



Internet Association



Submission For The 2020 USTR National Trade Estimate Report

Docket No. USTR-2019-0012

Internet Association



Introduction	8
American Digital Trade Leadership	9
Key Issues Impacting Internet Companies Around the World	10
Copyright-Related Barriers	10
Customs Barriers To Growth In E-Commerce	12
Data Flow Restrictions And Service Blockages	12
Divergence From Privacy Best Practices	13
Infrastructure-Based Regulation Of Online Services	13
Non-IP Intermediary Liability Restrictions	14
Unilateral Or Discriminatory Digital Tax Measures	14
Emerging Issues	15
Foreign Digital Trade Barriers	16
Argentina	16
Divergence From Privacy Best Practices	16
Customs Barriers To Growth In E-Commerce	16
Restrictive Regulation Of Online Services	16
Sharing Economy Barriers	16
Copyright-Related Barriers	17
Australia	17
General	17
Copyright-Related Barriers	17
Non-IP Intermediary Liability Restrictions	18
Unilateral Or Discriminatory Digital Tax Measures	19
Bahrain	19
Restrictions On Cloud Service Providers	19
Bangladesh	20
Non-IP Intermediary Liability Restrictions	20
Belarus	20
Non-IP Intermediary Liability Restrictions	20
Brazil	20
Divergence From Privacy Best Practices	20
Customs Barriers To Growth In E-Commerce	21
Data Flow Restrictions And Service Blockages	21
Filtering, Censorship, And Service-Blocking	21
Restrictions On Cloud Service Providers	22
Infrastructure-Based Regulation Of Online Services	22
Copyright-Related Barriers and Non-IP Intermediary Liability Restrictions	22
Canada	23
Discriminatory Or Opaque Application Of Competition Regulations	23
Divergence From Privacy Best Practices	23
Non-IP Intermediary Liability Restrictions	23
Unilateral Or Discriminatory Digital Tax Measures	24



Chile	24
Copyright-Related Barriers	24
Divergence From Privacy Best Practices	24
China	25
Data Flow Restrictions And Service Blockages	25
Discriminatory Or Opaque Application Of Competition Regulations	25
Electronic Payments	25
Filtering, Censorship, And Service-Blocking	26
Restrictions On U.S. Cloud Service Providers	26
Infrastructure-Based Regulation Of Online Services	27
Colombia	27
Copyright-Related Barriers	27
Customs Barriers To Growth In E-Commerce	27
Sharing Economy Barriers	28
Unilateral Or Discriminatory Digital Tax Measures	28
Ecuador	28
Burdensome or Discriminatory Data Protection Regimes	28
Egypt	28
Filtering, Censorship, And Service-Blocking	28
Sharing Economy Barriers	29
European Union (EU)	29
Broad, Unclear, And Intrusive Monitoring And Filtering Obligations	29
Divergence From Privacy Best Practices	30
Copyright-Related Barriers And Other Issues	31
Ancillary Copyright And Neighboring Rights	31
Liability For Hyperlinks	32
Restrictions On Text And Data Mining	32
Weakening Of E-Commerce Directive Protections For Internet Services In EU Member States	32
Customs/Trade Facilitation	33
Extended Producer Responsibility (EPR)	33
Data Flow Restrictions And Service Blockages	34
Infrastructure-Based Regulation Of Online Services	34
Non-IP Intermediary Liability	35
Sharing Economy Barriers	36
Unilateral Or Discriminatory Digital Tax Measures	36
EU Member State Measures	37
Austria	37
Sharing Economy Barriers	37
Unilateral Or Discriminatory Digital Tax Measures	37
Belgium	38
Sharing Economy Barriers	38



Denmark	38
Sharing Economy Barriers	38
France	39
Copyright-Related Barriers	39
Data Flow Restrictions And Service Blockages	39
Non-IP Intermediary Liability Restrictions	39
Restrictions on U.S. Cloud Service Providