or under consideration by France, Austria, Brazil, the Czech Republic, the EU, India, Indonesia, Italy, Spain, Turkey, and the UK, which specifically target the U.S. digital sector.

USTR's Section 301 investigation into France's DST last year was an important step in exercising American leadership to stem the tide of new discriminatory taxes, and to push countries towards a multilateral OECD solution. That investigation correctly determined that the French DST discriminates against U.S. digital companies, contravenes prevailing tax principles (due to its retroactivity, its application to revenue rather than income, and its extraterritorial application), and unreasonably burdens U.S. commerce. Unfortunately, recent statements from the French government indicate an attempt to double down on discriminatory taxation towards U.S. companies, both nationally and at the European level. For example, the French junior economic minister stated on June 25 that an EU-wide digital services tax would be an important step to "restore Europe's digital sovereignty by charging for access to our single market."[13] Similarly, a June 17 letter from the UK, Spanish, French, and Italian governments framed the DST as a tool to address "digital giants" that currently "benefit from free access to the European market."[14]

[11] http://www.oecd.org/tax/beps/
[12] https://www.oecd.org/tax/beps/programme-of-work-to-develop-a-consensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.pdf
[13] http://www.senat.fr/cra/s20200624/s20200624_0.html
[14] Letter to Secretary Mnuchin from Bruno Le Maire, María Jesús Montero Cuadrado, Roberto Gualtieri, and Rishi Sunak, June 17, 2020.

In the meantime, countries beyond Europe – including India, Indonesia, Kenya, and Turkey – have developed or implemented digital taxes on U.S. companies, often with the express purpose of using new tax revenue from U.S. companies to fund local economic recovery. These new digital taxes unfairly and unilaterally appropriate tax revenue that would otherwise be due to the United States.

Additional countries not named in USTR's recent 301 investigation are also reportedly considering DSTs, including Belgium, Hungary, Nigeria, Pakistan, and the Philippines. The USTR should pay close attention and if warranted, investigate these countries' measures under 301, as they would be unreasonable and would discriminate against U.S. digital companies.

Emerging Issues

Finally, with the rapid pace of internet innovation, IA calls on USTR 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. IA urges USTR to ensure that any cross-cutting regulations are implemented in an objective and non-discriminatory way. Where regulations fall short of this standard, IA encourages USTR to identify these issues as key impediments to digital trade in the 2021 NTE.

Foreign Digital Trade Barriers

Argentina

Copyright-Related Barriers

The lack of a framework on intermediary liability protections in Argentina has led to significant uncertainty for foreign firms seeking to do business in Argentina. IA supports Bill 0942-S-2016, which provides a clear framework that limits the liability of intermediaries for content generated, published, or uploaded by users until they are given appropriate notice under Argentine law.

Customs Barriers To Growth In E-Commerce

In recent years the government of Argentina (GOA) has sought to reform the customs agency and has made positive strides. In 2016, the GOA implemented the Comprehensive Import Monitoring System (SIMI) in order to promote competitiveness and facilitate trade, while maintaining sufficient controls to manage risks. The SIMI established three different low-value import regimes (Postal, Express Courier, and General). However, given the challenges that persist in clearing goods through the General import regime, only the Express Courier regime works functionally for e-commerce transactions. Thus, the limits within the Express regime create serious roadblocks for U.S. companies seeking to export to Argentina. The Express regime limits shipments to packages under 50 kilograms and under $1,000, with a limit of three of the same items per shipment, with duties and taxes assessed. While import

certificates and licenses for products are not required, the government limits the number of shipments per year per person to five, which is strictly enforced. U.S. companies have had to stop exporting to Argentina altogether given the complexities within the General regime and the inability to know how many shipments a customer has already received.

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:* The City of Buenos Aires has enacted a supply cap of an arbitrary maximum of 2,500 for-hire vehicles.
- *Independent operator restriction:* All for-hire vehicles must be affiliated with a for-hire agency and work exclusively for that agency.
- *Return-to-garage rule:* For-hire vehicles are required to return to their registered place of business between trips.
- *Technology restrictions:* For-hire vehicles may be solicited only by either a phone call or email.

Unilateral Or Discriminatory Digital Tax Measures

Over the past twelve months, the Argentine government has applied a series of capital controls and new tax measures to the consumption of imports in an effort to make it more challenging for Argentine citizens to import goods and services. On October 28, 2019, the Central Bank established a limit of $200 per month that citizens were able to access through their bank accounts, limiting the amount of money those citizens could use to import goods and services. On December 23, 2019, the executive branch issued Decree 99/2019, implementing a temporary 30 percent tax (“PAIS tax”) on the purchase of foreign currency and purchases made online invoiced in foreign currency, among other things. And on September 16, 2020 the Central Bank introduced a new 35 percent tax on foreign currency purchases, including on cross-border transactions made with credit cards, to "discourage the demand for foreign currency.” Combined, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers.

Australia

General

Australia’s Telecommunications and Other Legislation (Assistance and Access) Act is a significant barrier to trade for U.S. technology companies. The law’s obligations are unprecedented and fundamentally unworkable. The law detrimentally affects the ability of businesses to rely on the safety and security of any digital service, the internet, or technology more generally. Legally introduced

security vulnerabilities designed to overcome encryption and other security features would have a material impact on any industry relying on encryption 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 law,

Australia introduces significant risk that may compel foreign technology providers to cease operations in and exports to Australia.

Copyright-Related Barriers

Under the Australia-U.S. Free Trade Agreement (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).[15] Instead, only a narrower subset of " service providers" are covered under Australian law,[16] rather than the broader definition of "internet service providers" in the AUSFTA. 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 USTR and others in the U.S. government 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.

In 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.[17] 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.[18] 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 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.[19] The Australian Government has indicated that it anticipates these changes will only

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

[16] Section 116ABA of the Copyright Amendment (Service Providers) Act 2018.
[17] Copyright Amendment (Service Providers) Act 2018 https://www.legislation.gov.au/Details/C2018A00071.
[18] 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

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

affect two U.S. companies.[20] 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 USTR 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."[21]

Discriminatory Or Opaque Application Of Competition Regulations

In July 2020, the Australian Government released its draft News Media and Digital Platforms Mandatory Bargaining Code, via amendment to the Australian Competition and Consumer Act.[22] The internet industry has strong concerns that the Code violates Australia's trade obligations and unfairly discriminates against U.S. companies. IA is expressly concerned that the Code targets two U.S. digital companies to assist a class of domestic players in a way that runs counter to Australia's international trade commitments. The ACCC's proposed Code would improperly require proprietary information sharing by U.S. digital platforms without transparent standards or safeguards, and would set a dangerous precedent of political interference in Australia's digital economy. Finally, the Code presents an unfair and arbitrary treatment of foreign investors. Given the wide ramifications, we believe the ACCC should reconsider its proposed legislation and pursue a balanced solution for Australia's digital economy and consumers. The draft code, if enacted in its current form, would run counter to Australia's trade obligations in the over fifteen-year-old AUSFTA as well as the WTO General Agreement on Trade in Services (GATS). It is also at odds with Australia's history of leadership in promoting cross-border digital trade.[23]

Non-IP Intermediary Liability Restrictions

Australia has passed and subsequently amended legislation that imposes civil liability on intermediaries in the context of online safety. The Enhancing Online Safety Act of 2015 includes powers to fine social media services or designated internet services for failing to remove cyberbullying material or intimate images.

The Criminal Code Amendment (Sharing of Abhorrent Material) Act was rushed through Australia's Parliament in early 2019 with no public consultation, putting in place disproportionate and ambiguous provisions targeting the removal of online terrorism content.[24] The act applies to an excessively broad range of technology companies, and has increased compliance risks for U.S. based social media,

[20] 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.
[21] Australian Productivity Commission, April 2016 report.
[22] *Draft News Media and Digital Platforms Bargaining Code - draft legislation and explanatory materials,* Australian Competition and Consumer Commission https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/draft-legislation
[23] Internet Association Comments On The Australian Government's Draft News Media Bargaining Code https://internetassociation.org/files/ia_comments-on-accc-draft-news-media-bargaining-code_august-2020_trade-pdf
[24]https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf

user-generated content and live streaming services, and hosting services. Its wide-ranging provisions give no consideration to the different business models of technology companies or their varying capabilities or roles in facilitating the sharing of abhorrent violent material online. It is markedly out of step with approaches in other countries, particularly in terms of its excessively broad scope and the regulatory framework applying to traditional media companies in Australia.[25]

On June 24, 2019, the Supreme Court of New South Wales, in a pretrial ruling for Voller v Nationwide News Pty Ltd; Voller v Fairfax Media Publications Pty Ltd; Voller v Australian News Channel Pty Ltd, ruled that mainstream media organizations are liable for the content posted by third party users on Facebook pages operated by these companies. The judgment specifies that the responsibility for the publication was "wholly in the hands of the media company that owns the public Facebook page." This ruling came out of a case where a former youth detention inmate sued media organizations like the Sydney Morning Herald for comments that members of the public made about him on Facebook posts and pages of the media organizations. Critics stated that the ruling was an overreach and would put a significant burden on media organizations to monitor their online presence and increase liability. Similarly, courts in several State jurisdictions in Australia have found Google liable for publishing defamatory content through links within Google Search.

Unilateral Or Discriminatory Digital Tax Measures

In 2016, Australia's Multinationals Anti-Avoidance Law entered into force. This law appears to be outside the scope of the OECD Base Erosion and Profit Sharing (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 released a discussion draft which suggests it is actively considering a third unilateral tax measure, targeted exclusively at digital technology, a major U.S. 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. IA urges the U.S. government to engage with counterparts in Australia to develop taxation principles that are consistent with international best practices.[26]

Bahrain

Divergence From Privacy Best Practices

Bahrain's Personal Data Protection Law, known as "PDPL" (Law No. 30 of 2018) came into force in August 2019, 12 months after its publication in the official gazette, and supersedes any law with contradictory provisions. While many companies active in Bahrain are seeking to comply with the requirements set out in the Personal Data Protection Law, the fact that associated Regulations have not yet been issued makes this difficult. Furthermore the fact that the Data Protection Authority contemplated in the law has not yet been established creates further ambiguity, even though Bahrain's Ministry of Justice is temporarily assuming the functions and powers prescribed to the Data Protection Authority until an independent Authority is allocated a budget and a board of directors is established.

[25] https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html
[26] *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/.

Restrictions On Cloud Service Providers

Effective starting October 2017, the Central Bank of Bahrain (CBB) Rulebook outlined in section OM-3.9.7 that conventional banks which utilize outsourced cloud services must ensure that various security requirements are implemented to safeguard personal data. These rules are generally compatible with global norms. However, these rules also require that licensees seek CBB's prior written approval to outsource functions or services that contain customer information, which discourages adoption of cloud. CBB reserves the right to order licensees to make alternative outsourcing arrangements in the event of a breach of confidential information or when CBB feels that it cannot adequately execute its supervisory functions, leaving cloud providers exposed.

Bahrain's Personal Data Protection Law prohibits the transfer of personal data out of Bahrain unless it is transferred to a country the Authority includes on its list of approved countries. The List, yet to be published, will consist of countries that, in the view of the Authority, have sufficient personal data protections. Transfers to countries that are not on the List are permitted in limited circumstances, for example, where the data owner provides consent or the data was obtained from a public source. This will obviously create further restrictions on Cloud Service Providers.

Bangladesh

Non-IP Intermediary Liability Restrictions

The Digital Security Act of 2018 gives the government broad powers to suppress "information published or propagated in digital media that hampers the nation or any part therein in terms of nations unity, financial activities, security, defense, religious values, public discipline or incites racism and hatred" and created new criminal provisions prohibiting publication of content online that may be defamatory, harmful to religious values, or critical of the government.[27] Service providers may only defend themselves if they can prove that they took all possible steps to try to prevent publication of material that violates the law or they will be subject to criminal penalties, including fines and/or imprisonment.

Unilateral Or Discriminatory Digital Tax Measures

Bangladesh has a 15 percent value-added tax (VAT) on digital sales. However, the National Board of Revenue (NBR) has not implemented a mechanism to allow non-resident service providers to register and remit tax dues.

Belarus

Non-IP Intermediary Liability Restrictions

Amendments to the Law on Mass Media made in 2018 have resulted in significant fines against media entities, including online blogs; new requirements to filter online content and government powers to mandate its removal; limitations on foreign ownership of media, including online media platforms;

[27] https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf

restrictions on disseminating foreign owned content; requirements for identity records be kept on users posting online comments; and criminal liability for online platforms for content posted on their sites.

Brazil

Copyright-Related Barriers And Non-IP Intermediary Liability Restrictions

Historically, the 'Marco Civil' law[28] has offered legal certainty for domestic and foreign online services and has created conditions for the growth of the digital economy in Brazil.[29] Recently, there have been attempts to revisit or change key provisions of this legal framework, including by compelling online companies to assume liability for all user communications and publications.[30]

Other Brazilian proposals would require online services to censor criticism of politicians and others, via a 48-hour notice-and-takedown regime for user speech that is "harmful to personal honor." This is a vague and overbroad standard that would present a significant market access barrier for U.S. companies seeking access to the Brazilian market.

There is also a bill on the Brazilian Senate[31] that includes a provision that requires digital platforms to "pay news publishers for use of their content (other than hyperlinks)," distorting fair play and placing unfair burden on digital platforms.

Customs Barriers To Growth In E-Commerce

Brazil's de minimis threshold (Decree No. 1804 of 1980 and Ministry of Finance Ordinance No. 156 of 1999) — for which no duty or tax is charged on imported items – only applies to customer-to-customer transactions under $50 and sent through post. The current level is not commercially significant and serves as a barrier to e-commerce, increasing the time and cost of the customs clearance process for businesses of all sizes. At its current level, Brazil's de minimis threshold increases transactional costs for Brazilian businesses and restricts consumer choice in the market. IA encourages the removal of this barrier to trade by extending the de minimis threshold to both business-to-customer and business-to-business transactions, both to post and express delivery shipments, and increasing the de minimis threshold to a commercially meaningful level. Current Brazilian legislation allows an increase of the threshold up to $100 without need for Congressional approval. As a reference, OECD members have an average de minimis threshold of $70 for taxes and $194 for duties.

The Ex-Tariff regime consists of the temporary reduction of the tax rate for the import of capital goods (BK), information technology and telecommunications (BIT), as shown in the Common External Tariff of Mercosur (TEC), when there is no national production equivalent. The Ex-tariff regime promotes the attraction of investments in the country, since it exempts investments directed to productive

[28] Brazilian Civil Rights Framework for the Internet, Law No. 12.965 (2014).

[29] Angelica Mari, *Brazil Passes Groundbreaking Internet Governance Bill*, ZDNET, http://www.zdnet.com/brazil-passes-groundbreaking-internet-governance-bill-7000027740/.

[30] Andrew McLaughlin, *Brazil's Internet is Under Legislative Attack*, MEDIUM https://medium.com/@mcandrew/brazil-s-internet-is-under-legislative-attack-1416d94db3cb#.dy4aak1yk.https://medium.com/@mcandrew/brazil-s-internet-is-under-legislative-attack-1416d94db3cb#.dy4aak1yk.

[31] PL 4255/2020 at https://www25.senado.leg.br/web/atividade/materias/-/materia/144233

enterprises. In order for this regime to attract even more investments, we suggest changing the current regulation so that the Ex-tariff benefit is also granted for items considered for "consumption," which means the import of goods directly to be consumed in Brazil and not for manufactures.

Data Flow Restrictions And Service Blockages

Brazil maintains a variety of localization barriers to trade in response to the weak competitiveness of its domestic tech industry. It provides tax incentives for locally sourced information and communication technology (ICT) goods and equipment (Basic Production Process (PPB) – Law 8387/91, Law 8248/91, and Ordinance 87/2013); it offers government procurement preferences for local ICT hardware and software (2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903); and it does not recognize the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks (ANATEL's Resolution 323).

GSI (Institutional Security Office) revised its cloud guidelines and issued an executive order mandating local data storage for public data stored in the cloud. This could both disadvantage firms that wish to provide services to the Brazilian public sector but that do not have the capacity to store data in Brazil, andcreate a de facto data localization requirement for cloud services in Brazil, spreading outside of just public cloud. While this is only applicable to government data and these are just guidelines, this precedent raises serious concerns.

In addition, recently a member of Congress introduced Bill 4723/2020, which amends Brazil's Data Protection Law (Law No. 13.709 of August 2018) and aims to impose data localization requirements by requiring that all personal data would have to be stored within the national territory. This bill also aims to forbid the use of cloud computing for any data processing when data is stored outside the national territory.

Divergence From Privacy Best Practices

On August 15, 2018, Brazil's President Michel Temer signed the General Data Protection Law Lei Geral de Protecao de Dados (LGPD), inspired by the EU's GDPR. Businesses have until August of 2020 to come into compliance with the LGPD.

Certain provisions within the data protection law risk harming both Brazil's own growing digital economy and market access by foreign services, including a new type of "adequacy" regime for assessing whether companies in other countries can move data in and out of Brazil.[32]

In addition, there are several bills before the Brazilian Congress that would implement a form of the "right to be forgotten" in Brazil, requiring that online services remove information that is deemed "irrelevant" or "outdated," even if it is true.[33] These developments conflict with Brazil's strong commitment to freedom of expression and access to information, and would present market access barriers for both small and large U.S. services seeking to enter the Brazilian market.

[32] *Localization Barriers to Trade: Why Demanding Too High a Price for Market Access Threatens Global Innovation*, Global Trade Magazine (Oct. 6, 2016), http://www.globaltrademag.com/global-trade-daily/localization-barriers-trade.

[33] Matt Sandy, *Brazilian Lawmakers Threaten to Crack Down on Internet Freedom*, Time (Jan. 20, 2016), http://time.com/4185229/brazil-new-internet-restrictions/.

For privacy regulations to be relevant and effective in today's environment, the U.S. and Brazil should advocate for interoperability of privacy regimes and frameworks that ensure accountable cross-border flows of information, while both protecting consumers and allowing for the benefits of e-commerce. For example, the U.S. should encourage Brazil to consider the APEC Cross Border Privacy Rules model as a best practice.[34]

Filtering, Censorship, And Service-Blocking

Brazil has blocked WhatsApp multiple times as part of legal disputes related to specific users, cutting off access to a U.S.-based messaging service for more than one-hundred million Brazilians in the process.[35]

Infrastructure-Based Regulation Of Online Services

Brazil is currently debating revisions to the legal basis for its telecom sector, and some legislators have supported the idea of regulating online services in a similar way to telecom services.[36] However, this approach risks raising costs for online entrepreneurs and halting Brazil's innovation due to increased bureaucracy and artificial limits on services, harming both local consumers and foreign providers of internet services.

Generally, product safety testing must be performed at in-country labs, unless the necessary capability does not exist in Brazil. Industry finds in-country testing problematic, both logistically and from a cost perspective. If testing has already been completed at a laboratory accredited to internationally accepted standards, the requirement to undertake similar testing at an additional in-country (local) lab duplicates the testing itself and increases the number of samples required and testing costs, all the while delaying the placement of products on the Brazilian market. INMETRO is a signatory to the Mutual Recognition Arrangement (MRA) of the International Laboratory Accreditation Cooperation (ILAC), which can facilitate acceptance of test results from participating labs in signatory countries. We encourage INMETRO to utilize this MRA to consistently accept international test reports and we also encourage the Brazilian government to implement the Inter-American Telecommunication Commission (CITEL) mutual recognition agreement with respect to the United States. Doing so would allow for recognition of testing done in the U.S., easing the time and cost of exporting to the Brazilian market. ANATEL's Resolution 323 of 2002 is particularly onerous in that it requires producers of telecommunications equipment to test virtually all of their products in the country before they can be placed on the market, increasing price and delaying the time it takes for the products to be available to Brazilian consumers. By allowing

[34] *Cross Border Privacy Rules System*, CBPRS, http://www.cbprs.org/ (last visited Oct. 25, 2016).

[35] *See WhatsApp Officially Un-Banned In Brazil After Third Block in Eight Months*, The Guardian (July 19, 2016), https://www.theguardian.com/world/2016/jul/19/whatsapp-ban-brazil-facebook;https://www.theguardian.com/world/2016/jul/19/whatsapp-ban-brazil-facebook Glen Greenwald & Andrew Fishman, *WhatsApp, Used By 100 Million Brazilians, Was Shut Down Nationwide by a Single Judge* , The Intercept (May 2, 2016), https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/.https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/.

[36] *Taxation on OTT in Brazil*, Tech in Brazil (June 10, 2015), http://techinbrazil.com/taxation-on-ott-in-brazil; Juan Fernandez Gonzalez, *Brazil's Creators Demand VOD Regulation,* Rapid TV News (July 5, 2016), http://www.rapidtvnews.com/2016070543482/brazil-s-creators-demand-vod-regulation.html#axzz4O8DTZE5y.

international mutual recognition agreements, Brazil can avoid having multiple, duplicative testing requirements that delay products to market and increase costs for Brazilian consumers.

Good Regulatory Practices

Brazil took a significant step towards good regulatory practices when the Brazilian Foreign Trade Council (CAMEX)'s published Resolution 90 in 2018, thereby establishing good practices for the preparation and review of regulatory measures affecting foreign trade. The resolution encourages Brazilian regulatory bodies to develop regulatory agendas, conduct regulatory impact analysis, evaluate regulatory alternatives, use international standards, conduct transparent public consultations of a minimum of 60 days for all regulations with international trade effects, ensure all regulations comply with Brazil's international trade commitments, notify regulations to the WTO via the inquiry point, use evidence-based decision making, coordinate with other relevant regulators to ensure coherence and compatibility with other regulations, and review and manage regulatory stock. Despite this development, however, recent consultations notified by ANATEL through the WTO TBT inquiry point included very short timeframes for response. We appreciate ANATEL extending the deadlines for comments on a case-by-case basis, but we encourage all agencies in Brazil to notify consultations with a minimum 60-day comment period. Agencies are also encouraged to consider the regulatory impact imposed by requirements and whether the benefits are commensurate with the impacts. For example, the recent operational procedures published for Resolution No. 715 contain a number of submission procedures and additional bureaucratic steps that increase burden to industry without providing additional assurance of conformity. We encourage ANATEL to consider the impacts of regulations in comparison to the benefits provided and to provide an explanation of these benefits in any proposed regulation.

In addition, we encourage Brazil to take an approach rooted in good regulatory practices that considers the legitimate objective of the public policy and the specific characteristics of the value added services, such as video on demand streaming or other OTTs, in order to avoid any potentially overly burdensome rules that would limit access to these services. It is critical that Brazil prohibits permanent customs duties for digital products and electronic transmissions to ensure that added cost does not impede the flow of music, video, software, games or information. Also, we encourage Brazil to join the ITA and its expansion, enabling Brazil to tap into global ICT supply chains and position itself as a leader in the region on forward-looking tech policy. By reducing their costs, the ITA leads to increased use of ICT goods, which spurs productivity and economic growth in signatory nations.

National AI Strategy

Brazil is currently reviewing and restructuring its national AI strategy at the federal level, and several bills of law governing AI have been introduced in the Congress. There is concern that some policymakers have taken positions on these initiatives that could isolate Brazil with unique standards, onerous certification or localization requirements, or heavy-handed regulations. We advocate the adoption of a flexible and diversified regulatory approach that encourages strong public-private collaboration and responsible development of AI. Further, to promote innovation, we also encourage the facilitation of data sharing, advancement of structured and standardized AI R&D, and support for STEM-informed workforce development.

Restrictions On Cloud Service Providers

Presidential Decree 8135 of November 5, 2013 and subsequent Ordinances (No. 141 of May 2, 2014, and No. 54 of May 6, 2014) required that federal agencies procure email, file sharing, teleconferencing, and VoIP services from Brazilian "federal public entities" such as SERPRO, Brazil's Federal Data Processing Agency. Such measures disrupt the global nature of the ICT industry and disadvantage both access to technology in Brazil and the ability of U.S. ICT companies to do business in Brazil. The Brazilian Government (through the Ministry of Planning and the Ministry of Communications, Science and Technology) announced in August 2016, that Decree 8135 would be revoked. However, actual revocation of such legal imposition has not yet taken place, creating substantial uncertainty. The U.S. government should urge Brazil to immediately revoke this Decree and its Ordinances and ensure that any new measures avoid provisions that would hinder Brazilians' access to best-in-class, cloud-based communication services.

Unilateral Or Discriminatory Digital Tax Measures

There are four bills in the Brazilian Congress that seek to implement or raise taxes on digital services. At this moment, the most relevant bill creates the Social Contribution on Digital Services (CSSD), with a rate of 3 percent on the gross revenue from digital services, and 10 percent on the revenue from online betting. The bill targets companies domiciled in Brazil or abroad, that have earned in Brazil a gross revenue greater than BRL 100 million ($17 million). The bill has support from traditional members of Congress, from both opposition and government support base. On the other hand, neither the speakers of the House and the Senate nor the Ministry of Economy endorsed any of the proposals. Brazil's proposals share characteristics with the French Digital Services Tax enacted in July 2019, many of which contravene long-standing international taxation principles and present significant burdens for companies in the tech sector as well as the companies that rely on these services. The Brazilian Government should refrain from introducing any tax measure that is discriminatory in nature and to recommit to reaching a multilateral solution to the tax challenges arising from the digitalization of the global economy. Additionally, any tax changes to reflect the digitalization of the economy should be pursued at a global level through the OECD, not unilaterally.

Canada

Discriminatory Or Opaque Application Of Competition Regulations

The ongoing expert panel legislative review of Canada's Broadcasting Act and Telecommunications Act (also known as the Yale Panel) is expected to recommend that foreign digital video services, such as Amazon Prime and YouTube, be regulated under the CRTC's Canadian Content rules (CanCon) in order to offer service to Canadians. Potential regulations could include (1) Canadian content quotas; (2) requirements to give prominence to Canadian content in online menus and/or algorithms; (3) mandatory spending on CanCon or contributions to the Canadian Media Fund. Mandating these requirements for foreign digital services would impose an unfair burden on these foreign companies, as they do not benefit from the many market protections given to domestic providers (ex. simultaneous substitution, must-carry regulations). To be clear, U.S. industry does not desire the market protections given to domestic operators; the industry instead prefers to offer a customer-driven (rather than

regulatory-driven) service. Further, these requirements would primarily impact large U.S. digital media services, as the Canadian government would not realistically be able to attain regulatory compliance from streaming services located in countries such as China.

Divergence From Privacy Best Practices

In 2019 the Office of the Privacy Commissioner (OPC) proposed revising its policy position on transborder data flows under the Personal Information Protection and Electronic Documents Act (PIPEDA), to assert that a company that is disclosing personal information across a border, including for processing, must obtain consent. Although the OPC ultimately withdrew its proposal, it did so with the caveat that it would maintain the status quo only "until the law is changed." It reiterated this observation in its most recent annual report.[37] The OPC, and other like-minded regulators and third party groups, continue to advocate within Ottawa for a protectionist approach to privacy legislation that would hinder the cross-border movement of data, and the industry expects to encounter a similar proposal again in the near future. The Government of Quebec has introduced new privacy legislation that, among other things, would make data transfers extraordinarily difficult. A Canadian legal requirement to obtain consent for the processing of data outside of Canada would impede the flow of data across borders and cause great harm to U.S. businesses. Such a rule would serve as a de facto data localization requirement, as obtaining consent from all Canadian customers, employees, or contractors, or customers would often not be possible. Placing such a restriction on cross-border transfers of data runs counter to Canada's commitments under the USMCA, which prohibits parties from restricting the flow of personal information between one another (Art. 19.11).

The Privacy Commissioner has published guidance that argues existing legislation allows for a "right to be forgotten" in Canada[38] and Quebec has introduced legislation that creates a similar "right to delist."

Non-IP Intermediary Liability Restrictions

The Liberal platform and government mandate letters call for new rules regulating online content and expands the role of internet companies in addressing content posted online.[39] The plan includes significant penalties for social-media companies that fail to address online harms within 24 hours. There will also be legislation introduced to address civil remedies for victims of online hate. The plan runs counter to USMCA Article 19.17, and IA urges USTR to engage with Canadian officials on this issue.

Unilateral Or Discriminatory Digital Tax Measures

Late in 2019, Canadian Prime Minister Justin Trudeau has proposed a digital services tax similar to the French DST.[40] According to a cost analysis conducted by Canada's Office of the Parliamentary Budget Officer, the tax would "replicate" the French measures and impose a 3 percent digital services tax to advertising services and digital intermediation services with global revenue over C$1 billion ($755 million) and Canadian revenue over C$40 million.[41] There have been renewed calls for this tax in the wake of the COVID pandemic and the relatively slow progress on OECD proposals. IA urges USTR to

[37] https://www.canada.ca/en/privy-council/campaigns/speech-throne/2020/stronger-resilient-canada.html
[38] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/
[39] https://2019.liberal.ca/wp-content/uploads/sites/292/2019/09/Forward-A-real-plan-for-the-middle-class.pdf
[40] https://2019.liberal.ca/wp-content/uploads/sites/292/2019/09/Forward-A-real-plan-for-the-middle-class.pdf
[41] https://www.pbo-dpb.gc.ca/web/default/files/Documents/ElectionProposalCosting/Results/32977970_EN.pdf?timestamp=1569835806287

seek to prevent Canada from implementing this unilateral tax measure concerning digital products and services.

Chile

Copyright-Related Barriers

Chile does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Chilean Intellectual Property Law includes a long but inflexible list of rules[42] that does not clearly provide for open limitations and exceptions that are necessary for the digital environment – for example, flexible limitations and exceptions that would enable text and data mining, machine learning, and indexing of content. This handful of limitations leaves foreign services and innovators in a legally precarious position. In order to reduce market access barriers to U.S. services, IA urges USTR to work with Chile to implement a multi-factor balancing test analogous to fair use frameworks in the U.S and Singapore, to enable copyright-protected works to continue to be used for socially useful purposes that do not unreasonably interfere with the legitimate interests of copyright owners.

Divergence From Privacy Best Practices

Under Chile's Comisión para los Mercados Financieros, its compilation of updated rules (Recopilacion Actualizada de Normas Bancos or "RAN") Chapter 20-7 requires that "significant" or "strategic" outsourcing data be held in Chile. The same requirement is outlined in Circular No. 2, which is addressed to non-banking payment card issuers and operators. In effect, these regulations can apply to any confidential records. In the case of the international transfer of such data, transfer may occur but duplicate copies of such records must be held in Chile.

Chile has joined several other governments in Latin America in responding to data privacy concerns by advancing a heavy handed data privacy bill that seeks to align their privacy regulations with GDPR, without fully comprehending the impact on the local economy or how the systems are effectively implemented and enforced. This bill raises a number of challenges for U.S. companies, including the introduction of the right to be forgotten, which would make it more difficult for all U.S. companies operating in Chile that need to transfer data across borders.

China

Copyright-Related Barriers

Online piracy remains rampant in China, for example with respect to e-books and software. At the same time, China has not expedited amendments to its Copyright Law, which have been under review since 2011. The latest draft proposes increased penalties that would provide a greater deterrent to copyright violators. For example, under the current law, there is no criminal provision for digitalization of written works and circumvention of digital technological protection measures, and pirates can only be pursued for criminal liability with the purpose of making profits. The cost of selling pirated ebooks or software remains unreasonably low in China as online shops are immune from criminal charges if they sell pirated

[42] Law No. 17.336 on Intellectual Property (as amended 2014), Art. 71.

copies valued under a significant threshold $7,365) or the online works being transmitted have been accessed less than 50,000 times. As industry has repeatedly communicated to authorities, piracy would be improved if China's Criminal Law introduced new crimes of online piracy, lowered the criminal threshold, increased criminal liability for piracy, implemented stronger civil remedies, and expressly criminalized the commercial use of pirated content.

Data Flow Restrictions And Service Blockages

China imposes numerous requirements on internet services to host, process, and manage data (personal information and other important data gathered or produced within China) to be stored locally within China, and places significant restrictions on data flows entering and leaving the country.[43] China continues to moderate the public's access to websites and content online. On June 4, 2019, access to CNN was blocked[44] after the media company published a story on Tiananmen Square prior to the anniversary of the event.

Member companies including Twitter, Facebook, and Google continue to be blocked in mainland China.

China's restrictive requirements on data localization and cross-border information flows will significantly impact foreign companies' ability to operate in the online space, create extra burdens, and hurt related business prospects. The data localization requirement would extend the scope of Critical Information Infrastructure (CII) to all internet business players, and mandates all original users' information be retained within China only, with no copies being transmitted beyond the country, unless an authority's approval is obtained. A new draft Measures for Security Assessment of Personal Information Cross-border Transfer released for comments in 2019 imposes cross-border data transfer restrictions on ordinary network operators and requires companies to obtain customer consent for cross-border transfers of their sensitive personal information. Expanding the scope of CII requirements will make ordinary data transfers much more complicated and inflict unnecessary burdens on foreign companies. In addition, an increased burden on MNCs was reflected in the first draft of the Data Security Law (DSL) released for comments in 2020. The law states that entities face legal liability outside of China if they "engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations" in China. The draft law also states China will establish a data security review mechanism, and data processors shall obtain licenses, cooperate with national security agencies, and go through data review processes for various data related activities in China. China has also released more measures regarding data security, lacking necessary clarifications on key terms and procedures (e.g. clarification on important data and criteria for triggering a data security review), bringing more ambiguity and uncertainty, and increasing the already complex and uncertain compliance burdens on MNCs.

Discriminatory Or Opaque 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

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

[44] https://techcrunch.com/2019/06/04/china-blocks-cnns-website-and-reuters-stories-about-tiananmen-square/

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.

IA urges 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 licenses by restricting the ability to acquire existing licensed entities, 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.[45] 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.

Infrastructure-Based 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

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

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.

Restrictions On U.S. Cloud Service Providers

U.S. cloud service 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 surrender use of their brand 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 fully implement these restrictions, effectively barring U.S. CSPs from operating or competing fairly in China.

China's Ministry of Industry and Information Technology (MIIT) 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.

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.

Colombia

Artificial intelligence (AI) Strategy

Colombia is currently constructing a national AI strategy at the federal level and there is concern that some policymakers have taken positions on these initiatives that could isolate Colombia with unique standards, onerous certification or localization requirements, or heavy-handed regulations. We advocate the adoption of a flexible and diversified regulatory approach that encourages strong public-private collaboration and responsible development of AI. Further, to promote innovation, we also encourage the facilitation of data sharing, advancement of structured and standardized AI R&D, and support for STEM-informed workforce development.

Copyright-Related Barriers

To date, Colombia has failed to comply with its obligations under the U.S.-Colombia Free Trade Agreement to provide copyright safe harbors for internet service providers. A bill to implement the U.S.-Colombia FTA copyright chapter is pending.[46] Without a full safe harbor, intermediaries remain liable for civil liability. Action should be taken by the government to provide a full safe harbor as required by the FTA.

Customs Barriers To Growth In E-Commerce

Colombia has not implemented the $200 de minimis threshold on duties or taxes commitment provided for in the U.S. Colombia Trade Promotion Agreement (CTPA). On July 2, 2019, the Colombian government published Decree 1165 of 2019, which established Colombia's New Customs Regime. The new regime combined all relevant decrees and regulations issued over the last few years and by doing so, scrapped Decree 349, and removed any specific timeline to implement the de minimis provision of the CTPA. In addition, Colombia has also significantly delayed implementation of customs reforms that would allow traders to submit electronic copies of invoices instead of physical copies.

Non-IP Intermediary Liability Restrictions

This fall, legislation is moving in Colombia targeting U.S. digital platforms. The draft bill "Por el cual se modifica la Ley General de Turismo y se dictan otras disposiciones" was drafted by the Vice Minister of Tourism Julian Guerrero at the urging of traditional hotel associations. The bill proposes regulations against digital platforms' responsibilities. It would hold digital platforms legally liable for any user's violation of terms of service (Article 21), which will be impossible to implement. The bill would require digital platforms to register with the National Tourism Registry (Article 20), which would make U.S. companies subject to local law and further sanctions beyond the user's violation of terms of service. It would also require digital platforms to create a permit field and obligate Colombian hosts to submit a permit number from the National Tourism Registry (Article 20), which would burden those who share their space for income, and require home sharing platforms achieve the impossible task of confirming all

[46] USTR, Intellectual Property Rights In in the US-Colombia Trade Promotion Agreement, US-U.S.-Colombia Trade Agreement, https://ustr.gov/uscolombiatpa/ipr visited Oct. 25, 2016).

listings are registered. Any company incorporated in the U.S. or abroad that participates as an intermediary in the travels and tourism sector is subject to the Bill, including online travel agencies, metasearch companies, short-term rental platforms and Global Distribution Systems. The Bill also poorly defines an electronic or digital platform broad enough to account for a wide swath of IA member companies.

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 restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of for-hire vehicles.

- → *License cap:* In February 2015, the Ministry of Transport froze the granting of any new for-hire vehicle licenses. No technical study or research of any sort was conducted to provide an underlying rationale for this licensing freeze and the ministry made no public statement justifying the step.

Ecuador

Divergence From Privacy Best Practices

In January 2019, the National Directorate for the Registration of Public Data (DINARDAP), an Ecuadorian public entity attached to the Ministry of Telecommunications, presented the first law of personal data protection of Ecuador to the public. The bill is still being deliberated in Congress. Key topics for the bill include GDPR-like strict requirements on express consent and a right to be forgotten provision, which add unnecessary friction to cross-border digital trade and information flows.

Egypt

Filtering, Censorship, And Service-Blocking

Egypt President Abdel Fattah al-Sisi ratified a cybercrime law which obliges ISPs to block websites, whether hosted in Egypt or internationally, which are deemed to have committed a cybercrime that threatens national security , under threat of fines and/or imprisonment. Critics state that the law increases censorship and silences political opposition. In March 2019, Egypt's top media regulator the Supreme Media Regulatory Council (SMRC), with support from President Abdel-Fattah al-Sissi, put into effect tighter restrictions for online content that allow the government to block websites and social media accounts with over 5,000 followers if they are deemed a threat to national security.[47] State censorship continues, and in April 2019, internet service providers in Egypt blocked 34,000 internet domains to prevent the public from accessing the "Void" campaign opposing amendments to the Egyptian constitution, including U.S. and international NGO websites. Member companies including Facebook, Twitter, and Google continue to operate in Egypt.[48]

[47]https://www.haaretz.com/middle-east-news/egypt/egypt-can-now-block-websites-social-media-accounts-deemed-a-threat-1.7041232
[48]https://madamasr.com/en/2019/04/16/news/u/egypt-blocks-over-34000-websites-in-attempt-to-shut-down-constitutional-a

In May 2020, the SMRC issued Decree no. 26 of 2020 that enforces a strict licensing regime on Media and Press outlets, as well as both national and international online platforms. The regulation requires a 24-hour window for the removal of harmful content. It also obligates international companies to open a representative office in Egypt, while naming a liable legal and content removal point of contact. The regulation lacks safe harbor protections for international companies, and stipulates an average of $200,000 in licensing fees. The fees are argued to exceed the ceiling of that stipulated in the Media law of 2018, and are hence unconstitutional.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps 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.

- → *Data sharing requirements:* Implementing regulations issued in September 2019 require ride-hailing apps to share data with government authorities without the procedural safeguards set out in the original ride-hailing law. Ride-hailing apps are also able to obtain an operating license only once they have received the approval of the Egyptian national security agencies.

Unilateral Or Discriminatory Digital Tax Measures

In their bid to raise fiscal revenues, the Egyptian Government proposed Amendments to the Value Added Tax Law No. 67 for 2016, to include taxation of ad revenue, including digital advertising through a proposed stamp tax in addition to the VAT. While the stamp tax was dropped, companies are still liable to the currently proposed 14 percent VAT. Online platforms suffer from the lack of distinction between digital and non-digital services for VAT liability, while international companies face the obscurity of how the VAT will be applied to their services. Other issues of concern include designating an accounts point of contact and e-billing. Online transactions are automatically registered at the authority and VAT value is determined.

European Union (EU)

Since the European elections in 2019, EU leaders have actively promoted a multi-pronged approach towards "technological sovereignty" or "digital sovereignty" as a main policy objective.[49] In updates to the EU's digital and industrial agenda calls for "technology sovereignty" have been advanced with regards to data, artificial intelligence, cloud services, as well as on the responsibility of online platforms and competition policy with the latter two packaged as the Digital Services Act and Digital Markets Act.

While the precise meaning of sovereignty or autonomy in the realm of technologies remains ambiguous, EU leaders have emphasized the desire to limit the market position of U.S. providers. For example, some

mendments-opposition-campaign/

[49]https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_mission_letters/president-elect_von_der_leyens_mission_letter_to_thierry_breton.pdf

EU officials have called for a range of policies to support "a European way of digitization, to reduce our dependence on foreign hardware, software and services."[50]

A recent draft document from the European Commission –A European Strategy for Data – calls the amount of data held by "Big Tech firms" a "major weakness" for Europe, and proposes several regulations to require sharing of data between public and private firms to create a "European data space." This document also proposes subsidizing European cloud providers while contemplating potential ex ante competition rules that would be applied against foreign firms.

It is important for the U.S. to engage with the EU on this issue to ensure that any proposals on sovereignty and European data do not include tools that would result in protectionism and discrimination against U.S. firms.

In particular, it is important to ensure that "digital sovereignty" proposals do not morph into de facto forced data localization requirements, restrictions on cross-border data transfers, or other market barriers for U.S. firms. The EU should be a critical ally of the U.S. in pushing back on foreign data localization requirements and championing open digital trade, not instituting new domestic barriers to information flows. Localization measures 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 disasters, intrusion, and surveillance. All U.S. industries would be negatively impacted by data localization or sovereignty requirements, including firms that rely on cross-border data transfers in the agriculture, manufacturing, financial services, and health sectors.

In a recent whitepaper on AI, the European Commission has signaled that it is pursuing a restrictive path on AI regulation that clearly seems designed to target U.S. competitors. In the paper the Commission has proposed an elaborate ex ante conformity assessment system to audit AI applications originating from the U.S. and other non-EU locations. This system would empower European regulators, and potentially even European industrial competitors (if they are tasked to conduct the conformity assessment), to impose audits and delays on U.S. AI applications before they can be introduced to the EU market. This could create barriers to entry for non-EU AI services and slow down their time-to-market. The EU should be encouraged to focus on reciprocity between U.S. and EU certification/testing methodology and avoid ex-ante conformity assessments in the EU for non-EU AI products.

Copyright-Related Barriers And Other Issues

The European Union's (EU) passage and adoption of the Copyright Directive in 2019 serves as a market access barrier for U.S. technology companies doing business in Europe, and underscores the industry's position that the strong and balanced U.S. copyright system has continued vitality in promoting the strongest content and technology sectors in the world. The principles behind Articles 15 and 17[51] are at odds with fundamental principles of U.S. law and longstanding U.S. intellectual property policy and practice and should be resisted through U.S. foreign and trade policy. Regrettably, these aspects of the Directive appear to be part of a larger pattern of unfair actions by the EU against the innovative U.S. internet technology sector.

[50] Axel Voss, A manifesto for Europe's digital sovereignty and geo-political competitiveness, https://www.politico.eu/wp-content/uploads/2020/01/Axel-Voss-Digital-Manifesto-2.pdf
[51] Article 15 was previously known as Article 11 and Article 17 was previously known as Article 13.

The changes to copyright made by the Copyright Directive, specifically those requiring proactive filtering and licensing for snippets, impose significant unwarranted liability on internet companies, and will have a disproportionately large impact on the ability of small companies to compete. The directive also risks limiting access to European content for American consumers, as platforms unable to negotiate licenses may be forced to block European-based publisher content from their sites.

The EU Directive effectively requires internet services of all sizes to implement comprehensive content filtering systems, without regard for the inevitable consequences of such filtering, including the removal of protected speech; content protected by the "fair use" doctrine; and misidentified, legally distributed works from all types of online platforms. This is completely at odds with U.S. policy as found in the USMCA. The USMCA maintains the U.S. law-endorsed balance among stakeholders by allowing (1) the public to legally enjoy copyrighted content, (2) rights holders to identify allegedly infringing material online, and (3) internet platforms to expeditiously remove access to such material without incurring legal risk for the actions of third parties about which they have no knowledge. The new EU policy destroys that careful balance.

U.S. copyright law provides strong rights for publishers, but has always protected permitted using brief snippets of copyrighted material for legitimate, referential purposes, and Article 10(1) of the Berne Convention further protects the right to provide "quotations from a work lawfully made available to the public." Online platforms consistently promote these goals when they provide services that index websites, aggregate news headlines, and refer online users to third-party articles. This benefits consumers by providing access to information, allows users to share and connect, and promotes the ability for publishers to reach new audiences. Yet the new EU policy includes vague measures that would create a "quasi-copyright" publisher right whose primary goal is to require U.S. services to remunerate European authors or obtain authorization for the use of such content otherwise permitted by copyright law.

The internet industry and the creative ecosystem both flourish under the balance of the U.S.'s innovation-oriented copyright regime.[52] The EU's efforts to hamstring U.S. companies by abandoning that balance risks thwarting the continued growth of the commercial internet. IA respectfully requests that USTR remain steadfast in efforts to include the elements of the U.S.'s innovation-oriented copyright system in trade agreement negotiations and find opportunities to highlight the problems with this directive when engaging with EU counterparts. In addition, IA encourages USTR to engage with any other countries that are considering copyright proposals modeled on the EU's copyright directive. The EU passed changes to its copyright framework which will make it harder for U.S. businesses to effectively compete in Europe and will burden U.S. companies with compliance obligations if they decline to pay European companies or organizations for activities that are entirely lawful and legal under the U.S. copyright framework. The copyright proposal diminishes needed checks and balances, tilting rights in favor of just rights holders, in an approach that will significantly harm American exporters and innovators.

Particular problems with the Directive include new "neighboring rights" for news publishers that conflict with the Berne Convention (Article 15), broad and unclear monitoring and filtering obligations for service providers (Article 17), as well as potentially intrusive multi-stakeholder processes regarding the design and operation of content recognition technologies (Article 17). These barriers are discussed in more

[52] https://www.techdirt.com/skyisrising/

detail below, along with other concerns about restrictions on text and data mining and liability for hyperlinks.

The industry encourages USTR to reiterate the U.S. government's opposition to these and other measures as currently drafted and to seek obligations through the upcoming U.S./EU bilateral trade negotiations to prohibit such measures. Departures by the EU from the proven, successful policies that both sides of the Atlantic have followed to date risk thwarting the continued growth of innovative and creative industries alike.

Ancillary Copyright And Neighboring Rights

"Ancillary copyright" or "neighboring rights" laws refer to legal entitlements for "must carry must pay" obligations that enable countries to impose levies or other restrictions on the use of this information. Such levies negatively impact the ability of U.S. services to use or link to third-party content, including snippets from publicly available news publications.

The subject matter covered by ancillary copyright is ineligible for copyright protection under international law and norms. Article 10(1) of the Berne Convention provides that "[i]t shall be permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries."[53] It is further provided as an example that "quotations from newspaper articles and periodicals in the form of press summaries" are fair practice. As incorporated into TRIPS Article 9, Article 10(1) of the Berne Convention creates an obligation on Member States to allow for lawful quotations.[54]

However, ancillary copyright laws impose a levy on quotations in direct violation of these obligations under TRIPS and create new rights contradictory to international standards meant to protect market access. For example, these laws would require online services that aggregate news content to pay a tax to the news publisher for the ability to link to one of its articles. Rather than attempting to navigate complex individual negotiations with publishers in order to include a headline or other small amount of newsworthy content on a third-party site, online services might simply stop showing such content, causing traffic to news publishers to plunge. These laws create a stealth tax on U.S. internet services operating in foreign jurisdictions, and unfairly disadvantage internet services from offering services otherwise protected under copyright law by raising barriers to market entry.

Previous implementations of this principle in EU Member States such as Germany and Spain have generated direct and immediate market access barriers for U.S. services.[55] The EU's directive , like those earlier provisions, runs afoul of international obligations in the Berne

[53] Berne Convention for the Protection of Literary and Artistic Works, art. 10(1), last revised July 24, 1971, amended Oct. 2, 1979, S. Treaty Doc. No. 99-27, 828 U.N.T.S. 221 (hereinafter "Berne Convention").

[54] The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, art. 9.

[55] *EU Lawmakers Are Still Considering This Failed Copyright Idea*, Fortune (March 24, 2016), http://fortune.com/2016/03/24/eu-ancillary-copyright/http://fortune.com/2016/03/24/eu-ancillary-copyright/ (describing failed attempts in Germany and Spain, which included causing Google to shutdown its Google News service in Spain and partially withdraw its news service in Germany, and news publishers' revenue to tank in both countries).

Convention by giving some publishers the right to block internet services from making quotations from a work.[56]

The threat posed by ancillary copyright laws to U.S. stakeholders is genuine and timely, especially as Europe considers more widespread proposals that would violate international copyright obligations to the detriment of U.S. copyright stakeholders, and hinder the growth of new business models. The discriminatory harm done by these stealth taxes on search engines and news aggregators creates economic and legal barriers to entry that effectively deny market access and fair competition to U.S. stakeholders whose business models include aggregation of quotations protected by international copyright standards. Expressing such concerns after legislation is enacted or is inevitable is too late.

Liability For Hyperlinks

IA has concerns about the Court of Justice of the CJEU's decision in GS Media v. Sanoma Media, which held that linking to copyrighted content posted to a website without authorization can itself be an act of copyright infringement.[57] This case is generating additional lawsuits testing the extent of the ruling, which may create new liability for online services doing business in the EU. It has also resulted in new monetary demands from publishers to those who provide links to content. IA urges USTR to monitor this situation and engage with European counterparts to prevent other negative impacts from this ruling.

Restrictions On Text And Data Mining

The European Commission proposals for text and data mining further restrict technology startups and businesses of all types from engaging in cutting-edge research and data analytics. By limiting who can legally engage in machine learning, these restrictive proposals will have a significant impact on the emerging market and the jobs associated with data analytics, technology, and artificial intelligence.

Weakening Of E-Commerce Directive Protections For Internet Services In EU Member States

Despite existing protections under the E-Commerce Directive for internet services that host third-party content, courts in some EU Member States have excluded certain internet services from the scope of intermediary liability protections. For example, one platform that hosted third-party content in Italy was found liable because it offered "additional services of visualisation and indexing" to users.[58] Another U.S.-based platform was found liable because it engaged in indexing or other organization of user content.[59] A third internet service was held liable for third-party content because it automatically organized that content in specific categories with a tool to find "related videos."[60] All of these activities represent increasingly

[56] Eur. Comm'n, Directive of the European Parliament and of the Council on Copyright in the Digital Single Market (Article 11), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0596&from=EN.

[57] C–*GS Media BV v Sanoma Media Netherlands BV* et al., ECLI:EU:C:2016:644, European Court of Justice (September 2016).

[58] RTI v. Kewego (2016).

[59] Delta TV v. YouTube (2014).

[60] RTI v. TMFT (2016).

common features within internet services, and the existence of these features should not be a reason to exclude a service from the scope of intermediary liability protections under the E-Commerce Directive, in Italy, or any other Member State.

Customs/Trade Facilitation

In December 2017, the Commission initiated a two-part legislative proposal (the Goods Package) aimed at improving product safety across the EU: (1) a draft regulation on compliance and enforcement (market surveillance); and (2) a draft regulation on mutual recognition for the EU Single Market. The Commission notified the package to the WTO in February 2018. The final Regulation (EU) 2019/1020 on market surveillance and product compliance entered into law on July 15, 2019 with the majority of its provisions applicable as of July 16, 2021.

The regulation includes a number of ambiguities that may prejudice legitimate traders seeking to access the EU market, while doing little to improve overall customer safety. Specifically, Article 4 includes a requirement for a dedicated "Responsible Person" who must be based in the EU and who will be responsible for maintaining compliance documentation and cooperating with market surveillance authorities to furnish that information, as necessary. Article 4 lacks clarity, however, regarding the responsibilities and liabilities for the Responsible Person, including fulfilment service providers, by taking a one-size-fits-all approach to liability regardless of objective and risk. Further guidance is needed to provide clear advice and mechanisms to businesses who want to comply and to ensure implementation of the Regulation is consistent with the EU's obligations under the WTO TBT Agreement.

Extended Producer Responsibility (EPR)

Companies are facing disproportionate administrative barriers originating from EU environmental legislation [e.g. the WEEE, Batteries and Packaging Directives, so called extended producer responsibility legislation (EPR)] when moving goods cross border in the EU. EU EPR legislation obligates the "producer" to register, report, and pay for certain products or materials the producer ships to an EU jurisdiction. The definition of "producer" is widely understood to be the seller of record. EU legislation is in the form of directives, and country implementation is not harmonized. As an example of the complexity, countries have adopted varying EPR fees for different types of products, and require registration with various so called "compliance schemes" (e.g. organizations in charge of the collection of recycling fees) at the national level, filing of complex reports in thousands of different categories which do not align between countries, when selling goods to the market. As a result, a seller shipping a single item into all EU countries would technically be required to register, report, and pay in nearly all 28 jurisdictions, under 28 different regimes. A third-party consultant estimated a cost of approximately €5,000 per country per seller in registration and administrative fees (not including the actual EPR fees due, which tend to be minimal). Online marketplaces are not allowed to remit fees on behalf of their sellers, unless they become a so called "authorized representative" which requires lengthy and costly contractual set up between marketplace and seller and still requires detailed product and material level reporting, hence not enabling the seller (often an SME) to benefit from the single market. Furthermore, under the current regime, sellers on online marketplaces are often faced with double payments issues where the vendor pays the relevant EPR fee in the country where it places the goods on the market originally, and the sellers are then asked to pay the relevant EPR fee in the country of destination, if the goods

are exported to another country. Some (not all) countries allow for the reimbursement of fees, however the documentary evidence is substantial and often discourages SMEs. The solution is the introduction of a simplified flat fee payment, based on average product information rather than actual detailed data, on the basis of which a marketplace will be allowed to remit recycling fees on behalf of its sellers.

Data Flow Restrictions And Service Blockages

IA is monitoring new developments in France and Germany, including efforts to establish local infrastructure for cloud data processing, and new local data retention requirements for internet services in Germany.

In addition, the EU and some Member States have been proposing various restrictions on cloud services. As of this submission, the EU was preparing a Joint Declaration on cloud services that would erect protectionist barriers to entry into the European market. According to the leaked draft, providers "must fulfil the need of cloud users to maintain control over strategic and sensitive data, including by ensuring that cloud capacities and services are not subject to the laws of foreign jurisdictions that could oblige access to be granted to EU data."[61]

The draft document would exclude non-EU cloud providers from participating in the European Cloud Federation. Those providers, which are naturally subject to applicable laws in the countries where they are headquartered, much like European providers are subject to European law when they operate abroad.

Divergence From Privacy Best Practices

The European high court on July 16, 2020 issued a major decision that severely limits mechanisms for data flows to the United States, and if not addressed, will seriously impede U.S.-EU digital trade and U.S. exports. In the Schrems II case, the European court invalidated the EU-U.S. Privacy Shield and cast doubt upon any data transfer to the United States. Moreover, there is ongoing interpretation of the high court ruling by European Member States that could equate to a full data localization regime for U.S. companies by applying what should be a global standard for EU data flows but targeted against the United States and U.S.-based companies.

If there isn't a meaningful political resolution, the decision could lead to all transatlantic data flow mechanisms being invalidated, which would upend transatlantic trade. It could leave many U.S. (and EU) companies without viable mechanisms to transfer data to the U.S., undermining trillions in transatlantic trade. Thousands of companies from all industries and of all sizes are affected – whether in the technology, financial services, healthcare, transportation, or other sectors. U.S.-EU data flows support $7.1 trillion in transatlantic trade and investment.

Moreover, as it stands, the EU is unfairly singling out the U.S. – stopping data flows to the U.S. only, while allowing data flows to many other countries in the world that clearly have less adequate protection for individual privacy than either the EU or the U.S., and fewer shared values. Such a result would be discriminatory and be an affront to transatlantic trade.

[61] https://www.politico.eu/wp-content/uploads/2020/09/Draft-cloud-declaration.pdf?

In addition, the EU General Data Protection Regulation[62] still contains considerable ambiguity. How EU data protection authorities choose to interpret the law will have a significant impact on companies' ability to operate in the EU and offer consistent services and products across the globe.

IA is also concerned about measures in the ePrivacy Bill that would prohibit processing of all electronic communications data and metadata, except in very limited circumstances where there is explicit consent from all parties.

On October 4, 2019, the Court of Justice of the European Union delivered an opinion arguing that pre-checked boxes to collect users' consent to collect cookies failed to meet the requirements of GDPR. The opinion comes as part of a German case Bundesverband v Planet49 GmbH. The decision will be disruptive to the basic technological function of webpages and other online media.

Infrastructure-Based Regulation Of Online Services

There are currently active consultations and proposals regarding the extension of certain telecom and broadcasting obligations to online voice and video services, including obligations concerning emergency services, limited accessibility requirements, data portability, interoperability, confidentiality of communications, and data security,[63] as well as local content quotas relating to the Audiovisual Media Services Directive (AVMS).[64]

The EU is in the process of transposing an update to the AVMS, which will update the regulatory framework for audiovisual services throughout the EU, covering traditional broadcast and On Demand Program Services (ODPS), including video-on-demand services. There are new provisions for ODPS, such as quotas and financial levies, that would impact original programming on online video platforms. Furthermore, with this new Directive, video-sharing platforms ("VSPs") are coming under scope for the first time. The VSP obligations are focused on mandatory safeguards related to child safety, terrorist content and hate speech, and advertising and product placement. As some open questions remain on how the provisions can best be implemented, USTR should monitor this situation carefully.

Separately, the EU is considering a new regulation on "platform-to-business" (P2B) relations that would require online intermediaries to provide redress mechanisms and meet aggressive transparency obligations concerning delisting, ranking, differentiated treatment, and access to data. These rules would apply not just to marketplaces with business users but also to non-contractual relations between businesses and platforms. Among other obligations, online intermediaries would be required to "outline the main parameters determining ranking," including "any general criteria, processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the

[62] *See* Warwick Ashford, *D-Day for GDPR is 25 May 2018*, Computer Weekly (May 4, 2016), http://www.computerweekly.com/news/450295538/D-Day-for-GDPR-is-25-May-2018.

[63] *See* Fact Sheet, *State of the Union 2016: Commission Paves the Way for More and Better Internet Connectivity for All Citizens and Business,* European Commission (Sept. 14, 2016), http://europa.eu/rapid/press-release_MEMO-16-3009_en.htm; *Report On OTT Services,* BEREC (Jan. 29, 2016), http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services; Lisa Godlovitch et al., *Over-the-Top (OTT)Players: Market Dynamics and Policy Challenges*, European Parliament (Dec. 15, 2015), http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)569979 (last visited Oct. 25, 2016).

[64] https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd

ranking."[65] These and other obligations represent disproportionate requirements that are likely to create market access barriers for developers, platforms, and SMEs seeking access to the EU market.

Recently, the European Parliament has sought to strengthen the P2B regulation by increasing the types of platforms covered (including mobile operating systems), banning vertical integration, introducing 'choice screens' for default services, and exposing search engines to more requirements. IA encourages USTR to monitor these developments and ensure that the P2B regulation does not threaten trade secrets and potentially violate the principles in Art. 19.16 of the USMCA.

Non-IP Intermediary Liability

The EU has proposed a draft terrorism regulation that would include a one-hour turnaround time for removing terrorist content upon notification from national authorities, backed by significant penalties, including fines of up to 4 percent of global turnover for certain systemic failures. The European Commission has included provisions that would require companies to take proactive measures to prevent abuse and re-uploading of terrorist content (in contravention of Article 15 of the e-Commerce Directive). It further authorizes national authorities in the EU to impose specific technical requirements on companies and require hosting providers to identify benchmarks and timelines for implementation, raising the likelihood of a web of conflicting and impractical requirements that would make it more difficult for U.S. services to compete in the European market, and decreasing the likelihood of a coordinated effort to fight against terrorist content.

On October 3, 2019, the Court of Justice of the European Union (CJEU) gave a decision in the case C-18/18 Glawischnig-Piesczek v Facebook that could have a negative global impact on free expression. The Court ruled that the e-Commerce Directive does not preclude national courts from ordering hosting service providers to block or remove illegal defamatory content on a global basis, not simply in the EU. The ruling also allows national courts to order the removal of "identical" or "equivalent" content. While the court suggested that removals of "equivalent" content must be understood narrowly, there is a danger that the ruling could be read in an overly broad way, leading to the over-removal of lawful speech and jeopardizing legitimate expression and innovation.

IA also encourages USTR and other agencies to engage with the European Commission on potential development of the Digital Services Act, a proposal by the EU Commission to reform the e-Commerce Directive that could starkly depart from U.S. law in this area. The Commission has suggested that this act would "update and uniform all the rules for all digital services in the Single Market, including rules on liability, illegal content, algorithmic accountability, and online advertising. It would also seek to reinforce and expand home-country control and put in place a dedicated regulator for online platforms and digital services." This Act has the potential to depart sharply from transatlantic principles on notice-and-action requirements, good Samaritan protections, avoidance of monitoring requirements, and other critical principles.

Separately, in the Delfi opinion, the European Court of Human Rights held an Estonian news site responsible for numerous user comments on articles, even though the company was acting as an intermediary, not a content provider, when hosting these third-party comments. In response to that

65 https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services.

decision, the Delfi.ee news site shut down its user comment system on certain types of stories, and the chief of one newspaper association stated: "This ruling means we either have to start closing comments sections or hire an armada of people to conduct fact checking and see that there are no insulting opinions." Without clarification following this opinion, numerous internet services are likely to face increased liability risks and market access barriers in Estonia.

Restrictions On Cloud Service Providers

The EU has taken legal action in the form of a proposal to regulate how EU banks and other financial companies use cloud services. This is part of a package of measures to help digitize the financial sector and modernize the EU's rulebook for the online market. The package of measures include initiatives to harmonize companies' online defense and regulate digital financial assets. The package also includes policy strategies on retail payments and capital markets. The draft addresses concerns about dependence on a small group of U.S. providers: chiefly Amazon Web Services, Google Cloud, and Microsoft Azure. The bill would create an oversight system designed to preserve the EU's financial system stability, along with monitoring of operational risks, which may arise as a result of the financial system's reliance on critical outsourced services.

Sharing Economy Barriers

EU treaties establish fundamental principles to ensure an adequate level of competition within the EU Single Market. The European Commission is the guardian of these treaties and is responsible for their enforcement between and within Member States. Across the EU, app-based service providers face barriers aimed at protecting incumbents, affecting the level of typical competition and infringing on principles such as the freedom of establishment, equality, non-discrimination and access to the profession. These shortcomings have been acknowledged in EU-funded sectoral studies but without any action by the EU.[66] The failure to enforce EU principles and to ensure effective competition in a level playing field creates barriers for new entrants, lowers the quality of services provided and raises prices for consumers.

Unilateral Or Discriminatory Digital Tax Measures

The European Commission is considering a DST as part of the financing package for its proposed COVID-19 recovery plan. While details are unknown, the EU DST could be based on a 2018 proposal that was not adopted due to opposition by a number of European nations. The 2018 EU proposal included a 3 percent tax on revenues from targeted advertising and digital interface services, and would have applied only to companies generating at least €750 million in global revenues from covered digital services and at least €50 million in EU-wide revenues for covered digital services. The structure of the tax expressly targeted U.S. companies and was the template for France's national DST.

The EU should refocus its efforts on digital taxation models that guarantee fairness and avoid discrimination and double taxation. IA believes that the EU proposal that includes a new DST would be unreasonable and would discriminate against U.S. digital companies by creating a targeted burden on U.S. commerce.

[66]https://ec.europa.eu/transport/sites/transport/files/2016-09-26-pax-transport-taxi-hirecar-w-driver-ridesharing-final-report.pdf

Several European governments continue to consider new revenue taxes targeting U.S. digital companies that conflict with international trade commitments and Member States' double taxation treaties, as well as undermine the process at the G20/OECD level to achieve a consensus-based solution on international tax reform. While the European Union ultimately decided not to pursue an EU-level digital tax, the new Commission President has announced plans to re-propose an EU-wide digital tax in early 2021 if an OECD solution is not reached by the end of 2020. Appetite to adopt unilateral digital taxes – politically rebranded as COVID-19 relief – is increasing and some Member States are moving ahead to enact national taxes, with the French DST signed into law in July 2019 (with retroactive effect as of January 2019). As of September 2020, France, Italy, and Austria have enacted unilateral DST measures. Further unilateral measures are expected to be enacted during 2020, notably in Czech Republic and in Spain. The more national digital taxes targeted at U.S. tech firms are enacted, the less likely that a consensus-based solution, that does not discriminatorily target U.S. tech companies, will be achieved at the OECD. Once enacted, these digital taxes will be difficult to remove. Further, some proposals, including the enacted French DST, contain no commitments to remove the national tax following an international agreement. DSTs may violate the EU's commitments under the WTO's General Agreement on Trade in Services ("GATS") by discriminating against U.S. companies in favor of EU companies. More specifically, under the GATS, the EU has agreed to provide "national treatment" to services and service suppliers of other WTO Members in the economic sectors that are covered by the DST. This means that the EU may not discriminate against those services and service suppliers in favor of its own "like" domestic services and service suppliers. The EU should refocus its efforts on reaching consensus with other leading economies within the OECD on any new digital taxation models so as to guarantee fairness and avoid discrimination and double taxation.

Complex VAT Registration And Compliance Requirements In Intra-EU Trade

The cost of compliance with VAT requirements when selling into the EU Single Market is higher for non-EU businesses than for EU businesses and constitutes a significant non-tariff barrier. The current EU VAT registration system is generally found to be fragmented, complex, and particularly costly for SMEs. This in effect restricts access to EU trade.

EU Member State Measures

Austria

Non-IP Intermediary Liability Restrictions

In September 2020, Austrian lawmakers presented a new law for platform accountability, the Kommunikationsplattformen-Gesetz (KoPl-G), or Communication Platforms Act, is a "draft federal act on measures to protect users on communication platforms."[67] The draft law is part of a larger package targeting "Hass im Netz" (online hate), amending the Austrian civil and penal codes — as well as media law — well beyond the introduction of the Communication Platforms Act itself. The draft law is a NetzDG-style law regarding intermediary liability.[68]

[67]"Draft Federal Act on measures to protect users on communication platforms (Communication Platforms Act)." https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2020&num=544
[68] London School of Economics and Political Science Blog. "A primer on Austria's 'Communication Platforms Act' draft law that

Unilateral Or Discriminatory Digital Tax Measures

In October 2019, Austria adopted a DST that applies a 5 percent tax to revenues from online advertising services. The law went into force on January 1, 2020. The tax applies only to companies with at least €750 million in annual global revenues for all services and €25 million in in-country revenues for covered digital services. The structure of the tax expressly targets U.S. companies. IA believes that the Austria DST is unreasonable and discriminates against U.S. digital companies by creating a targeted burden on U.S. commerce.

Belgium

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 and raising the price consumers must pay for their services.

- → *Vehicle requirements:* In the Brussels Capital Region, for-hire vehicles must cost at least €33,952.02 (excluding VAT) and have a wheelbase longer than 2.8 meters.
- → *Exams:* In the Brussels Capital Region, any prospective independent driver must pass a test entitled "examen d'accès à la profession d'indépendant" which includes accounting and corporate finance.
- → *Minimum trip duration and price:* Legislation in the three Belgian regions requires each for-hire vehicle trip to last a minimum of three hours and cost a minimum of €108.

Unilateral Or Discriminatory Digital Tax Measures

In fall of 2020, the new Belgian government indicated it will impose a digital service tax by 2023 if an international deal on digital taxation can not be reached.

Czech Republic

Unilateral Or Discriminatory Digital Tax Measures

The Parliament of the Czech Republic is considering a draft law that would apply a 7 percent DST to revenues from targeted advertising, digital interface services and the sale of user data. Subsequently the Ministry of Finance announced its support for a lower, 5 percent rate, while shifting the effective date to the beginning of 2021. The tax, which has a similar structure to the French DST, would apply to companies that meet the following thresholds, either individually or as part of a group: global revenue

aims to rein in social media platforms" https://blogs.lse.ac.uk/medialse/2020/09/14/a-primer-on-austrias-communication-platforms-act-draft-law-that-aims-to-rein-in-social-media-platforms/

exceeding EUR750 million; and revenue from supplying covered services in the Czech Republic exceeding CZK 100 million and the revenue from the supply of covered services in the EU amounts to at least 10 percent of total revenue in the EU. The structure of the tax will expressly target U.S. companies while insulating Czech competitors in the advertising and digital markets from scope of coverage. IA believes that the Czech Republic's DST draft law would be unreasonable and would discriminate against U.S. digital companies by creating a targeted burden on U.S. commerce.

Denmark

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services must be licensed to provide commercial passenger transport. These new entrants face multiple market access and operational restrictions that serve no public interest but are instead intended to protect incumbents.

- → *License cap:* There are currently caps on the number of commercial passenger transport licenses and these caps will only be fully removed in January 2021.
- → *Exams:* Prospective drivers must attend a 74-hour course and pass a test on first aid, conflict prevention, and other subjects. This test includes a Danish language test. Drivers must either join a taxi booking company or establish their own booking office, which requires a separate licensing exam that tests issues of contract, tax, insurance, employment and transportation law; work environment; economics and accounting; tender processes; conflict management; and maintaining a dispatch center.
- → *Financial capacity:* Drivers must show DKK 40,000 in available funds for the first permit/vehicle and DKK 20,000 for any subsequent permit/vehicle.
- → *Mandatory redundant equipment:* Vehicles must be equipped with various in-car equipment, including taximeters and signage that are redundant given current smartphone-based technology.
- → *Maximum prices:* Commercial transport providers must price below set ceilings, limiting competition and the use of dynamic pricing algorithms to balance supply and demand and thus deliver consumers a more reliable service.

Finland

Data Flow Restrictions And Service Blockages

In a communication issued in 2018, the Finnish Ministry of Finance announced its intention to introduce a requirement for companies in the financial sector to build back-up systems in Finland in the event of exceptional circumstances and serious disruptions. According to this, in-scope companies would be subject to precautionary measures to maintain in Finland such information systems and information resources that are necessary for the uninterrupted operation of the financial markets. In July 2020, in order to assess any gaps in preparedness capacity, the FIN-FSA requested entities under scope to submit by December 31, 2020 an entity-specific plan on how to ensure the operability and accessibility

of critical services for end customers in circumstances where foreign service provision is completely unavailable. Firms' preparedness plans will then inform the work of the Ministry of Finance, with a view to issue legislation on this in 2021. Effectively, this could represent an indirect data localization requirement, presenting a market barrier and a risk to free market and competition in Finland for CSPs which don't have local data centers.

France

Copyright-Related Barriers

Under France's "image indexation" law, an "automated image referencing service" must negotiate with a French rights collection society and secure a license for the right to index or "reference" a French image. Individual artists or photographers cannot opt out of this licensing regime. This law requires online services to seek a license for any indexation of an image published in France.[69] This law reflects the same spirit as the German and Spanish ancillary copyright regimes, insofar as it creates a regulatory structure intended to be exploited against U.S. exporters – a "right to be indexed." By vesting these indexing "rights" in a domestic collecting society, the law targets an industry that consists largely of U.S. exporters. As several industry and civil society organizations have previously noted, the law will impact a wide range of online services and mobile apps.[70] These requirements present significant market access barriers for the large number of online services in the U.S. and elsewhere that work with images.

Data Flow Restrictions And Service Blockages

France's ministerial regulation on "public archives" requires any institution that produces public documents to store and process these data only on French soil. These regulations function as data localization requirements for U.S. cloud providers seeking to provide cloud services to the French public sector.

Non-IP Intermediary Liability Restrictions

Then French Prime Minister Édouard Philippe announced a proposal on illegal content that includes a one day removal requirement (expanding on Germany's NetzDG Law), which could be extended to other forms of problematic content such as so-called "obvious" hate speech. The law would also require platforms and search engines to implement "the appropriate means" to prevent the "re-broadcasting" of removed content in certain circumstances. It would allow a regulator to assign fines up to 4 percent of global annual turnover for repeated non-compliance, and for courts to assess fines of up to €1.25M for individual failures.

On July 9, 2019, members of the lower house of parliament in France approved a measure that requires tech companies like Facebook and Google to remove content the French government deems "hate

[69] Art. L. 136-4, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032854341&fastPos=1&fastReqId=643428459&categorieLien=id&oldAction=rechTexte. Loi 2013-46 du 10 décembre 2013 Project de Loi Dispositions relatives aux objectifs de la politique de défense et à la programmation financière, rapport du Sénat, http://www.senat.fr/petite-loi-ameli/2015-2016/695.html.

[70] Open Letter to Minister Azoulay, March 2016, available at http://www.ccianet.org/wp-content/uploads/2016/03/OpenLetter-to-Minister-Azoulay-Image-Index-Bill-on-Creation-Eng.pdf.

speech." The bill was sponsored by Laetitia Avia of La Republique en Marche, who has received personal death threats online. The provision was adopted to be part of a larger internet regulation bill, Law No. 2004-575, and would create a 24 hour deadline for social networks to remove hate speech from their platforms once it's flagged. Companies would also be required to provide the government with identification information of users cited to produce "hate speech," which includes content including "acts of terrorism, making the apology of such acts or involving an attack on the dignity of the human person, incitement to hatred, and violence." Companies that fail to comply with the law risk fines up to €1.25 million. The upper-house of the Senate will examine the legislation next.

In May 2019, France released an interim report Creating A French Framework To Make Social Media Platforms More Accountable with an outline for what French legislation will look like to regulate Facebook, Twitter, YouTube, and Snapchat specifically. The report outlines recommendations that include transparency for how companies order content on their platforms, transparency for which aspects of Terms Of Service apply to moderating content, and creating an independent administrative authority, open to civil society, to oversee company actions in following the guidelines.

Restrictions On U.S. Cloud Service Providers (CSPs)

France adopted a 'Cloud First' policy in 2018. This momentum has been followed rapidly by a tender to reference public CSPs. However, despite this good momentum, cloud adoption is still fragile in France from the U.S. CSP perspective. Indeed, the French Minister of Finance recently announced France's intention to build a national "trusted cloud." French CSPs have been requested by the French government to invest in the project, which could constitute a protectionist obstacle to the use of U.S. CSPs cloud in the public sector in France.

SecNumCloud

The French cyber-security agency ANSSI is currently blocking our application to enter into the qualification process of their SecNumCloud security certification due to concerns around the CLOUD Act and localization of certain AWS services. Receiving the certification is important validation of the security of the cloud to commercial sector (i.e. enterprise) customers. USTR can raise concerns with the Prime Minister and the Ministry of Foreign Affairs that SecNumCloud qualification is not accessible to U.S. companies thus preventing fair trade conditions in public tenders.

Sovereign Cloud Program

In parallel to the GAIA-X initiative, France is pursuing its own 'sovereign cloud program'. It is yet to be defined but will likely incorporate two key components; first, a legal protection for French companies from foreign laws with extraterritorial effects (including the U.S. CLOUD Act). It would prevent any cloud provider from transferring customer's data to a non-EU country. Concretely, this law would enforce GDPR's fine standards. The second key element of the French 'sovereign cloud program' would be a cloud services' portfolio dedicated to sensitive data and opened only to domestic CSPs. USTR can raise concerns with the Prime Minister and the Ministry of Foreign Affairs that there is a massive work in France to ban U.S. CSPs from a serious number of workloads. If SecNumCloud qualification is not accessible to U.S. companies, if a blocking statute creates a legal arsenal to prevent sharing data with U.S. authorities and if a specific portfolio is restricted to domestic providers, France is proactively preventing fair trade

conditions in public tenders.

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.

- *Platform liability:* French law holds app-based dispatchers of licensed transportation liable for the transportation service provided by the drivers using the app. The app-based dispatcher of licensed transportation, or "platform," is also responsible for making sure that the independent drivers and vehicles comply with the specifications listed hereafter.
- *Vehicle requirements:* For-hire vehicles must be less than six years old and equipped with at least four doors. They must have a minimum length of 4.5 meters, a minimum width of 1.7 meters, and 115 horsepower (electric or hybrid vehicles are exempt from these restrictions).
- *Exams:* French law requires prospective for-hire vehicle drivers to pass stringent exams. The exams include both written and practical sections, covering topics such as general culture, business management, and English language. Examination slots are offered infrequently and there is a delay of approximately 3 months between the written and practical exams. As a result, prospective for-hire vehicle drivers require between six and 12 months to become licensed. The average pass rate in 2018 was below 50 percent due to the difficulty of the process.
- *Capital requirements:* Drivers must provide €1,500 in equity or a bank guarantee when registering their company with the Ministry of Transportation.
- *Return-to-garage rule:* Between trips, drivers must return either to their registered place of business or to an authorized off-street parking space, unless a new trip request is received on the way to either place.
- *Geolocation prohibition:* French rules forbid for-hire drivers and apps facilitating their services from informing consumers about the availability and the location of a for-hire vehicle prior to a booking request—taxis face no such restriction.

Unilateral Or Discriminatory Digital Tax Measures

In 2019 France moved forward with a Digital Services Tax (DST) that specifically targets the U.S. digital sector. The French DST is expected to hit 29 non-French companies and potentially zero French companies, generating some €500 million per year, with significant increases over time.[71]

The French DST will be applicable to gross revenues derived from certain digital services provided in France in which there is user involvement.[72] The rate is set at 3 percent of "qualifying" revenues and will

[71] https://www.dentons.com/en/insights/articles/2019/july/15/french-digital-services-tax-dst

[72] https://www.ey.com/gl/en/services/tax/international-tax/alert--frances-parliamentary-commission-agrees-on-digital-services-tax

concern companies with worldwide revenues of at least €750 million and French "qualifying" revenues of at least €25 million.[73] Efforts by the French and others contradict longstanding global consensus-based practices and would result in double taxation on American businesses.

IA believes that global tax rules should be updated for the digital age, but discriminatory taxes against U.S. firms are not the right approach. In proceeding with their DST, France took a unilateral approach even as a worldwide solution at the Organisation for Economic Co-operation and Development (OECD) is being developed.

IA encourages the U.S. government to continue to engage in the OECD process.[74] It is positive that the 129 members of the OECD/G20 Inclusive Framework on Base Erosion and Profit Shifting agreed on a road map for resolving these tax challenges and committed to work toward a consensus-based long-term solution by the end of 2020.[75]

By choosing to go-it-alone, France sets the stage for a country-by-country approach toward taxation of tech companies in Europe. The French DST comes after the European Finance Ministers decision in December 2018 to reject new revenue taxes narrowly targeted at U.S. digital companies. After the Finance Ministers' vote, similar DST's have been either announced or published in Austria, Belgium, Czechia, Italy, Poland, Slovenia, Spain, and the United Kingdom.[76] As these individual countries consider these discriminatory actions, countries throughout Asia and Latin America are tracking and preparing to follow their lead in specifically targeting U.S. tech companies.

France should refocus its efforts on reaching consensus with other leading economies within the OECD on any new digital taxation models to guarantee fairness and avoid discrimination and double taxation.[77] This is especially true as the French online economy is one of the largest markets in the world, ranking second in Europe and fifth in the world in terms of online consumption in 2017. The market grew by 14.3 percent between 2016 and 2017.[78]

IA believes that the DST sends a strong signal to internet companies of all sizes – from small businesses to major organizations – that France is no longer a welcoming environment for business investment and exports. Due to previous forward-thinking policies from successive governments and a reasonable and stable business, legal, and regulatory environment, France has earned a reputation as a strong place for U.S. firms to invest and export to, especially internet companies aiming to export to not only France but also European markets.[79]

The DST puts this position at risk. Companies are likely to either reduce their exports to and investment in France, or divert their focus to more welcoming jurisdictions. Consideration must also be given to who ultimately bears the burden of the DST. Although it is branded as a tax on large digital companies, there is a high likelihood that the cost of the tax will be passed down the supply chain to small- and medium-sized enterprises (SMEs) and end consumers, and it is those SMEs and consumers in France

[73] https://www.gouvernement.fr/en/gafa-tax-a-major-step-towards-a-fairer-and-more-efficient-tax-system
[74] http://www.oecd.org/tax/beps/
[75]https://www.oecd.org/tax/beps/programme-of-work-to-develop-a-consensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.pdf
[76] https://taxfoundation.org/digital-taxes-europe-2019/
[77] https://www.gouvernement.fr/en/tax-on-digital-services-an-efficacious-fiscal-justice-measure
[78] https://2016.export.gov/france/doingbusinessinfrance/index.asp
[79] France Country Commercial Guide (CCG 2018), U.S. Commercial Service. https://2016.export.gov/france/doingbusinessinfrance/index.asp

who will suffer the incidence of the tax. A recent study found only 5 percent of the digital tax's burden will fall on the large internet companies it aims to target. Instead, the study said consumers will absorb 55 percent of the cost and 40 percent will be borne by businesses that use digital platforms.[80]

The design of the DST also creates complexity in the French tax system and creates uncertainty for U.S. SMEs looking to export because they will now have to determine if they will be captured by the tax, either directly or indirectly. Consequently, it places a new compliance burden on SMEs, even if they are exempt from the tax, as significant work would be required to produce bespoke financial information purely to identify whether they are within the scope of the DST. The DST further makes France a less attractive place to operate an internet business. In addition, the thresholds will also create a disincentive to grow for firms that are at the margin for exemption.

The initiation of the 301 investigation is an important step in exercising American leadership to stem the tide of new discriminatory taxes across Europe, and IA looks forward to working with USTR throughout this process.

Germany

Copyright-Related Barriers

Ancillary copyright laws in Germany and Spain have proven detrimental for U.S. companies, EU consumers, publishers, and the internet ecosystem that requires adequate protection of rights under copyright law. The German Leistungsschutzrecht was enacted in August 2013, and holds search engines liable for making available in search results certain "press products" to the public.[81] The statute excludes "smallest press excerpts," making the liability regime less clear and exposing search engines to confusing new rules. These laws specifically target news aggregation, imposing liability on commercial search engines and other online platforms while exempting "bloggers, other commercial businesses, associations, law firms, or private and unpaid users."[82] By extending copyright protection to short snippets or excerpts of text used by search engines and other internet platforms, this law violates Article 10(1) of the Berne Convention, directly violating the ability of online platforms to use permissible quotations under the TRIPS Agreement.

On December 24, 2018, the Higher Regional Court of Saarbrucken, Germany ruled that a domain registrar could be held secondarily liable for the infringing action of a customer which offered access to copyright-infringing material on a website linked to a domain sold by said registrar. Secondary liability can be established, according to the court, if the registrar fails to take action in spite of rightsholder notification.

Discriminatory Or Opaque Application Of Competition Regulations

Germany is reportedly considering allowing competition authorities to subject certain market-leading companies to prohibitions and penalties even if there has been no showing of anti-competitive abuse, which would be flatly inconsistent with U.S. and global practice. The companies that would be targeted

[80] https://taj-strategie.fr/content/uploads/2020/03/dst-impact-assessment-march-2019.pdf
[81] German Copyright Act (1965, as last amended in 2013), at art. 87f(1), http://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html#p0572.
[82] Id.

are online platforms and other companies that German authorities accuse of "transcending" their dominance in a given market because, for example, they are vertically integrated or control sensitive business data. Other proposed rules would also target online platforms, including a rule that would make it easier for competition authorities to oblige platforms to provide access to data. Many of these proposed rules include fuzzy definitions of longstanding concepts in competition law (such as "dominance" and "essential facilities") and depart from global competition norms, including by shifting the burden of proof away from competition authorities and towards targeted companies. Together these rules could stifle U.S.-German digital trade and could serve as a model for other countries that are looking to challenge or undermine U.S. businesses operating in this sector. Despite a finding from Germany's own Monopolies Commission that these changes are not empirically necessary, the proposal continues to advance.

Non-IP Intermediary Liability Restrictions

The German NetzDG law, which is now in force, mandates removal of "obviously illegal" content within 24 hours and other illegal content within seven days. Online services are subject to penalties of up to €50 million if they are found to be out of compliance with this law. The law applies to online services with more than 2 million users in Germany, including a wide range of U.S. services. It covers provisions of the German Criminal Code connected to illegal content – not just obviously illegal content related to terrorism and abuse, but also a wide range of other activities that are criminalized under German law, including incitement to hatred, insults, and defamation. On July 2, 2019, German authorities announced a €2.3 million fine for Facebook for violating the NetzDG law. The law requires providers to report the number of complaints of illegal content to German authorities. The German Interior and Justice Ministers have announced their intention to re-open the NetzDG to expand its provisions further.

Despite NetzDG, on January 12, 2019, the District Court of Tubingen in Germany ruled that Facebook violated its duties by deleting a comment that one user had posted which insulted right-wing extremists. The court argued that the user had not violated the platform's community standards, and that his comment was "covered by the freedom of opinion that indirectly binds Facebook to its customers in Germany."

This significant divergence from U.S. and EU frameworks on non-IP intermediary liability is concerning on its own, and is being closely observed by governments around the world that may be considering similar actions. IA urges USTR to monitor these developments and engage with counterparts in Germany and elsewhere to ensure that any measures on controversial content do not introduce burdensome market access restrictions on U.S. services.

Overly Restrictive Regulation Of Online Services

The German film levy law[83] extends film funding levies from Germany to also foreign pay video on demand (VOD) services despite the EU Audiovisual Media Services Directive's Country of Origin principle, according to which providers only need to abide by the rules of a Member State rather than in multiple countries. The law further extends the levy to foreign ad-funded VOD services insofar as they make cinematographic works available to Germans. Such services have to pay a proportion of their German revenues to the regulatory body, thus hindering cross-border businesses and raising costs for consumers.

[83] https://www.ffa.de/film-levy.html

Restrictions On U.S. Cloud Service Providers

The German Ministry for Economic Affairs works on a concept to promote a European alternative to the large U.S. cloud service providers (CSPs) for the German economy. In a first draft concept, the Ministry writes that it wants to address dependency on foreign cloud providers. The project is called GAIA-X, and would connect existing central and decentral infrastructure solutions via open source applications and interoperable standards. An official release is currently scheduled for German Digital Summit on October 29, 2020. IA is concerned this project could lead to protectionist limitations for cloud public sector entities in Germany for U.S. CSPs.

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.

- → *Exams:* Local chambers of commerce organize exams for prospective operators. Exam spots are limited and typical waiting times can stretch up to several months. Some parts of the exam have nothing to do with running a for-hire vehicle company (for example, where to dispose of special waste). These tests are very burdensome and a major hurdle for prospective drivers to open an independent business, resulting in a failure rate of approximately 70 percent.
- → *Return-to-garage rule:* For-hire vehicle drivers must return to their place of business/residence after completion of each trip, unless they receive a new trip request during their trip or on their way back to the place of business/residence. That request, however, must be actively accepted and dispatched at the company's place of business/independent driver's residence. This is especially burdensome for small businesses and independent operators.

Greece

Copyright-Related Barriers

Greece's "Committee for Online Copyright Infringement," an administrative committee that can issue injunctions to remove or block potentially infringing content, is now up and running. Instead of adhering to the U.S. system by submitting a DMCA notice, a rights holder may now choose to apply to the committee for the removal of infringing content in exchange for a fee.

On November 9, 2018, the committee ordered internet service providers to block access to 38 domains offering access to copyright-infringing material, specifically targeting pirated movies with added subtitles. The commission has previously attempted to have websites blocked that allow copyrighted material to be illegally displayed, but the Athens court had stated that barring access to torrent sites is disproportionate and unconstitutional. While examples of implementation are still limited, this measure represents a significant divergence from U.S. procedures on efficient removal of infringing content.

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 operational restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by greatly raising the price consumers must pay for for-hire services and lowering the quality of the services they can provide.

- → *Minimum trip duration:* For-hire vehicle trips must last a minimum of three hours.
- → *Return-to-garage rule:* Between trips, drivers must return to their registered place of business.

Hungary

Filtering, Censorship, And Service-Blocking

In Hungary, legislation enables the order by local authorities of a 365-day ban of online content, such as websites and electronic applications that advertise passenger transport services.[84]

Unilateral Or Discriminatory Digital Tax Measures

Hungary has implemented an advertising tax aimed at foreign suppliers of media content and advertising services.

The government is limiting foreign entities' ability to obtain ownership in Hungarian companies in "strategic sectors," with the latter defined broadly. The limitation was introduced via decree in May during the state of emergency, which decrees were automatically invalidated when the state of emergency was lifted a few weeks later. However in another decree, the limitation was essentially maintained and extended until the end of 2020.

This means that the Minister of Innovation and Technology, László Palkovics, must consent to the following transactions above a value limit of 10 percent of the business share or an investment exceeding EUR 1 million; transfer of a certain proportion of ownership; capital increase; transformation, merge, or division of a strategic company; the issue of a convertible or subscription bond; establishment of a usufruct right on the shares of a strategic company. The minister has 30 days to make this decision.

Italy

Copyright-Related Barriers

The Italian Communications Authority is empowered to "require information providers to immediately put an end to violations of copyright and related rights, if the violations are evident, on the basis of a rough assessment of facts." This law amounts to a copyright 'staydown' requirement that conflicts with

[84] *See* Marton Dunai, *Hungarian Parliament Passes Law That Could Block Uber Sites*, Business Insider (June 13, 2016), http://www.businessinsider.com/r-hungarian-parliament-passes-law-that-could-block-uber-sites-2016-6. http://www.businessinsider.com/r-hungarian-parliament-passes-law-that-could-block-uber-sites-2016-6.

both Section 512 of the DMCA and the E-Commerce Directive, and will serve as a market access barrier for U.S. services in Italy.

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:* While Italian transportation laws do not impose a cap on the number of for-hire vehicle licenses available, municipalities nevertheless grant for-hire vehicle licenses on an irregular and arbitrary basis. In Rome, for example, there are only 1,024 for-hire vehicle licenses and the last one was issued in 1993 (compared to 7,800 taxi licenses). In Milan, there are only 229 for-hire vehicle licenses and the last one was issued in the 1970s (compared to 5,200 taxi licenses).

Unilateral Or Discriminatory Digital Tax Measures

Italy has adopted a DST, with similar structure to the French DST that includes a 3 percent tax on revenues from targeted advertising and digital interface services. This tax applies only to companies generating at least €750 million in global revenues for all services and €5.5 million in in-country revenues for covered digital services. Key details are still to be defined but the government intends to begin collection in 2021. We expect the tax to predominantly affect U.S. firms, as senior government officials, including Former Deputy Prime Minister Luigi Di Maio, directed that prior iterations of the tax be scoped to impact large U.S. tech firms. IA believes that the Italy DST is unreasonable and discriminates against U.S. digital companies by creating a targeted burden on U.S. commerce.

Poland

Copyright-Related Barriers

In January 2017 the CJEU in the case of OTK v. SFP[85] concluded that Article 13 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (the Enforcement Directive) shall not preclude EU Member States from allowing a rights holder in an infringement proceeding to demand payment in an amount higher than the appropriate fee which would have been due if permission had been given for the work concerned to be used. In addition, in such a situation, the court clarified that there is no need for the rights holder to prove the actual loss caused to him as a result of the infringement. This equates to the introduction in EU law of punitive damages, without any appropriate safeguards.

[85] C-367/15 Stowarzyszenie 'Oławska Telewizja Kablowa' v. Stowarzyszenie Filmowców Polskich, ECLI:EU:C:2017:36, European Court of Justice (January 25, 2017).

Restrictions On Cloud Service Providers

Article 6 of the Polish Bank Law provides that financial authorities can outsource some of their operations to third parties pending an assent from the supervising authority (including processing data in the cloud). The law, however, due to security reasons, limits this possibility to only one level of subcontractors, meaning that they cannot rely on third party cloud providers. This significantly limits the potential of growth in the financial sector for cloud providers.

Portugal

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 category. In addition, for-hire platforms will face restrictions that will limit their capacity to compete.

- → *Regulatory tax:* Platforms will have to pay a 5 percent regulatory tax on their service fee to promote taxi modernization and public transportation. No other regulated transportation activity pays such a tax.
- → *Cash payments prohibited:* Mandatory electronic payments will exclude significant segments of the population from these services. Taxi services face no such restriction.
- → *Price controls:* Prices will not be able to fluctuate freely according to supply and demand and are instead capped at twice the average fare price of the previous 72 hours. This will decrease service reliability and driver earnings.

Spain

Copyright-Related Barriers

In Spain, reforms of the ley de propriedad intelectual in 2014 resulted in an unworkable framework, requiring "equitable compensation" for the provision of "fragments of aggregated content" by "electronic content aggregation service providers."[86] Like the German law, the Spanish law creates liability for platforms using works protected under international copyright obligations in the TRIPS Agreement. The Spanish law is arguably even worse than the German law because it does not allow publishers to waive their right to payment: they have to charge for their content, irrespective of whether they have existing contractual or other relationships with news aggregators, and irrespective of creative commons or other free licenses. The tariffs are arbitrary and excessive: one small company was asked to pay €7,000 per day (€2.5 million per year) for links or snippets posted by its users.[87]

[86] Boletín Oficial de las Cortes Generales, Congreso de los Diputados, Informe de la Ponencia: Proyecto de Ley por la que se modifica el Texto Refundido de la Ley de Propriedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, No. 81-3 (July 22, 2014), available at http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-81-3.PDF.

[87] https://www.elconfidencial.com/tecnologia/2017-02-07/canon-aede-meneame-internet-facebook-agregadores_1327333/

The Spanish ancillary copyright law yielded similar results to the German law. Soon after the enactment of the Spanish law, Google News shut down in Spain.[88] An economic study prepared by the Spanish Association of Publishers of Periodical Publications found that the result of ley de propriedad intelectual, which was meant to benefit publishers, was higher barriers to entry for Spanish publishers, a decrease in online innovation and content access for users, and a loss in consumer surplus generated by the internet. The results are most concerning for smaller enterprises facing drastic market consolidation and less opportunity to compete under the law.[89]

These ancillary copyright laws have proven detrimental for U.S. companies, consumers, publishers, and the broader internet ecosystem.

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:* Transportation law limits the number of for-hire vehicle licenses that a region may grant to one for every 30 taxi licenses in that region.
- *Licensing insecurity:* In September 2018, the national government approved a Royal Law Decree that transfers power over for-hire vehicles from the national government to the regions. This was a step acknowledged as so likely to lead directly to the cancellation of VTC licenses by subnational governments that the national government delayed its implementation for four years and described the delay as an expropriation payment to compensate VTC license holders.
- *Minimum wait time:* In January 2019, the regional government of Catalonia issued a law decree that mandates a minimum delay of 15 minutes between the time at which a for-hire vehicle trip is booked and the time at which the trip may begin. Other regional governments (e.g. Valencia, Aragon, and the Balearic Islands) have since followed suit, introducing similar minimum wait times.
- *Return-to-garage rule:* Catalonia, Valencia, Aragon, and the Balearic Islands have also introduced versions of "return to garage" requirements, prohibiting for-hire vehicles from traveling on public streets unless carrying a passenger or headed to a pickup.
- *Geographic restrictions:* For-hire vehicles may only provide service in regions other than their home region up to a maximum of 20 percent of their trips in any three-month period.

[88] *An Update on Google News in Spain*, Google Europe Blog (Dec. 11, 2014) http://googlepolicyeurope.blogspot.com/2014/12/an-update-on-google-news-in-spain.html.

[89] *Economic Report of the Impact of the New Article 32.2 of the LPI (NERA for AEEPP)*, Spanish Association of Publishers of Periodicals (July 9, 2015), http://coalicionprointernet.com/wp-content/uploads/2015/07/090715-NERA-Report-for-AEEPP-FINAL-VERSION-ENGLISH.pdf.

- *De facto price floor:* For-hire vehicles are prohibited from selling their service on an individual seat basis and must instead sell the service of the entire vehicle.
- *Data sharing demands:* In 2017, the regional government of Catalonia passed a Law Decree (implementing regulation required before it enters into force) that requires for-hire vehicle licensees to electronically submit to the government's online registry the following data before any trip is begun: (1) name and ID number of the for-hire vehicle licensee, (2) license plate number of vehicle, (3) name and ID number of the rider, (4) the location and time of the agreement for service to be provided, (5) location and time where the service will be initiated, (6) location and time where the service will be terminated, (7) other data that the government may choose to require. A similar Royal Decree was approved in December 2017 at the national level and a national electronic registry has been in place since April 2019.

Unilateral Or Discriminatory Digital Tax Measures

Spain is considering a draft DST, with similar structure to the French DST, which would apply a 3 percent tax to revenues from targeted advertising and digital interface services. This tax would apply only to companies generating at least €750 million in global revenues for all services and €3 million in in-country revenues for covered digital services. The structure of the tax expressly targets U.S. companies. IA believes that the Spanish DST proposal is unreasonable and would discriminate against U.S. digital companies by creating a targeted burden on U.S. commerce.

Sweden

Copyright-Related Barriers

A recent Supreme Court ruling[90] in Sweden has resulted in the banning of websites displaying mere photos of public art exhibited in public spaces. Even though Sweden has a copyright exception for such photos, the Court found the commercial interest a site may have in using works of art is a limit to the application of the exception. The case was brought by a visual arts collecting society against offentligkonst.se, an open map with descriptions and photographs of works of public art across Sweden which is operated by Wikimedia SE. This means that even in the case of a webpage written by an amateur blogger, the mere reproduction of a photo of public art, which would elsewhere be deemed fair use, can now lead to fines when this page displays an ad.

On October 15, 2018, Sweden's Patent and Market Court ordered local ISP Telia to block torrent and streaming platforms offering access to copyright-infringing material, following a decision in February 2017 applying to a local ISP Bredbandsbolaget. Telia has since appealed the decision.

Restrictions On U.S. Cloud Service Providers

U.S. CSPs continue to face challenges in Sweden caused by the conflict of law perception between Swedish law (disclosure under the Secrecy Act) and the U.S. CLOUD Act fueled in part by protectionist sentiment. Since the first negative statement by the eSam legal expert group in late 2018, we have seen

[90] April 4, 2016, case Ö 849-15, Bildupphovsrätt i Sverige ek. för v. Wikimedia Sverige.

a proliferation of negative statements, guidelines, and opinion pieces emerging based on misconceptions about the U.S. CLOUD Act, questioning whether it is compatible with Swedish law for the public sector to use U.S. CSPs. A formal public investigation began in 2019, and will run until Q3 2021 to consider 1) the legal preconditions for outsourcing IT operations and 2) more durable forms of coordinated state IT operations. AWS is currently engaged with State and Commerce to put pressure on Sweden to resolve the issue. The U.S. Department of Commerce at the U.S. Embassy to Sweden is engaging on this issue, but the Embassy is constrained due to Ambassador Ken Howery's conflicts of interest arising from his investments in the cloud industry. The USTR could potentially serve as a more effective interlocutor in the bilateral dialogue to unblock the issue with the Swedish Government.

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services must be licensed as a taxi driver. These new entrants face multiple market access and operational restrictions that serve no public interest but are instead intended to protect incumbents.

- *Capital requirements:* Swedish rules impose a capital requirement of SEK 100,000 for one vehicle and SEK 50,000 for each subsequent vehicle.
- *Mandatory redundant equipment:* Every vehicle must either be equipped with an approved taximeters (or secure an exemption) and must be connected to a central accounting system, making it more difficult for drivers to report their taxes when working via apps.

Hong Kong

Copyright-Related Barriers

Previously, 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. USTR should urge Hong Kong counterparts to adopt reforms introducing a safe harbor regime in line with 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.

Data Flow Restrictions And Services Blockages

In October 2019, the Hong Kong Securities and Futures Commission (SFC) issued a circular that mandates financial institutions to store data in Hong Kong with locally-registered external electronic service providers (EDSP) or requires the financial institution's internationally-registered EDSP to provide the SFC unrestricted access to a financial institution's data hosted with the EDSP as a condition for doing business. The circular, as written, bypasses existing legal processes and provides blanket authorization for the regulator to access customer records. The circular mandates EDSPs to respond to the SFC's request for customer data in contradiction with the EDSPs' legal obligation to their customer. We urge the Hong Kong SFC to consider alternative options to make the implementation of the circular workable for EDSPs located in and outside of Hong Kong.

Filtering, Censorship, And Service-Blocking

There have been concerns about the ability of Hong Kong to maintain a free and open digital ecosystem after the imposition of a national security law on Hong Kong on June 30, 2020. The internet serves as a platform to exchange information and knowledge and drive collaboration between both public and private sectors. The Hong Kong government should continue to support a free and open internet which is the foundation of digital trade.

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.

- → *License cap:* For-hire vehicle licenses (Hire Car Permit - HCP) are capped at 1,500 by regulation.
- → *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.

India

Copyright-Related Barriers

India's intermediary liability framework (mentioned below) poses a significant risk to U.S. internet services. In particular, India does not have a clear safe harbor framework for online intermediaries,[91] meaning that internet services are not necessarily protected from liability in India for user actions in case of copyright infringements.

Divergence From Privacy Best Practices

The Indian Government has issued several policies re-emphasizing its intention to impose data localization requirements on foreign companies over the last year. Most significant of these is the Personal Data Protection Bill, 2019 (PDP Bill). Introduced in Parliament in December 2019 by the Ministry of Electronics and IT (MeitY), the PDP Bill proposes a data localization mandate, requiring businesses to ensure the storage of 'sensitive personal data' in India. Sensitive personal data includes financial data which is often routinely processed by businesses. Cross-border transfers of sensitive personal data would be allowed on limited legal bases, such as under contracts that are approved by a proposed regulator. Separately, the law would require a category of 'critical personal data' to be stored and processed almost exclusively within India. Overseas transfers of critical personal data would only

[91] 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 . . .").

be allowed when the transfer was necessary for a particular person or entity engaged in the provision of health services or emergency services; where the transfer was directed to a person or entity in a country or international organization pursuant to an adequacy determination, and if the transfer did not harm India's security interests. This category of critical personal data would be prescribed by the central government. The PDP Bill is currently being examined by a parliamentary committee, which could recommend amendments that the government may choose to accept. Given the wide and open-ended definitions of sensitive and critical data, this proposal could seriously impede cross-border data flows and free trade.

In August 2020, a MeitY committee tasked to look into the issue of non-personal data (NPD) released recommendations proposing a governance framework for NPD. Borrowing from the PDP Bill, the committee recommended localization of 'sensitive' non-personal data (such as health anonymized/aggregated personal data) and 'critical' non-personal data. While cross-border transfers of sensitive non-personal data would be allowed in limited conditions, the framework would require that critical non-personal data was only be stored and processed within India.

The government is also working on a national e-commerce policy. Reports have suggested that the current draft recommends that: (i) certain categories of data such as defense, medical records, biological records, cartographic data, and genome mapping data should not be transferred outside India; (ii) certain categories of e-commerce data should be mirrored/stored in India (with the government/a proposed e-commerce regulator deciding the categories). Such proposals, if implemented, would significantly affect cross-border flows of data and pose barriers to free trade.

IA strongly encourages USTR and other U.S. agencies 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.

On August 5, 2019, Kashmir imposed a complete communications blackout that blocked internet access across the state of Jammu & Kashmir. The blackout is part of measures the government has taken to prevent protests against the government's move to revoke a controversial special status for the state. As of September 10, 2019, the internet blackout remains in the area.

In September 2019, the MeitY constituted a committee to deliberate on a governance framework for non-personal data. In August 2020, it released a report outlining a mandatory sharing and access framework for non-personal data. The NPD Framework would apply to aggregated data held by private companies, much of which would be considered proprietary. Such a requirement would set a negative precedent for digital businesses worldwide. Businesses would be compelled to share such data with competitors and the government. Any framework of mandatory data sharing would raise serious IP concerns and would infringe upon India's obligations under international treaties such as the TRIPS. The framework would also impose severe compliance burdens on business, including mandatory disclosure and registration requirements; building and maintaining significant data-sharing infrastructure; and obtaining user consent before using anonymized personal data. The imposition of unnecessary

regulatory requirements would undermine ease of doing business and lead to increased and potentially unviable compliance and operational costs for foreign corporations.

The Indian government's think tank, the NITI Aayog, released a draft policy document – the 'Data Empowerment and Protection Architecture' (DEPA) in September 2020. The DEPA is a consent-based framework for individuals to securely access and share their information between businesses. By proposing a new technological architecture consisting of India-specific data protection, processing, and sharing standards, the DEPA could lead to trade restrictive standards that inflict unnecessary burdens on foreign companies.

In August 2018, the Ministry of Health and Family Welfare (MoHFW) released a draft set of amendments to the Drugs and Cosmetics Rules (1945), to regulate online pharmacies in India. Proposed Article 67.k(3) mandates that the e-pharmacy portal shall be established in India and that it shall keep the data generated localized. It further prohibits the transfer or storage of data generated or mirrored through the e-pharmacy portal outside of India. While a final version of the rules have not yet been released, if enacted, this policy would discriminate against foreign players by raising barriers to entry and operation, given that many foreign companies leverage global storage systems for optimizing service delivery by default.

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 could 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 "sensitive personal data" 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 disasters, 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 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 to handle law enforcement requests in a way that honors baseline principles of privacy, human rights, and due process. IA encourages 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 USTR 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 Opaque Application Of Competition Regulations

IA is 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. This is consistent with the practice of other agencies around the world, notably the European Commission and UK Competition and Markets Authority.

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 October 2018, the Reserve Bank of India (RBI) implemented a requirement for all foreign payment system providers to ensure that data related to electronic payments by Indian citizens are stored on servers located in India. The directive was issued under the Payment and Settlement Systems Act (2007) and implied that non-compliance could result in imprisonment and penalties including cancellation of the licenses. The requirement for local storage of all payment information is explicitly discriminatory as it raises costs for payment service suppliers and disadvantages foreign firms, which are more likely to be dependent on globally distributed data storage and information security systems. Furthermore, the notification came unannounced and companies had been given a short six-month window for compliance.

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 that 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, and 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 that 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. It is permitted only in the marketplace model, with the exception of food retail. The draft New Economic Policy (NEP) recommended that the limited inventory model be allowed for 100 percent made in India goods sold through platforms whose founder or 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 pushback on this 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 duties on electronic transmissions which goes against its current WTO obligations. Levying customs duties on electronic transmissions will hurt e-commerce companies by acting as a deterrent for buyers and sellers to transact on online platforms. It will also create barriers for India in the global e-commerce market, adversely impacting the country's economy. 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.[92]

[92] *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.aljazeer

Non-IP Intermediary Liability Restrictions

USTR correctly highlighted numerous problems with India's non-IP liability framework in the 2019 National Trade Estimate:

The absence of a safe harbor framework for Internet intermediaries discourages investment in Internet services that depend on user-generated content. India's 2011 Information Technology Rules have provided an insufficient shield for 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. Draft regulations announced in late 2018 (the "Information Technology (Intermediary Guidelines) Rules 2018"), threaten to further worsen India's intermediary liability protections. These draft rules would require platforms to become proactive arbiters of "unlawful" content, shifting the onus of the state to private parties. If these draft rules come into force, they will incentivize overly restrictive approaches to policing user-generated content, and will undermine many Internet-based platform services.

Safe harbors from intermediary liability power digital trade and enable a wide range of U.S. companies to access new markets. Where such safe harbors are incomplete or nonexistent, U.S. stakeholders in the digital sector – and small businesses that rely on consumer reviews or other user-generated content platforms to reach new customers – face significant barriers in accessing these markets.

Unfortunately, the publication of draft rules to amend India's intermediary guidelines include additional problematic requirements on issues such as the "traceability" of originators of content, local incorporation requiring certain intermediaries to establish a physical office in India, proactive filtering, and compressed timelines for content removal.[93]

Separately, on December 24, 2018, the IT ministry released draft changes to the Information Technology Act to impose more strict penalties for companies that fail to prohibit the spread of misinformation online. Platform "intermediaries" must trace the origins of information. This follows the IT ministry's attempt to amend Section 69A of the IT Act in 2018, which would enable the government to block apps and platforms that do not remove false information. On February 23, 2019, the Indian Draft National e-Commerce Policy was published with outlined proposals to change the country's rules for commerce online. The policy includes monitoring items listed for sale, and requires companies to remove prohibited items from sale no later than 24 hours after the item is flagged, block the seller, and notify relevant authorities. The draft also discusses content liability, stating that "it is important to emphasize on responsibility and liability of these platforms and social media to ensure genuineness of any information posted on their websites."

Finally, the Supreme Court of India recently directed the government to issue guidelines to address social media misuse.[94] The government has informed the Supreme Court that it is likely to complete the

a.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.").

[93] http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf
[94] https://www.livemint.com/news/india/sc-flags-tech-pitfalls-asks-centre-to-curb-social-media-misuse-1569350515906.html

process of notifying the new rules by Jan 15, 2020. In 2018, India's Home Ministry has already ordered Facebook, Google, and WhatsApp to appoint local grievance officers to establish content monitoring systems to ensure "removal of objectionable/malicious contents from public view." The Ministry reviewed actions taken to prevent misuse of the platforms to spread rumors, cause unrest, or incite cyber crimes or any activities going against national interest.

Infrastructure-Based Regulation Of Online Services

In March 2015, India's telecom regulator, Telecom Regulatory Authority of India (TRAI), issued a consultation paper on "Regulatory Framework for Over-the-Top services."[95] TRAI has recently recommended that there is no need to regulate OTT communication services. However, it is up to the government to accept or reject these recommendations. In 2016, there were additional consultation papers on issues including net neutrality,[96] VoIP,[97] and cloud service.[98] 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. TRAI's recent recommendations[99] proposing light touch regulation of cloud services is a worrying example of regulatory overreach. 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.[100]

Restrictions On U.S. Cloud Service Providers

TRAI released recommendations on a proposed Regulatory Framework for CSPs in September 2020, including a proposal for all CSPs to register with a government-controlled trade association. While TRAI's recommendations are currently non-binding, they will be sent to the Department of Telecommunications (DOT), who will decide whether to accept them as binding and on implementation. TRAI's recommendations include: (1) mandatory enrollment of all CSPs with a DOT-controlled industry body, failing which, telecom service providers will be disallowed from providing these CSPs with infrastructure services; (2) government oversight on the industry body, including the ability to issue directions, rules and standards, and to cancel registrations of "errant" CSPs; and (3) an exemption for channel partners and SaaS businesses, who may voluntarily enroll in these industry bodies. These proposals create an unnecessary barrier to trade by placing restrictions on CSPs' operations. In the medium-to-long term, they also pose a risk of "nationalizing" CSPs by granting them "critical infrastructure" status.

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

[95] 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.

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

[97] 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.

[98] 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.

[99] https://trai.gov.in/sites/default/files/PR_No.70of2020.pdf

[100] 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.

including 1) inability to buy dark fiber 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, 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 capital and operating costs incurred in offering cloud services in India.

Disaster Recovery

MeitY regulations require that CSPs who wish to be empaneled to bid for government contracts need to maintain data centers at least 100km apart. The Securities and Exchange Board of India (SEBI) has similar requirements (the request is for data centers to be at least 500 km apart). The Insurance Regulatory and Development Authority of India (IRDAI) and the Reserve Bank of India (RBI) do not appear to have any overriding policy statements, but are known to advise banks and insurance companies to follow a similar mandate. These pose significant burdens to U.S. companies' operations in India, especially for many U.S. CSPs who are unable to comply with these cumbersome requirements.

Cloud Empanelment Guidelines

Released in 2015, the Department of Electronics and Information Technology (DeitY; now known as MeitY), issued Cloud Computing Empanelment Guidelines for CSPs to be provisionally accredited as eligible CSPs for government procurement of cloud services. Within these Guidelines, Article 2.1(d) requires CSPs to store all data in India to qualify for this accreditation. This Article can be fulfilled by-default by Indian CSPs, whereas non-resident CSPs would have to modify their services to be eligible for consideration; hence creating a service barrier for U.S. CSPs.

Unilateral Or Discriminatory Digital Tax Measures

In March 2020, India adopted a 2 percent equalization levy, expanding on an earlier equalization levy that targeted digital advertising revenue earned by non-resident providers. The tax applies only to non-resident companies and covers online sales of goods and services to, or aimed at, persons in India. The tax applies only to companies with annual revenues in excess of approximately Rs. 20 million (approximately U.S. $267,000). Although the tax went into effect on April 1, 2020, many key details remain undefined. Earlier this year, IA joined a multi-association letter to USTR urging attention on the new expansion of India's Equalization Levy.[101] IA appreciates USTR including India in this Section 301 investigation as the digital industry believes that the Indian Equalization Levy is unreasonable and discriminates against U.S. companies by creating a targeted burden on all U.S. exports to India through the internet.

[101] https://internetassociation.org/files/ia_india-el-multiassociation-letter-ustr_march-2020_trade/

Indonesia

General

Indonesia's "Draft Communications & Informatics Ministerial Regulation on the Governance of Electronic Systems Providers for Private Scope" targets online services and would require platforms to take responsibility for a very broad list of content types, including content with no clear definition such as "creating public disturbances and disorder" to be removed with a very short turnaround time (i.e. certain content types must be removed within two hours from time of notice).[102] 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

While the government of Indonesia has introduced Government Regulation 71/2019 to revise the earlier GR 82/2012, forced data localization measures still remain. In the draft implementing regulations of GR 71/2019 (in the form of Communications & Informatics Ministerial Regulation on the Governance of Electronic Systems Providers for Private Scope), storing and processing of data offshore by any Electronic Systems Providers (ESPs) will require prior approval from the Minister. These measures reflect market access barriers, which require foreign services to undergo additional red tape when delivering product and services online.[103]

While Indonesia's GR71 provides greater visibility on its data localization policy[104] (i.e. only Public Scope Electronic System Providers are required to store and process data onshore), the ensuing implementing regulations (or the lack thereof) continue to be a significant barrier to digital trade, and is inhibiting foreign firms' participation in Indonesian e-commerce. Public Scope ESPs are defined to also include public administration which goes beyond national security and intelligence data. No further clarity has been made on the circumstances by which data can be stored and processed offshore in the case of Public Scope ESP including the guidelines that the Minister of Communications and Informatics will use when reviewing every individual data offshoring request by Private Scope ESPs. Indeed, U.S. firms have lost, and continue to lose, business in Indonesia from customers due to the ambiguity in the data localization requirements. GR71 was a step in the right direction towards reforming Indonesia's data localization policy and strengthening international trade, but the lower-level regulations are at risk of resurfacing significant market access barriers because of the incongruent approach with GR71 as the umbrella regulation. Further, data localization policy remains in place for banking and financial sectors despite the possibility of Private Scope ESPs to store and process data offshore based on GR71. Additionally, GR71 has mandated the advent of an interagency committee to set up and oversee the exception for Public Scope ESPs to store and process data offshore. However, the industry is concerned that there is limited progress in the finalization of the implementing regulations of GR71, creating tremendous business uncertainty and increased compliance risks. IA urges USTR to strongly encourage Indonesia to move swiftly in finalizing the implementing regulations of GR71 and for these regulations to prohibit data localization.

[102] https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/
[103] https://www.lexology.com/library/detail.aspx?g=9ae4aa21-dcb0-4c26-8e68-840f483873f6
[104] https://www.bakermckenzie.com/en/insight/publications/2019/10/new-regulation-electronic-system-and-transactions

Indonesia has also progressed towards passing the Personal Data Protection bill which presently differentiates the responsibilities between data controllers and data processors with major references from EU GDPR. Cross-border data transfer is currently limited to countries which have the same standard of data protection but there are no guidelines on assessing the data protection level across countries. The draft bill will also impose extraterritoriality as its cross-jurisdictional basis similar to EU GDPR. IA urges USTR to encourage Indonesia to remain consistent with its cross-border data flow principles in its personal data protection bill in order to promote international digital trade.

The government has also engaged in blocking activity including on May 22, 2019 when, in response to unrest in Jakarta, the government restricted access to social media platforms including Facebook, WhatsApp, and Instagram. The ban was lifted three days later.

Discriminatory Or Opaque 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 offerings. 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.

Indonesia's GR80/2019 on Electronic Commerce (followed by the Trade Minister Regulation No. 50/2020) requires any e-commerce provider passing a set of thresholds (i.e. more than 1000 transactions or more than 1000 delivery packages in one year) to set up or appoint a local trade representative to act on behalf of the foreign entity. The local trade representative office is then required to handle consumer protection, promotion of domestic products, and dispute resolution locally. This requirement effectively forces U.S. businesses to establish a local presence without a business need which also triggers unintentional tax consequences. To strengthen consumer protection, Indonesia should consider an option of having customer protection measures without forcing a local presence for digital products and services.

Disciplining Digital Platforms And Overly Restrictive Regulation of Online Services (OTT)

Indonesia's GR71/2019 and its ensuing implementing regulations by the Minister of Communications and Informatics will be the primary regulations for digital platforms. However, the government seems to have indicated further regulations on OTT as it relates to broadcasting services. The plan is gaining momentum amidst the judicial review of the Broadcasting Law and a subsequent plan to revise the Law with an outlook of subjecting OTT platforms under a new regulation. The regulation will ostensibly seek to create an equal playing field between OTT platforms and traditional platforms (e.g. broadcasting, telecommunications, media), but will likely impose additional requirements on foreign providers such as the need for foreign providers to submit to screening of content and provide law enforcement access as a condition for operating in the Indonesian market. The government has introduced a draft Ministerial Regulation in 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. Should this regulation be revived and passed into law, it would severely impact and even cripple the ability of many foreign digital suppliers to do business in Indonesia.[105] IA strongly recommends USTR urge the Indonesian government to cease efforts on this regulation, which would create a new precedent for imposing regulation on internet-based services and limit access for foreign providers.

Excessive Government Access On Cybersecurity

Indonesia has shown clear intention to pass two policies: Cybersecurity law and cybersecurity regulation. Both policies are driven by the new Cybersecurity and Crypto Agency, which is struggling to improve their competencies in order to understand how digital technology works. The Agency is heavily influenced by how China and Russia run their cybersecurity operations, which is inspiring Indonesian government to have direct access to private communications on the internet. In addition, the Cybersecurity law plans to impose a 50 percent local content requirement for cybersecurity equipment that is being used in Indonesia, and also additional licensing for public and private sector cybersecurity operators.

Duties On Electronic Transmissions

Indonesia has taken an unprecedented step to impose customs barriers and potentially duties on electronic transmissions. Indonesia 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 2019.

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.

[105] 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/.

Unilateral Or Discriminatory Digital Tax Measures

Indonesia has taken steps on taxation that significantly deviate from global norms, bilateral tax treaties, and WTO commitments. Earlier this year, Indonesia adopted an electronic transaction tax (ETT) that targets cross-border, digital transactions but implementing measures are still required to enable taxpayers to comply. The ETT applies to sales of goods and services over the internet by foreign companies to Indonesia consumers. This new tax law would require significant resources from online service providers, many of which are small companies that lack the necessary legal and technical resources to comply and could have significant tax consequences that conflict with OECD multilateral principles. Furthermore, this requirement would likely violate Indonesia's WTO commitments to allow computing and other digital services to be provided on a cross-border basis. IA believes that Indonesia's ETT is unreasonable and discriminates against U.S. companies by creating a targeted burden on all U.S. exports to Indonesia through the internet.

Jamaica

Divergence From Privacy Best Practices

IA encourages USTR to monitor developments on a data protection bill modeled on the GDPR. This bill is currently being discussed in Parliament.

Japan

Infrastructure-Based Regulation Of Online Services

The Ministry of Internal Affairs and Communications (MIC) has extended the Telecommunications Business Act (TBA) to apply extraterritorially to a wide range of intermediate online services that have not previously been within the scope of the TBA. Specifically, the extraterritorial application of the TBA would oblige foreign over-the-top (OTT) service providers (potentially including search, digital ads, and services that intermediate two-party communications, including email or message services) using third-party local facilities to 1) assign a local representative to notify and register as a service provider with MIC; and 2) based on this notification, to comply with a wide range of TBA obligations, including a "secrecy of communications" requirement (TBA Article 4), a "duty to inform suspension or abolishment of telecom services to users" (Article 26-4), and a "duty to report to MIC unexpected disruption of telecom services" (Article 28). The bill passed the Diet in June 2020, and is likely to be enforced by April 2021.

If these proposed TBA changes are interpreted broadly, the secrecy of communications provision, among others, would prohibit online service providers from using metadata and other content that is indispensable to the operation of different communications services. IA is concerned that such regulations are overly restrictive and likely to undermine innovation in a wide variety of online services. The extraterritorial application of the TBA without careful consideration and clearly articulated rationales will hamper innovation and the free flow of data.

The extraterritorial exercise of the TBA, particularly the planned revision to require a local representative, appears to be in violation of national treatment requirements under the General

Agreement on Trade in Services (GATS) as well as prohibitions on local presence requirements in other agreements. Given that the TBA would oblige a foreign service provider to have a local representative in Japan, a foreign company would be disadvantaged against a domestic firm and this would constitute differential treatment in violation of GATS Article XVII. This limitation on cross-border service provision is also inconsistent with free flow of data requirements that the U.S. and Japan recently agreed to in the U.S.-Japan Digital Trade agreement. MIC's current direction contradicts the agreed positions of both the U.S. and Japan, and is not a desirable path forward.

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 two 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.
- *Pooled rides restrictions:* Regulators have allowed only limited tests of a restricted pooled ride model where all persons who will be riding, and their drop-off locations, must be determined before the first person is picked up. In this pilot program, new requests for pick-up cannot be accepted in the middle of a trip.

Copyright-Related Barriers

Despite limited exceptions for search engines[106] and some data mining activities,[107] Japanese law today does not clearly provide for the full range of limitations and exceptions necessary for the digital

[106] 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").

[107] 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).

environment[108] – 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.

Divergence From Privacy Best Practices

On June 5, 2020, the amendment of Act on the Protection of Personal Information (APPI) passed the Diet. The amendments include extending the scope and enforcement methods of exterritorial applications, and obligation to report and notify data beaches. Enforcement of the majority of the provisions of the amended law and regulations will be enforced within the next two years (by June 2022).

Infrastructure-Based Regulation Of Online Services

Japan has established a new regulation on "platform-to-business" (P2B) relations that would require online intermediaries to meet aggressive transparency obligations concerning differentiated treatment, and access to data. These rules will be targeted to "specific digital platforms" that will be assigned by the Ministry of Economy, Trade and Industry (METI) under certain thresholds. The Japanese government says this new law will only target App Markets and Online Shopping Malls at the moment, but METI is able to assign other types of platforms like digital ads and search without changing the law.

The law is planned to be enforced by April 2021.

Jordan

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps 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 vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- → *License caps:* Each app provider may only have a maximum of 6,000 licensed drivers working on its platform. An overall industry cap is also set at 13,000. No market research or empirical evidence was produced to justify this cap.
- → *Vehicle ownership:* The driver must be either the owner of the vehicle or a relative up to a "second degree" of the owner.
- → *Licensing fees and exclusivity:* Drivers must obtain a license that costs up to $600 per year and that restricts the driver to working via one app provider only.

[108] 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.

→ *On-shoring requirements:* Technology companies seeking to operate in Jordan are required to have a significant local physical presence (staff).

Kenya

Burdensome Or Discriminatory Data Protection Regimes

Kenya's Data Protection Law was adopted in 2019. It establishes the Office of the Data Protection Commissioner, regulates the processing of personal data, establishes data subject rights, and regulates data protection offenses. The law refers to a "right to be forgotten" or "right to erasure." Hosting platforms already give users the ability to delete or erase information that the user has posted or uploaded to the platform. In those contexts, giving users a "right to erasure" with respect to content that they have uploaded would not meaningfully change the options that users already have. However, there is a risk that a "right to erasure" could be interpreted more broadly, creating significant operational burdens and legal uncertainty for small companies and startups in Kenya and elsewhere.

There are complex legal and operational issues regarding how to balance the interests of users and publishers, how to balance one user's privacy interests with another user's free expression and journalistic interests, and how to account for the broader public's right to know the truth and have access to accurate historical records. In many cases, individual content hosts and publishers are not well-placed to adjudicate conflicts between these rights.

This compliance obligation would drastically reduce the possibility for new platforms, search engines, and internet services – including local services – to enter the Kenyan market.

The law also provides for extra-territorial application of its provisions to data processors and controllers "not established or ordinarily resident in Kenya, but processing the personal data of subjects located in Kenya." This provision does not include a description of what actions bring a foreign business within its scope, including, for example, targeting the data subjects in the country.

A new ICT Policy was gazetted in August 2020, which includes a clause on "equity participation." The policy proposes an increase to 30% of the local ownership rules, which are currently set at 20 percent, although that requirement would not come into effect for 3 years. If these provisions were enacted, only firms with 30 percent "substantive Kenyan ownership" would be licensed to provide ICT services. This policy does not have a direct effect on the implementing bodies, namely the Kenyan Communications Authority and the (as yet unformed) Office of the Data Commissioner, but it does set a direction of travel for those agencies.

Separately, the ICT Policy also "requires that Kenyan data remains in Kenya, and that it is stored safely and in a manner that protects the privacy of citizens to the utmost." However, this provision runs counter to the 2019 Data Protection Act, which enables cross-border data transfers subject to conditions set out by the Data Commissioner. The Data Commissioner has still not been appointed almost a year after the Act was written into law, so the default position should not be for data localization in the current circumstances.

Copyright-Related Barriers

The East African Legislative Assembly passed the East African Community Electronic Transactions Act in 2015. While the Act provides for some level of protection of intermediaries from liability for third-party content, it fails to include any 'counter-notice' procedures for a third party to challenge content takedown requests, and it removes legal protections if the intermediary receives a financial benefit from the infringing activity. Lack of a counter-notice provision exposes internet intermediaries to business process disruptions through frivolous takedown notices.

Even more problematic, vague language about "financial benefits" can remove an entire class of commercially-focused intermediaries from the scope of liability protections, and can result in a general obligation on these intermediaries to monitor internet traffic, disadvantaging commercial services from entering numerous East African markets, including Kenya, Uganda, Tanzania, Burundi, Rwanda, and South Sudan.

The requirements in the Act diverge from prevailing international standards for intermediary liability frameworks, and serve as market access barriers for companies seeking to do business in these countries. IA urges USTR to engage with counterparts in Kenya and elsewhere to amend this provision on the grounds highlighted above, and develop intermediary liability protections that are consistent with U.S. standards and international norms.

Data Flow Restrictions And Service Blockages

The 2020 National ICT Policy Guidelines require that Kenyan data collected by the government for the purpose of providing public services "remains in Kenya."[109] The Data Protection Act,[110] which was passed in 2019, gives the government some residual power to mandate that certain types of data shall be processed through "a server or data centre located in Kenya" and requires that before data may be transferred outside of Kenya the Data Commissioner is provided with proof of the security of the data. Data localization without careful consideration of how and what types of data are processed restricts cross-border data flows and undermines product design, user experience, and the local industry's access to global infrastructure while not materially improving privacy or security.

Infrastructure-Based Regulation Of Online Services

The ICT regulator plans to conduct a study on how to treat "over-the-top technologies and services (OTTs)."[111] IA encourages USTR to monitor the development of this plan and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach.

Unilateral Or Discriminatory Digital Tax Measures

In April 2020, a rushed COVID-19 tax relief law was passed with a clause for 20 percent withholding tax charged on 'marketing, sales promotion and advertising services' provided by non-resident persons.

[109] https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf
[110] Data Protection Act. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019
[111] Lilian Ochieng, *Kenya Plans ICT Sector Reforms to Regulate Internet Firms*, Daily Nation (Mar. 17, 2016), http://www.nation.co.ke/business/Kenya-plans-new-bill-to-reign-in-on-rider-tech-firms/996-3121342-ayu7lsz/index.html.

This was followed by a 1.5 percent digital services tax law for both resident and non-resident entities in July 2020, which is scheduled to come into effect in January 2021. At the same time, the Ministry of Finance is preparing regulations on VAT (14 percent) on "digital marketplace services" for both non-resident and resident providers. Kenya's unilateral corporate tax proposals create concerns not only around targeting

and discriminating against ICT services, but also around the legitimacy of an international tax system that has been built around multilateral coordination.

Non-IP Intermediary Liability Restrictions

While the Copyright Act has introduced a form of protection for online service providers from liability for third-party content that violates copyright, it provides a 48-hour mandatory take-down period for such content, rather than removal 'within a reasonable time' in consideration of the need to review the removal requests in a duration that would be commercially reasonable in the circumstances of each case.

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. There is a broader, worrying trend of South Korean regulators requiring local presence as a condition to operate in the cross-border services space, which may be inconsistent with Korea's commitments in the Free Trade Agreement.

Copyright-Related Barriers

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

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, there is pending legislation that may be interpreted to 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 three percent fine based on revenue.

Discriminatory Or Opaque 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 often 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. In addition, on March 8, 2019, the Korea Communications Commission announced its key plans for 2019 which included drawing up "Network Use Guidelines" which would "require overseas operators designate a domestic representative, pursue introducing a system that would temporarily suspend services in case of violations." Civil society organizations argued that the measure is aimed at controlling internet services providers as well as online users. The guidelines give Korea the authority to shut down domestic operations of foreign internet-related companies that hold personal information of South Korean users, such as Google and Facebook. Previously, foreign companies were not subject to domestic regulations regarding violations of user privacy or misuse of user information, which Koreans stated gave foreign companies an advantage.

In May 2020, the Korean National Assembly passed amendments to the Telecommunications Business Act (TBA), forming the legal basis for allowing Korean telcos to charge online platforms for utilizing the network by requiring "value-added telecommunications service providers"(VTSP) to ensure that "users are provided with convenient and stable telecommunication services regardless of the device used." The related presidential decree is nicknamed the "Netflix Law" and was designed specifically to bring certain U.S. tech companies within its scope through arbitrary thresholds.[112] These provisions would alter the conditions of competition by imposing burdensome and costly requirements that are incongruent with Korea's obligations in the Korea-US FTA and WTO, including national treatment, MFN, local presence, domestic regulation, and telecommunications access and use. Some of the measures that would impede a U.S. company's ability to supply their services on a cross-border basis include the requirement to disclose trade secrets through an annual report, requirements to consult with internet service providers (ISP) on network design decisions that are both commercially sensitive and should be allowed to be made independent of the ISP, the high financial and legal risk created by shifting the burden of service reliability on VTSPs despite their lack of control, and other conditions that U.S. suppliers could not reasonably meet without establishing a local presence. The proposed measures do not appear to propose the least trade-restrictive way to achieve the intended purpose of the law and ignore a technical reality that despite best efforts from all parties involved, it is impossible to achieve 100 percent stable and continuous service.[113]

[112] MSIT's supplementary materials demonstrate that they decided on 1-percent web traffic and 1 million users (despite ISPs' recommendation of .35%) to "minimize the number of operators subject to the Act" but to "cover foreign as well as domestic operators" so as to not appear to be discriminatory despite their original intent.
[113] MSIT's explanatory notes define the concept of "convenient and stable service" as "the service provided by the value-added telecommunications service provider according to the contract with the user that is 1) normal without errors and 2) continuously available without interruption."

Restrictions On Cloud Service Providers

The Korean government continues to maintain a protectionist stance to keep global CSPs out of the Public Sector market through the KISA CSAP, which is a requirement that applies to all administrative and public institutions, including central government, municipalities, affiliated public institutions and all education institutions. The CSAP includes four technical requirements that have prevented all global CSPs from being able to obtain the CSAP: (1) physical separation; (2) Common Criteria (CC) certification; (3) vulnerability testing; and (4) use of domestic encryption algorithms. Through these onerous requirements, which are not based on international standards, the CSAP blocker effectively casts technical blockers to trade and prohibits global CSPs from accessing public-sector workloads in Korea. The government has also begun requiring CSAP in other sectors, such as in healthcare, with the Ministry of Health and Welfare (MOHW)'s recent inclusion of the CSAP as a requirement for Electronic Medical Record (EMR) system providers who seek to use public cloud services. While MOHW claims that the CSAP is not mandatory, it plans to provide medical insurance reimbursement premiums only to medical institutions with certified EMR systems, thus creating an unlevel playing field for companies who are unable to obtain the CSAP.

Networking Charges

Local Internet Service Providers (ISPs) primarily provide connectivity between data centers owned by U.S. CSPs and Korean customers. In 2016, the Korean Ministry of Science and ICT (MSIT) issued Guidelines on Internet Interconnection (the Notification). The Notification stipulated that a preset rate should be charged for all internet traffic exchanged between the three major ISPs. Though the Notification was intended to set up only a price cap, in practice all three ISPs increased their rates to the highest allowed level. While it is expected globally to decline 25-40 percent annually, the unit cost of internet bandwidth is increasing year over year in Korea. The MSIT revises the Notification by lowering the set price cap for data interconnection that would be aligned with global/regional price ranges and imposes an obligation on the three major carriers to apply volume based discounts on such price cap; The KCC establishes guidelines which set out competition rules for carriers with market power and requires them to offer fair and cost-based access and interconnection prices to other market players.

Mexico

Customs Barriers To Growth In E-Commerce

A deep concern is Mexico's June 30 amendments to its Reglas Generales de Comercio Exterior in light of Mexico's obligations in Articles 7.8 (1)(f)(ii) and 7.8 (2) of Chapter 7 of USMCA. Rather than implement these articles to create a new-duty free threshold up to $117 and a meaningful informal clearance threshold up to$2,500, Mexico instead raised its "Tasa Global" import duties one percentage point on all USMCA low-value shipments between $50-$117 and by 3 percentage points for USMCA partners above $117 and up to $1000. These amendments violate the letter and the spirit of USMCA by raising import duties on U.S. and Canadian shipments and further complicate customs clearance operations.

These changes were made with little to no consultation with USMCA partners and left the private sector scrambling to comply with the new requirements overnight to the detriment of consumers, including many SMEs across North America.

Filtering, Censorship, And Service-Blocking

A bill on cybersecurity establishes certain broad monitoring obligations for ISPs in order to "discover" possible online crimes and stop that content's transmission (without judicial or administrative order). Further, a broad felony is set forth to criminalize online platforms as intermediaries due to the uploading of illegal content.

Restrictions On Cloud Service Providers

Mexican financial sector regulators, National Banking and Securities Commission (CNBV), and the Central Bank of Mexico (Banco de México), have issued Draft Provisions Applicable to Electronic Payment Fund Institutions (IFPEs). The particular articles of concern in the draft regulation are Articles 50 and 49. Article 50 would impose the obligation of data residency and multi-scheme providers to E-Payment Institutions (IFPEs) that use cloud computing services. Article 49 would establish an authorization model with a high degree of discretion and lack of transparency for the use of cloud computing services. These draft requirements to localize data run counter to the spirit, if not the letter, of USMCA's landmark digital and financial services provisions. These draft regulations undermine U.S. financial services providers, which already face lengthy and uncertain approval processes from CNBV or Banco de Mexico in order to use secure U.S.-based cloud computing services. Additionally, the regulation could negatively affect the adoption of cloud computing in the country and create an uneven playing-field, where U.S. cloud computing companies would be at a disadvantage with respect to local data center companies.

Most notably, Article 50 of the draft regulation imposes on the IFPEs that use cloud services the obligation of data residency, or alternatively, a multi-provider scheme, once they reach certain transaction thresholds. This proposed Article requires IFPEs that use cloud services to have a secondary infrastructure provider, once they reach certain transaction thresholds. Either this provider shall have an in-country infrastructure, or its controlling company must be subject to a different jurisdiction than that of the first cloud provider. A similar data localization requirement is being imposed on financial service providers that have requested to participate in Mexico's national payments system (SPEI), regulated and operated by the Central Bank. Overall, there is information that Mexico's financial sector regulators, most notably the Central Bank, have been requiring financial service providers to have data residing in Mexico, and introducing regulatory biases against cloud computing. In addition to Article 50, the provisions proposed in Article 49 establish an authorization model with a high degree of discretion and an absence of clear approval processes.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps 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 vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- *License cap:* Certain states (e.g. Colima, Querétaro, and Guanajuato) limit the number of vehicles that can work with app-based transportation services.
- *Cash payment prohibition:* Drivers working with app-based transportation services are prohibited from accepting cash payments in several states (Mexico City, Puebla, Querétaro, Yucatán, Sonora, San Luis Potosí, Coahuila, Colima, Aguascalientes, and Tijuana-Baja California).
- *Vehicle requirements:* Depending on the state, vehicles providing app-based transportation services must not be more than 4-7 years old.
- *Vehicle identification:* Some cities and states require vehicles providing app-based transportation services to have visible external identification, increasing the risk of physical violence and intimidation by the incumbent taxi industry.
- *Data-sharing requirements:* Companies providing transportation apps are increasingly receiving requests for data sharing and some of them, as in Mexico City, require them to share specific trip data beyond any reasonable safety or public policy purpose, compromising privacy and even the security of users. The amount of information required poses a disproportionate cost and raises competitive concerns, given that city authorities currently operate an app-based system for hailing government concession taxi services.

Unbalanced Copyright Framework

With the USMCA, Mexico is now developing a comprehensive ISP safe harbor framework covering the full range of service providers and functions and prohibiting the imposition of monitoring duties.

In June 2020, a copyright reform was approved for the correct implementation of the USMCA, which entered into force on July 1. It successfully implemented a Notice & Takedown model based on DMCA, including a Safe-Harbour provision for platforms. Nevertheless, the approved bill sets forth a fine if platforms do not remove content upon receiving a valid notice.

At present, an unconstitutional legal action was filed before the Supreme Court against the amendments, as well as several bills that aim to modify approved wordings. A Private Copy Levy bill is being discussed in the House of Representatives, that will impose a tax for the manufacturing or importation of devices that can potentially store copyrighted material. The bill is being proposed and widely supported by collective societies.

Bills & Regulatory Processes In Discussion With High Potential To Be Approved:

- On September 8, the Secretary of Finance & Public Credit, Arturo Herrera, presented to the Mexican Congress the legislative project for the Government's Budget for 2021. Included in the proposal is the implementation of a "kill switch," which is an enforcement mechanism that the Mexican government initially proposed in their 2020 Budget against non-resident entities that do not comply with the application of the VAT on non-resident supplies of digital services to Mexican consumers. While the government ultimately removed the measure from last year's budget proposal, the fact that a limited number of companies registered in the government's regime (35 companies in Mexico, compared to more than 100 in Chile in the same timeframe,

due to Mexico's incredibly complex registration process) has led them to reintroduce the measure as way to force compliance. Should the regime be approved, it would empower the tax authority to work with the telecom regulator to require Internet Service Providers (ISPs) to block internet access to non-resident entities making cross-border supplies. Unilateral measures such as the Mexican proposal threaten the progress of multilateral, collaborative work that considers all aspects of the changing global economy.

- → Increase of costs of spectrum usage: The same Fiscal Bill 2021 includes a proposal to increase the costs to invest in spectrum in Mexico, that could substantially increase the costs of internet access to end-users.
- → In September of 2020, Senator Ricardo Monreal presented a legislative project that seeks to reform the Federal Telecommunications Act and require a 30 percent local content quota for Over-the-Top (OTT) platforms operating in Mexico. A local content quota for OTT platforms would violate Mexico's commitments under USMCA (Articles 14.10 and 19.4.1), as well as limit free expression and consumer choice, distort the growing audiovisual market, and stifle investment and competitiveness. If this policy were enacted and services failed to launch, Mexican audiences and creators would have fewer legitimate options for film and television content. The draft bill would also expand the Federal Telecommunications Institute (IFT) licensing requirement for restricted TV and audio services to cover OTT services – even those operating from abroad. Imposing such onerous new licensing requirements on OTT services would be inconsistent with USMCA Article 18.14.1 on applying requirements of public telecommunications to value-added services which are not public telecom services.
- → Net Neutrality: Telco Regulator could issue pending regulations in early 2021. These regulations could shift Internet consumption, as the draft proposal does not consider clear wording on how carriers promote their commercial offer, which could consolidate discriminatory practices against similar services on zero-rating and bundled services. The draft is also considering wording to increase the Telco Regulator capabilities to order ISPs to block traffic, which violates USMCA provision to promote free data flows while hindering freedom of speech.

Unilateral Or Discriminatory Digital Tax Measures

Although a DST discussion is still pending and mainly waiting for the OECD BEPs pillar discussion to finish, the implementation of the tax amendments (VAT and Income Tax retention) for digital services on June 1 was bumpy, and companies faced difficulties in registering with the Tax Authority.

New Zealand

Copyright-Related Barriers

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.

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.

Unilateral Or Discriminatory Digital Tax Measures

The New Zealand government is considering the introduction of a DST modelled on the UK Government's approach, potentially applying to both large online marketplaces and online advertising businesses irrespective of where the business is established. While the Government has stated its preference for a multilateral solution, they are nevertheless continuing to consider the design of a unilateral measure. The New Zealand proposal would potentially be a WTO violation, and could also be considered a 'covered tax' within the meaning of certain New Zealand double tax agreements (DTAs), including the DTA with the U.S. The New Zealand government should refocus its efforts on reaching consensus with other leading economies within the OECD on any new digital taxation models so as to guarantee fairness and avoid discrimination and double taxation.

Nigeria

Copyright-Related Barriers

Nigeria continues work on reforming its copyright laws. IA encourages USTR to be supportive of the development of a framework that is consistent with international best practices, including through the implementation of fair use provisions and safe harbors from intermediary liability. The absence of these provisions would create market access barriers in a key African market for U.S. companies.

The Code prevents Pay TV and other broadcasting/streaming platforms from making their content exclusive and directs them to sub-license content at prices the Commission will regulate. This would create an unfavorable environment for such platforms as it reduces their value to their subscribers with

a potential plunge in revenue. The Code takes away the liberty rights holders have to use and license their content as they deem fit. This appears to go against intellectual property rights.

Broadcasting Code

The Minister of Information, Alhaji Lai Mohammed working with the Director General of the NBC, recently made some amendments to the 6th edition of the National Broadcasting Code. The Code gives the minimum standards required in the broadcast industry, and is framed within the intent of increasing local content while increasing advertising revenue for local broadcast stations and content producers. Assuming without conceding that the Code was validly issued, there are also concerns around the far-reaching effect of the Code given that several provisions of the Code conflict with the Copyright Act and the powers of the FCCPC under the FCCPA to regulate competition.

Data Flow Restrictions And Service Blockages

The Data Protection Bill, which looks to create a Data Protection Commission, seeks to regulate the collection, storage and use of personal data of data subjects in Nigeria. It requires that personal data be processed lawfully based on a legal basis. The Bill applies to entities in the private and public sector as well as data controllers and processors operating within and outside the country. It extends its applicability to personal and biometric data of data subjects; personal banking and accounting records; academic transcripts; medical and health records; telephone calls; and messages, among other things. The application of the Bill exempts from its scope the processing of personal data by a data subject while carrying out purely personal or household activities.

While this current draft version has moved well beyond data localisation as well as requiring adequacy for international transfers, there remain concerns over provisions that give life to its extraterritorial application, which is often difficult to manage/litigate, and gives rise to ambiguities in the operations of data controllers/processors. Another concern is on the identification of a DPO – appointments should focus on the DPO as an "office" and not as a specific "individual."

Pakistan

Restrictions On Cloud Service Providers

In October 2019, Pakistan's cabinet approved an E-commerce Policy Framework.[114] The Framework states that "Consumer/Business Payments from Pakistani banks and payment gateways to unauthorized and unregistered (GST non-compliant) websites/applications will be barred." This would appear to prohibit payments to U.S. businesses unless they are registered with provincial tax authorities. IA encourages USTR to monitor the implementation of this policy and to promote a light-touch framework for regulating online services that is consistent with the U.S. approach, and that encourages innovation and investment.

[114]http://www.commerce.gov.pk/wp-content/uploads/2019/07/Final-Draft-E-Commerce-Policy-Framework-of-Pakistan.pdf11/e-Commerce_Policy_of_Pakistan_Print.pdf

Unilateral Or Discriminatory Digital Tax Measures

In May 2018, Pakistan's National Assembly passed its Finance Bill 2018 under its domestic tax law and created a new five percent withholding category for "fees for offshore digital services" on a gross basis, which leads to adverse tax rules for non residents. This law, effective as of July 1, 2018, is a significant deviation from international tax agreements. The law requires companies to approach the authorities each time they wish to apply treaty law, and thus serves as a de facto unilateral measure.

Non-IP intermediary Liability Restrictions

In February 2020, the Ministry of Information Technology and Telecommunication (MOITT) posted on its website the Citizens Protection (Against Online Harm) Rules.[115] The Rules contain onerous requirements including forced local office presence; forced storing of user data within Pakistan; and new procedures that would contravene both Pakistani and international laws and norms around disclosure of user data and intermediary moderation of online content. The government announced in March that a committee led by the Pakistan Telecommunication Authority would conduct an "extensive and broad based consultation process with all relevant segments of civil society and technology companies." However, a revised version of the Rules has not been circulated, and a broad-based consultation has not yet occured.

In May 2020, the Ministry of Information Technology and Telecommunication (MOITT) released a draft Data Protection Bill[116] which contains provisions on data localization (including an undefined "critical personal data" category), a powerful regulator in a newly established data protection authority, extraterritorial application, and criminal liability.

Panama

Burdensome Or Discriminatory Data Protection Regimes

In March 2019, Panama enacted Law No. 81 on Protection of Personal Data. This law does not recognize appropriate types of consent as a basis for transferring data outside the country. Any international transfer provision should permit transfers with the consent of the data subject, and the nature of that consent (e.g., whether it is express or implied, and the mechanism used to obtain it) should be based on the context of the interaction between the controller and the individual and the sensitivity of the data at issue. The required consent for transfers should not be burdensome, and should allow for the use of technology-neutral consent approaches. In addition, consent should be implied for common use practices, such as transferring data to cloud computing service providers located abroad. IA encourages USTR to engage with counterparts in Panama to develop interoperable data protection frameworks that clearly allow for the forms of consent described above.

In addition, Article 2 of the Data Protection bill mentions that databases containing "critical State data shall be kept in Panama." The definition of critical State data set forth in Article 3, however, is very broad. This could create a de facto data localization mandate for all data, even if this is not the objective

[115] https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2c%202020.pdf
[116] https://moitt.gov.pk/TopStoryDetail

of the law. The U.S. government should work with Panama to ensure that this language does not result in a data localization requirement.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps 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 vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- *Fleet restrictions:* No individual may own more than two vehicles that are used to provide app-based transportation services. Companies are not allowed to own fleets, a restriction that does not apply to the taxi industry or to other modes of transportation.
- *Vehicle requirements:* Vehicles providing app-based transportation must be less than seven years old. This requirement does not apply to any other type of transportation.

Peru

Copyright-Related Barriers

Peru does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Peruvian law currently includes a long but inflexible list of rules that does not clearly provide for open limitations and exceptions that are necessary for the digital environment[117] – for example, flexible limitations and exceptions that would enable text and data mining, machine learning, and indexing of content. To accomplish this objective, Peru should also remove the provision in Legislative Decree 822 of 1996 stating that limitations and exceptions "shall be interpreted restrictively" – which has limited the ability of Peruvian copyright law to evolve and respond flexibly to new innovations and new uses of works in the digital environment.[118]

In addition, Peru is out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement that require copyright safe harbors for internet service providers.[119] IA urges USTR to address this significant market access barrier for U.S. services and push for full implementation of the agreement.

In May 2020, the Digital Government Secretariat of Peru released for consultation a draft of Emergency Decree 007 - Digital Trust Framework regulations. The proposal appears to create unnecessary trade barriers for U.S. and other foreign service providers by giving preferential treatment to domestic data storage and domestic service providers. Peru's proposal includes:

- The creation of a whitelist, which will include the permitted countries for cross-border transfer of data, even though the Peruvian Data Protection Law does not include such restrictions. The

[117] Legislative Decree No. 822 of April 23, 1996, Title IV Chapter 1.

[118] Legislative Decree No. 822 of April 23, 1996, Title IV Chapter 1, Art. 50.

[119] https://ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file437_9548.pdf

proposal creates barriers for service´s trade and obstacles to product development and innovation by giving clearly preferential treatment to domestic data storage.

- → The issuance of digital security quality badges for private companies, which will be the governmental cybersecurity certification ignoring the existence of global security standards.
- → The creation of a national data center intended to host the information provided by the public sector entities.

The proposal also includes broad definitions of digital service providers that do not consider key differences among digital service providers, such as Cloud Services Providers, that do not have access to nor intervention in their client's information, and organizations that use digital channels to provide their services. The Data Protection Authority would determine model contract clauses, which appear to exceed what is currently required under the Data Protection Law. The national data center would incentivize domestic data storage by providing infrastructure to domestic data center operations, where the state would have total control over data. The ability to move data and access information across borders is essential for businesses regardless of size or sector. Data localization measures serve as barriers to trade and offer governments a false choice between achieving regulatory objectives, such as data privacy and security, and data movement. Instead of going down this path of data localization, Peru should rely the already approved Guidelines for the Use of Cloud Services for entities of the Public Administration, and endorse the use of international standards and best practices, which are accepted and adopted, such as ISO 9001, ISO 27001, ISO 27002, ISO 27017, ISO 27018 y SOC 1, 2 y3.

Philippines

Non-IP Intermediary Liability Restrictions

In the Philippines, the national legislature is currently proposing to regulate all internet transactions through the proposed Internet Transactions Bills (House Bill 6122 and Senate Bill 1591). The proposal seeks to introduce a new policy framework that intends to regulate non-resident online platforms and merchants, creates obligations and undertakings for platform providers, shifts the burden of policing online merchants to platform providers, and requires substantial changes in the business model, product design, and function of platforms to enable compliance with the requirements of the bills. Noteworthy is the mandatory registration and incorporation requirement for all online platforms and merchants that sell to Philippine customers, which in effect mandates setting up a permanent establishment in the country.

Qatar

Restrictions On Cloud Service Providers

The Modern Technology and E-Banking Services Risk circular, issued by the Qatari Central Bank in 2012, provides non-binding, but persuasive, advice for banks that utilize cloud computing services. Outlined in section 3.6.3, banks must ensure that "core sensitive information is not placed on a non-controlled cloud computing environment" when core sensitive information is understood to include customer records and account information. Banks are permitted to store core sensitive information in private

cloud facilities when such cloud facilities remain under the local control of the bank. This communicates an institutional preference for private cloud to the detriment of public cloud services. The content of the circular that is nearly a decade old might need to be updated to give further clarity on what is permitted, as some Qatari banks have already chosen to adopt the Cloud.

Russia

Data Flow Restrictions And Service Blockages

Russia has passed a series of localization requirements that amount to market access barriers for U.S. services seeking access to the Russian market, including:

- → Article 18 of Federal Law 242-FZ: requirement to store and process personal data concerning Russian citizens in Russian data centers. According to the current regulatory interpretation of this rule, the initial collection, processing, and storage of data must occur exclusively in Russia. Once this "primary processing" on local servers has occurred, data can be exported outside Russia subject to consent. Given the requirement to localize processing, a global web service would typically be compelled to re-architect its global systems and networks in order to comply with such a provision.
- → Articles 10.1 and 10.2 of Federal Law No. 149-FZ: requirement to retain metadata for provision to Russian security agencies, and content-posting restrictions for websites.
- → "Yarovaya Amendments" amending Federal Laws 126-FZ and 149-FZ: requires "organizers of information distribution on the internet" to store the content of communications locally for six months, with longer metadata storage requirements for different types of providers. In addition, this package of laws requires internet services to provide government officials with sensitive user information and to assist national security agencies in decrypting any encrypted user messages.
- → "News Aggregators Law": According to the recently adopted amendments to the Federal Law 149-FZ, news search and aggregation services that exceed 1 million daily visitors and are offered in the Russian language with the possibility of showing ads must be offered through a local subsidiary in Russia. Foreign providers are not permitted to offer such services directly across the border, even though they are allowed to own the local company that offers them. The law additionally provides for significant content restrictions.

In 2016, the Russian internet regulator appealed to a court to block LinkedIn over alleged non-compliance with the Russian data localization requirements. The court of first instance ruled that LinkedIn must be blocked in Russia entirely until the company is in compliance with these requirements. LinkedIn has appealed this order but remains blocked.

Filtering, Censorship, and Service-Blocking

Since 2012, Russia has been implementing a Blacklist law initially aimed at protecting children from harmful information online. The Blacklist law keeps getting expanded onto new types and categories of content including extremist, suicide-inciting, drugs-promoting, etc. By this law, intermediaries are

envisioned to block certain sites or certain types of content.[120] For example, Russia has ordered all of Wikipedia to be blocked due to problematic content on a single page.

On March 18, 2019, Putin signed laws No.30-FZ and No. 31-FZ which prohibit spreading misinformation online and prohibits on-line insults of government officials. The laws target online information that presents "clear disrespect for society, government, state symbols, the constitution and government institutions." Russian authorities can block websites that do not remove information that the state assesses is not accurate, and the law allows prosecutors to direct complaints to the government about material considered insulting to Russian officials, which can then block websites publishing the information.

On May 1, 2019, Putin signed a new law into effect titled the Internet Sovereignty Bill. The bill was introduced in February 2019, with the intention of routing Russian web traffic and data through points controlled by state authorities and building a national Domain Name System and providing the installation of network equipment that would be able to identify the source of web traffic and block banned content. The law took effect November 1, 2019.

In December 2019, Russia adopted a law requiring the pre-installation of Russian software on certain consumer electronic products sold in Russia. The Russian government has not yet identified neither the types of electronic products which should have Russian software nor specific applications that will be required for pre-installation. However, there is an understanding that the scope of devices covered will likely include smartphones, computers, tablets, and smart TVs and applications which will be covered are likely search engines, mapping and navigation software, anti-virus software, software that provides access to e-government infrastructure, instant messaging and social network software, and national payment software. The law is due to take force in January 2021.

Saudi Arabia

Customs Barriers To Growth In E-Commerce

In Saudi Arabia, a new product compliance regulation (IECEE certification – International Electrotechnical Commission for Electrotechnical Equipment) was enforced at all borders in 2018 by the Saudi Standards, Metrology and Quality Organization (SASO). It requires importers to register, upload several technical documents from foreign manufacturers (test reports, manufacturer certifications, translations, etc.) into an online portal, obtain prior authorization, submit several types of government and external lab company fees, and provide authorities with legal declarations. The regulation imposes an additional set of permits from the Saudi Telecom regulator (CITC) for specific product categories such as wireless electronic devices. All these measures constitute restrictions imposed to importers further complicating the ability to grow and thrive in the Saudi market. KSA also requires the provision of several sets of original signed and stamped international shipping and customs documents. Whereas in most "developed'' countries customs formalities are completed with commercial invoice copies only, Saudi Arabia still imposes importers to provide original copies from origin shippers signed, stamped, and legalized by origin Chamber of Commerce offices. Failure to do so results in fines and shipment delays at borders.

[120] *See New Russian Anti-Piracy Law Could Block Sites "Forever,"* Torrent Freak (Apr. 25, 2015), https://torrentfreak.com/new-russian-anti-piracy-law-could-block-sites-forever-150425/.

Data Flow Restrictions And Service Blockages

Saudi Arabia's Communications and Information Technology Council issued a Public Consultation Document on the Proposed Regulation for Cloud Computing, which contains a provision on data localization that may have the effect of restricting access to the Saudi market for foreign internet services. This regulation would also increase ISP liability, create burdensome new data protection and classification obligations, and require compliance with cybersecurity and law enforcement access provisions that are significantly out of step with global norms and security standards. For example, under this regulation, CITC would be granted broad powers to require cloud and ICT service providers to install and maintain governmental filtering software on their networks. These and other cloud regulations would also prohibit the cross-border transfer of certain classes of data.

The National Cybersecurity Authority (NCA) 2018 Essential Cybersecurity Controls (ECC) framework states that data hosting and storage when using cloud computing services must be inside KSA. Similarly, the draft NCA 2020 Cloud Cybersecurity Controls (CCC) framework requires operators to provide cloud computing services from within KSA, including all systems including storage, processing, monitoring, support, and disaster recovery centers. The requirement applies to all levels of data. Neither the ECC, nor the draft CCC, distinguish between data localization requirements for different levels of data classification, which is not in line with the 2018 Cloud Computing Regulatory Framework (CCRF). The CCRF allowed for lower sensitivity levels of data to be hosted outside of KSA, including: non-sensitive public authority data, sensitive private sector data where no sector-specific regulations apply, or "Content qualifying for Level 1 or Level 3 treatment, for which the Cloud Customer elects Level 2 treatment."

The ECC and draft CCC should only apply to government organizations (including ministries, authorities, establishments and others), its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs). However, the NCA has expanded the scope of their ECC enforcement powers by applying this localization mandate to companies that are neither government-owned or CNIs. This move could adversely affect the operations of U.S. and Saudi companies that use global cloud infrastructure to serve their customers in KSA, as it would force them to transition to domestic cloud service providers, who may not meet the same standards, pricing or service parity.

Restrictions On Cloud Service Providers

Saudi Arabia's Communications and Information Technology Council has issued a Cloud Computing Framework, which restricts access to the Saudi market for foreign cloud services. This regulation, which went into effect on March, 8 2018, requires that any cloud computing service provided to customers having a residence or address in Saudi Arabia: 1) register with the Communications and Information Technology Commission ("CITC"); 2) inform customers of any security breach or information leakage; 3) allow content to be filtered by the CITC; 4) comply with certain information security requirements; 5) comply with customer data protections; and, 6) disclose the location of their data centers and where their customer content will be transferred.

This regulation also creates new data protection and data classification obligations that apply to cloud services. Sensitive data classified at levels 3 or 4 require local storage. What specific types of data fall

into these categories is not explicitly defined in the framework, leaving it within the discretion of the regulator for the financial vertical (the Saudi Arabian Monetary Authority) to classify financial data as sensitive, requiring localization. It is important to note that the regulator has not yet issued any rules on data classification but could easily do so.

SAMA's Cyber Security Framework, which predates issuance of the cloud regulatory framework, also requires that "in principle only cloud services should be used that are located in Saudi Arabia," or foreign located services only with an "explicit approval" from SAMA.

Senegal

Infrastructure-Based Regulation Of Online Services

Senegalese regulators have conducted a study to help decide whether and how to regulate online services.[121] IA encourages USTR to monitor this study and to promote a light-touch framework for regulating information services that promotes market access for foreign services.

Singapore

Non-IP Intermediary Liability Restrictions

On Oct 2, 2019, Singapore's Protection from Online Falsehoods and Manipulation Bill (Bill No. 10/2019), as a measure to curb misinformation, came into force. The law would allow any Minister to instruct a competent authority to issue orders to take corrective action, and require online media platforms to carry corrections, on the grounds that (i) the statement is a false statement of fact and (ii) if a correction is in the public interest. The law requires media outlets to correct false news and to "show corrections or display warnings about online falsehoods so that readers or viewers can see all sides and make up their own mind about the matter." Internet intermediaries are required to either take down the content, or show corrections about the falsehoods on their platforms. The legislation was hastened after the Law Ministry stated that Facebook declined to take down a post that the government had declared was false.

South Africa

Duties On Electronic Transmissions

South Africa is currently working against the continuation of the World Trade Organization (WTO) Moratorium on Customs Duties on Electronic Transmissions, a commitment that South Africa reaffirmed as recently as December 2017. Imposing customs requirements on purely digital transactions will impose significant and unnecessary compliance burdens on nearly every enterprise, including many SMEs. South Africa's actions continue a dangerous precedent, and will likely have the effect of encouraging other countries to violate the WTO Moratorium.

[121] *See* Myles Freedman, *Senegal: ARTP Studies the Impact of VOIP Applications on Operators*, EXTENSIA (Jan. 5, 2016), http://extensia-ltd.com/tunisia-4g-license-has-been-set-at-77-million/.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps 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 vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- → *Demand demonstration requirement:* The Western Cape provincial government requires drivers and/or app providers to prove evidence of demand for their services before issuing additional licenses to drivers.
- → *Lengthy licensing process:* A licensing process that is supposed to take two months can take more than six months. Cities are also imposing moratoria on the issuance of licenses, making it even more difficult for drivers to become licensed.
- → *Lack of equal protection under the law:* Drivers who provide transportation via app-based services have been victims of targeted violence by taxi services. Law enforcement agencies are slow to intervene, directly threatening both the physical safety and economic wellbeing of those using app-based services.
- → *Vehicle identification:* The National Land Transport Amendment Bill requires vehicles providing app-based transportation services to have visible external identification, increasing the risk of physical violence and intimidation by the incumbent taxi industry.

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. Convoluted regulatory requirements mean that 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. This raises the price consumers must pay for those new services, and lowers the quality of the new service.

- → *License cap:* Taxi licenses are capped for taxi companies 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 but a flexible 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.

Unilateral Or Discriminatory Digital Tax Measures

Since 2017, Taiwan's Ministry of Finance has required nonresident suppliers to collect and remit a direct tax on cross-border business-to-consumer 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 U.S. companies to double taxation.

Taiwan's National Communications Commission is consulting on a draft bill that would impose registration requirements on Over the Top (OTT) services. The bill proposes broad requirements, including disclosure of subscriber numbers, appointment of a local representative, and membership of a self-regulatory body, that would present barriers to overseas based OTT services, including by requiring the disclosure of commercially sensitive data.

Thailand

Data Flow Restrictions And Service Blockages

Thailand's Personal Data Protection Bill lacks clarity in many areas that may lead to a number of concerning data localization requirements.

Non-IP Intermediary Liability Restrictions

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 they are assisting or facilitating the offense.[122] 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.[123] Such rules have resulted in the blockage of U.S. online services in Thailand.

[122] https://www.law.uw.edu/media/1423/thailand-intermediary-liability-of-isps-defamation.pdf
[123]https://www.eff.org/deeplinks/2012/05/suspended-sentence-good-news-thai-webmaster-jiew-threat-freedom-expression-remains

Turkey

Data Flow Restrictions And Service Blockages

Turkish Data Protection Law has entered into force in October 2016 but Turkish DPA did not announce yet a Safe Countries list to let data transferred abroad freely. According to the law all data controllers will need to get registered to the Verbis system run by DPA till September 30, 2020.

Furthermore the Communique on Information Systems Management (VII-128.9), published by the Capital Markets Board of Turkey, requires publicly traded companies to keep their primary and secondary information systems, data, and infrastructure in Turkey.

The Regulation on Information Systems of Banks, published in March 2020, does not change the status of data localization for companies in FSI and still requires banks and financial services to keep their primary (live/production data) and secondary (back-ups) information systems within the country. While the Regulation for the first time identifies cloud services in writing and draws a framework on how to procure those as an outsourced service, it only applies for services located in Turkey.

Non-IP Intermediary Liability Restrictions

In Turkey, internet services face liability if users post content that is blasphemous, discriminatory, or insulting. These are broad and vague limitations on user-generated content that make it very difficult for U.S. providers to operate in Turkey, whether they are running a communications platform or operating an e-commerce service that solicits user reviews of products and services.

Restrictions On Cloud Service Providers

Since there is no specific regulation dealing with the provision and use of cloud services, the Law on the Protection of Personal Data No. 6698 is considered the main regulatory framework for cloud service providers (CSPs). In addition to the data protection regulations, there are certain sector-specific regulations scattered amongst diverse regulations which, in general, require entities operating in such sectors to use localized information systems.

This situation creates a competition disadvantage for Turkey's local market, both in terms of attracting foreign investment due to concerns over sufficient practical means for hosting/processing data and around legal predictability and security. It also creates burdens for local businesses which are not able to benefit from the advanced opportunities offered by the hyperscale cloud services providers. As the world economy transforms into a data-driven economy, which requires the free flow of data as much as possible to maintain economic relations, all sectors as well as international trade are increasingly relying on cross-border data transfers. While Turkey and the U.S. are aiming to increase trade relations, restrictions created by Turkish data protection legislation confine companies' ability to actively participate in the Turkish economy. The current restrictive approach prevents the U.S. companies from selling their products and services requiring data transfers, including but not limited to IT solutions, and also restrains Turkish companies from connecting with U.S. companies as any engagement may result in significant changes to their operations.

The Presidential Circular on Information and Communication Security Measures No. 2019/12 published in July 2019 introduces important security measures, restrictions, and obligations to be implemented with the aim of mitigating and removing security risks and maintaining the security of certain critical types of data which may otherwise jeopardize public order and national security. Article 3 of the Circular states that data of public institutions and organizations shall not be stored in CSPs, except for the private systems of institutions or local service providers under the control of public institutions. ThisCSPs from public sector sales in Turkey. In addition to this, critical information (which will be defined gradually by the Digital Transformation Office) and data – such as population, health, and communication registration information – as well as genetic and biometric data shall be stored domestically in a safe environment.

Another sector specific regulation that brings localization requirements for companies in the financial services industry is the recent regulation on the Information System of Banks and Electronic Banking Services prepared by the Banking Regulation and Supervision Agency and which entered into force as of July 2020. This regulation requires banks and financial services to keep their primary information systems (production data) within the country. Furthermore the regulation prohibits banks from obtaining ad services from social media platforms and search engines that fail to implement adequate measures to prevent fake banking ads and requires banks to incorporate clauses in their contracts with ad service providers ensuring disclosure of information to banks in the event of fake ads.

Unilateral Or Discriminatory Digital Tax Measures

In December 2018 Turkey adopted a 15 percent withholding tax on businesses who do online advertising. Turkey has also adopted a DST that applies a 7.5 percent tax to revenues from targeted advertising, social media, and digital interface services. The tax applies only to companies generating €750 million in global revenues from covered digital services and TL20 million in in-country revenues from covered digital services. The structure of the tax expressly targets U.S. companies. The Turkish President has authority to increase the tax rate up to 15 percent. The law went into effect on March 1, 2020. IA believes that the Turkish DST is unreasonable and discriminates against U.S. digital companies by creating a targeted burden on U.S. commerce.

Law on Geographical Information Systems

In February 2020, the Government adopted a Law on Geographical Information Systems which requires real persons and private entities which collect, produce, release, sell geographical data to acquire a license from the Ministry of Environment and City Planning. Licencing fee is 50 lira for 1/1000 maps sections for foreign real persons and private law entities. In case of operating without licence 10 fold of the licencing fee sum will be charged.

Import Restrictions

The Turkish government is taking increasing actions in relation to imports. In April and May, the government temporarily increased the customs duty for imported game consoles by 50 percent and introduced a 30 percent “additional customs duty” for a variety of intermediary and consumer goods imported through commercial channels until December 31, 2020. This applies to nearly 3,000 types of products, including technological devices, home appliances, industrial products, cosmetic and beauty products, musical instruments, building materials and textile

products. These duties are imposed in the form of "additional customs duties" due to TR's obligation arising from its Customs Union with the EU to not amend "customs duty" rates. TR has argued the duties are justified based on provisions of WTO Agreements allowing members to take measures to protect domestic industries.

Regulation Social Network Providers

Turkey adopted the "Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications" (widely known as the social media law) in July 2020. The law requires social network providers with more than a million users to: (i) establish a representative office in Turkey, (ii) respond to individual complaints in 48 hours or comply with official take-down requests of the courts in 24 hours, (iii) report on statistics and categorical information regarding the Requests every 6 months, (iv) take necessary measures to ensure the data of Turkish resident users are kept in Turkey. In case of noncompliance, social network providers face serious monetary fines and 50-90 percent possible bandwidth reduction to their platform. While these amendments aim to regulate social network providers and enhance the obligations of hosting and content providers in order to protect the individuals in the internet environment, the vague obligation of data localization may require significant and costly operational changes for businesses and facilitating the execution of content removal/access blocking decisions raises significant concerns that it may lead to censorship of unwanted contents and may hinder free speech of individuals.

Ukraine

Copyright-Related Barriers

USTR included Ukraine on the 2016 Special 301 Report watchlist in part due to "the lack of transparent and predictable provisions on intermediary liability" and the absence of "limitations on [intermediary] liability" in Ukraine's copyright law.[124] These problems have not been effectively addressed in the past year.[125] Ukraine's intermediary liability law, which has now come into force, contains numerous problems, including an unfeasible requirement to remove information within 24 hours of a complaint, a requirement to provide user data to third parties even if an intermediary disputes the presence of infringing content, and a requirement to implement "technical solutions" for repeat postings that likely requires intermediaries to monitor and filter user content.[126] These and other provisions are in direct conflict with Section 512 of the Digital Millennium Copyright Act, and are harming the ability of U.S. companies to access the Ukraine market.

Restrictions On Cloud Service Providers

Article 11(4) of the Draft Cloud Law No. 2655 that was passed in the first reading prohibits processing of personal data and legally protected information of the Public users -- state and municipal authorities, state enterprises and organizations -- by any cloud means, if the cloud services and/or processing

[124] https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.
[125] See Tetyana Lokot, New Ukrainian Draft Bill Seeks Extrajudicial Blocking for Websites Violating Copyright, Global Voices (Feb. 1, 2016), https://advox.globalvoices.org/2016/02/01/new-ukrainian-draft-bill-seeks-extrajudicial-blocking-for-websites-violating-copyright/
[126] Law of Ukraine "On State Support of Cinematography in Ukraine"

centers are located outside of Ukraine. This requires any cloud infrastructure used by the Public users to be physically located in Ukraine. The Data Localization Requirement is discriminatory and contrary to the international commitments of Ukraine, and the national legislation, including Ukraine's WTO GATS commitments, the Ukraine-EU Association Agreement and Article 14 of the Law of Ukraine on Protection of Economic Competition.

United Arab Emirates

Infrastructure-Based Regulation Of Online Services

In the United Arab Emirates (UAE), nationally controlled telecom services have consistently throttled foreign VoIP and communications services, including WhatsApp VOIP, Apple Facetime, Google Hangouts and Duo, LINE, and Viber.[127] This throttling has created significant market access barriers in a key Middle East market for U.S.-based internet services and apps. However, despite acknowledging the negative implications for foreign services, UAE regulators have declined to intervene, and instead have continued to insist that only national providers can provide these forms of communications services.[128] These restrictions impede market access for U.S. services and appear to conflict with UAE's GATS commitments.

U.S internet services face similar barriers in Morocco, Saudi Arabia, and Oman, where nationally owned telecom services have engaged in similar forms of throttling, however, the throttling is most severe in the UAE.[129]

Non-IP Intermediary Liability Restrictions

The National Media Council Content Creators law applies to UAE residents and influencers operating in the UAE, including all social influencers who use their social media channels to promote and/or sell products. The law puts the responsibility on the owner of the account to obtain the license for their activities, and covers a broad scope, including "any paid or unpaid form of presentation and/or promotion of ideas, goods, or services by electronic means, or network applications". Influencers will need to clarify content that is sponsored and/or paid vs. editorial content on their social channels. The cost of the license is 15,000 AED and is valid for 12 months. The law is very selectively enforced and the NMC has the power to use it to respond to complaints made against a particular individual. Such onerous

[127] *See* Joey Bui, *Skype Ban Tightens in the UAE*, The Gazelle (Feb. 7, 2015), https://www.thegazelle.org/issue/55/news/skype/; *Is Skype Blocked In in the United Arab Emirates (UAE)?*, Skype, https://support.skype.com/en/faq/FA391/is-skype-blocked-in-the-united-arab-emirates-uae (last visited Oct. 24, 2016); Mary-Ann Russon, *If You Get Caught Using a VPN In in in the UAE, You Will Face Fines of Up to $545,000*, International Business Times (July 27, 2016), http://www.ibtimes.co.uk/if-you-get-caught-using-vpn-uae-you-will-face-fines-545000-1572888 (describing the government's ban on VPNs being motivated, in part, by blocking UAE consumers from accessing VoIP services); Naushad Cherrayil, *Google Duo Works in UAE – For Now*, Gulf News (Aug. 21, 2016) http://gulfnews.com/business/sectors/technology/google-duo-works-in-uae-for-now-1.1882838.

[128] *See* Mary-Ann Russon, *supra* note 98.

[129] *See* Saad Guerraoui, *Morocco Banned Skype, Viber, WhatsApp and Facebook Messenger. It Didn't Go Down Well,* Middle East Eye (Mar. 9, 2016), http://www.middleeasteye.net/columns/boycotts-appeals-petitions-restore-blocked-voip-calls-morocco-1520817507; Afef Abrougui, *Angered By Mobile App Censorship, Saudis Ask: What's the Point of Having Internet?,* Global Voices Advox (Sept. 7, 2016), https://advox.globalvoices.org/2016/09/07/angered-by-mobile-app-censorship-saudis-ask-whats-the-point-of-having-internet/; Vinod Nair, *Only Oman-Based VoIP Calls Legal*, Oman Observer (Apr. 16, 2016), http://omanobserver.om/only-oman-based-voip-calls-legal/.

licensing requirements covering a broad scope of social influencing activities add unnecessary friction to digital trade, and inhibit new social influencers particularly those based outside of the UAE but targeting the UAE market from participating in the UAE digital economy.

UAE's cybercrime laws contain several provisions that can act as market barriers to foreign players engaging and participating in the UAE digital market. These include:

- A penalty of imprisonment and a fine not exceeding AED 1,000,000 may be imposed on any person who creates or runs an electronic site or any IT means, to deride or to damage the reputation or the stature of the UAE or any of its institutions, the President of the UAE, the Vice President, any of the Rulers of the Emirates, the Crown Princes, the Deputy Rulers, the national flag, the national anthem, the emblem of the state, or any of its symbols.
- Producing, transmitting, publishing, and exploiting through an electronic site, gambling and/or pornographic material or any other material that may prejudice public morals;
- Insulting others or attributing to another an incident that may make him/her subject to penalty or contempt by others by using an electronic site;
- Using electronic sites to display contempt for any holy symbols, characters, figures, and rituals of Islam, including the Divinity and the Prophets, and for any other faiths or religions and any of their symbols, characters, figures and rituals.

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 and raising the price consumers must pay for those services.

- *Minimum price requirement:* For-hire transportation providers must charge 30 percent more than taxis.
- *Data-sharing requirement:* Companies providing transportation apps are routinely pressured to share data in real time, via integration into government computer systems.

United Kingdom

Copyright-Related Barriers

While the UK government has stated it has no plans to implement the recently passed EU Copyright Directive, the UK is considering its post-Brexit domestic policy priorities.[130] If the UK were to implement measures similar to those just passed in the EU, online service providers in the U.S. and elsewhere would be subject to a moving target in the UK for years to come. Smaller startups and entrepreneurs would be deterred from entering the UK market given the difficulty of raising funds from venture

[130] https://questions-statements.parliament.uk/written-questions/detail/2020-01-16/4371

capitalists that have consistently characterized such rules as strong impediments to investment.

Non-IP Intermediary Liability Restrictions

In April 2019, the UK government published an Online Harms White Paper that would create significant compliance issues for U.S. companies operating in the UK if it is enacted into law.[131]

In the White Paper the UK government proposes, among other things, to apply a new legal "Duty of Care" on a "wide range of companies of all sizes, including social media platforms, file hosting sites, public discussion forums, messaging services and search engines." The Duty of Care would require companies to protect users from a wide range of "online harms." The paper covers both illegal harms (e.g. terrorist content, child sexual exploitation material) and those "harms with a less clear definition" (e.g. cyberbullying, disinformation). The UK proposes to set up a new independent regulator – funded by industry – to assess how well companies are complying with the Duty of Care. The White Paper further consults on a range of penalties for non-compliance with the regulations, including fines, ISP blocking of services, and individual liability for senior management of companies not found in compliance.

IA is concerned that the scope of the recommendations is extremely wide-ranging and the unintended consequences for American companies is still not fully understood. Any proposal needs to be more targeted and practical for both big and small platforms to implement. As drafted, the proposals would potentially restrict access to key digital services that enable small businesses to grow and reach new markets. IA is also concerned that the proposed rules would disrupt the ability of startups and small businesses to build new digital services and to use existing user review and feedback mechanisms to connect with global customers.

IA urges USTR to engage with the UK government on these potential rules and to minimize any potential barriers to U.S.-UK trade.

Unilateral Or Discriminatory Digital Tax Measures

The UK has approved a DST as part of its Finance Bill 2020 that would apply a 2 percent tax on revenues above £25 million to internet search engines, social media, and online marketplaces. The tax applies only to companies generating at least £500 million in global revenues from covered digital services and £25 million in in-country revenues from covered digital services. The structure of the tax will expressly target U.S. companies. Payments would be due from affected companies in 2021. IA believes that the UK DST proposal meets the full threshold set under Section 302(b)(1)(A) of the Trade Act of 1974. IA notes that the UK Government has said that it would drop this tax if progress can be achieved at the OECD, and IA continues to urge all countries to prioritize these negotiations.

[131]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

Uruguay

Overly Restrictive Regulation of Online Services

Uruguay is currently considering a bill to regulate digital platforms and services.[132] However, this draft bill is vague and broad, and could affect a wide range of internet services and products. IA encourages USTR to monitor the development of this bill and advocate for consistency with the principles for regulation provided within this filing.

Vietnam

Copyright-Related Barriers

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 USTR 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. [133]

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

Cybersecurity Law

In June 2018, Vietnam's National Assembly passed the Law on Cybersecurity containing a broad and vague data localization requirement (Article 26.3), however, the Law states that data localization requirements will only be enforced after issuance of detailed guidance in the form of an implementing decree (Article 26.4). The latest draft implementing decree has reportedly been discussed by the Cabinet in August 2020 and has been privately shared with select foreign governments. Within this draft, there is a provision that would require all domestic companies to keep their data onshore, while foreign companies would only have to onshore their data if they do not adequately cooperate with law enforcement. Technically, this Law applies equally to local and foreign companies. If all domestic entities are required to localize data under this implementing decree, no hyper-scale CSP will be able to sell to Vietnamese customers, as none of them currently have a local region. On the other hand, if localization mandates are issued to foreign entities with no local presence, these foreign entities will incur significant additional overhead costs vis-à-vis their local entities. When read alongside other policy proposals, it is clear that the Government of Vietnam is creating a technical and regulatory barrier to favor nascent local telcos and CSPs. Localization requirements have therefore been explicitly used as a

[132] Transporte Público Y Creación De Plataformas Virtuales De Servicios, Carpeta No. 786, Repartido No. 388 (Feb. 16, 2016), available at http://vamosuruguay.com.uy/proyecto-plataformas-virtuales/.

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

de facto market access barrier.

Video On Demand Regulation (VOD)

The Authority of Broadcasting and Electronic Information (ABEI) has issued a draft regulation that would regulate VOD services in a matter similar to traditional broadcast television. This Decree 6 would require VOD services to obtain an operating license, maintain a local content quota, and translate content into Vietnamese. It is anticipated that officials intend to apply the requirements to services operating off-shore. The burdensome requirements of the Decree would be exceptionally difficult for these off-shore providers to comply with, and could serve to effectively shut out any VOD provider unable to obtain Vietnamese content, perform translation, and adhere to other requirements. Not only would adoption serve as a significant barrier to trade, it would be largely outside the norms for how governments treat curated content delivered over the internet. The U.S. should encourage Vietnam to consider global best practices with respect to VOD regulation, ensuring that Vietnamese consumers and content developers can benefit from the offerings of foreign providers.

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, as highlighted above, 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 three-hour window for compliance with content takedown requests, as well as numerous other market access barriers highlighted below.[134]

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 three 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.

As USTR identified in the 2016 National Trade Estimate, 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 USTR to take similar action on this Vietnamese decree and to highlight that this decree would serve as a market access barrier. In addition, IA encourages USTR to work with Vietnam and other countries to develop intermediary liability protections

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

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.[135]

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

Infrastructure-Based 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.[136]

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, USTR should monitor this or any similar requirements. In particular, USTR 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.

Cross Border Provision Of Advertising Services

On August 19, 2020, the Ministry of Information and Communications (MIC) released for public

[135] 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.

[136] *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.

consultation a draft Decree to amend the Decree 181/2013 (Decree on Elaboration of some Articles on the Law on Advertising). The draft seeks to regulate advertising content, and has expanded the scope of application to include Apps and social media. The draft lacks clarity on definitions, procedures and restrictions, imposes onerous reporting requirements, and obliges providers to actively manage ad content and placement. IA urges USTR to seek a removal of all clauses in the draft that have overlapping liability in other laws to avoid confusion, duplication and unclear reporting/responsible authority (e.g. take-down requests and tax obligation should be regulated only in Decree 72 and relevant tax laws). If online advertising content control is the main objective of this amendment, IA recommends that USTR encourage the Government to control content under a single legislation.

On June 3, 2020, Vietnam's Prime Minister signed Decision 749/QD-TTg, which announces the country's National Digital Transformation Strategy by 2025, and specifically calls for the introduction of technical and non-technical measures to control cross-border digital platforms. The Ministry of Information and Communications (MIC) has subsequently issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, which set forward cloud technical standards and considerations for state agencies and smart cities projects in favor of local private cloud use. These decisions clearly intend to create a preferential framework for domestic CSPs, creating de facto market access barriers. Furthermore, the MIC Minister has made public statements noting that "as Vietnamese firms are getting stronger hold of physical networks, [Vietnam] must do the same for cloud computing and digitalization infrastructures." While these standards are technically "voluntary," in practice, this will be adopted by the Vietnamese public sector as if it is mandatory.

Unilateral Or Discriminatory Digital Tax Measures

As part of the Government of Vietnam's plan to protect local businesses, the Tax Administration Law, effective 1 July 2020, taxes cross-border e-commerce and other digital services. The Ministry of Finance is drafting the implementation circular, which will mandate that cross-border digital service providers register, declare and pay taxes (VAT and CIT) from January 2021; and the official release of a draft circular is forthcoming. This tax is explicitly discriminatory, as it operates as a tariff on foreign-provided digital goods and services. Pending OECD recommendations on digital taxes, and in the absence of a Digital Tax Agreement between Vietnam and the U.S., unilateral taxes by Vietnam will put U.S. companies at risk of double taxation and create tax compliance burdens.

Zimbabwe

Overly Restrictive Regulation of Online Services

A June 2016 consultation paper focused on the absence of "over-the-top" regulation and suggested a licensing framework with emergency services and lawful intercept under discussion.[137]

[137] POTRAZ, *Consultation Paper No. 2 of 2016,* https://www.potraz.gov.zw/images/documents/Consultation_OTT.pdf.

Other Geographic Regions

East African Region

Copyright-Related Barriers

The East African Legislative Assembly passed the East African Community Electronic Transactions Act in 2015. While the Act provides for some level of protection of intermediaries from liability for third party content, it fails to include any 'counter-notice' procedures for a third party to challenge a content takedown request. Also, it removes legal protections if the intermediary receives a financial benefit from the infringing activity. Lack of a counter-notice provision exposes internet intermediaries to business process disruptions through frivolous takedown notices.

Even more problematic, vague language about 'financial benefits' can remove an entire class of commercially-focused intermediaries from the scope of liability protections, and can result in a general obligation on these intermediaries to monitor internet traffic, disadvantaging commercial services from entering numerous East African markets, including Kenya, Uganda, Tanzania, Burundi, Rwanda, and South Sudan.

The requirements in the Act diverge from prevailing international standards for intermediary liability frameworks, and serve as market access barriers for companies seeking to do business in these countries. IA urges USTR to engage with counterparts in Kenya and elsewhere to amend this provision on the grounds highlighted above, and to develop intermediary liability protections that are consistent with U.S. standards and international norms.

Latin America Regional

Burdensome or Discriminatory Data Protection Regimes

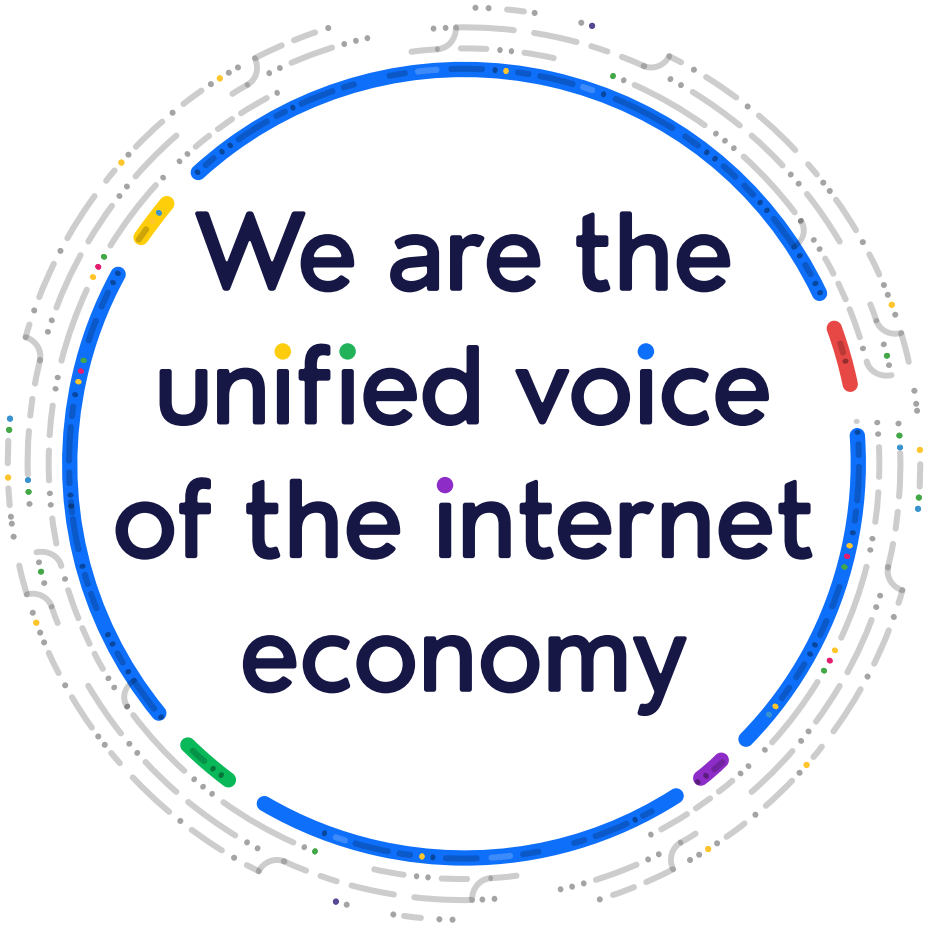
Governments in the region continue to respond reactively to data privacy concerns by advancing heavy handed data privacy bills that seek to align their privacy regulations with GDPR, without fully comprehending the impact on the local economy or how the systems are effectively implemented/enforced. These draft pieces of legislation—in Panama, Chile, Ecuador, Argentina, and Honduras, for example—raise a number of challenges for U.S. companies, including: 1) scope of application and extraterritoriality; 2) introduction of the right to be forgotten; 3) express consent for all situations; and 4) prior authorization by the authority for international data transfer. In some cases these rules could have a crippling impact on all U.S. companies that need to transfer data across borders.

Unilateral Or Discriminatory Digital Tax Measures

Numerous countries in the region have already implemented or are in the process of putting indirect taxes (VAT/GST) on cross-border supplies of electronically supplied services ("ESS"). However, in stark contrast to the dozens of other jurisdictions in the world, countries in Latin America are not leveraging global best practices or incorporating the key OECD principles of neutrality, efficiency, certainty,

simplicity, effectiveness and fairness, and flexibility. Through a newly invented process, they are creating an unlevel playing field. Specifically, governments should utilize the "Non-resident Registration" Tax Collection Model, instead of attempting to implement the "Financial Intermediary" Tax Collection Model that was recently created by the Argentine government and is potentially being replicated in Colombia, Chile, Costa Rica, and other countries.

U.S. suppliers of cross-border ESS have customers facing incidents of double taxation and there are other foreign services providers who are not having to pay the tax at all.



www.internetassociation.org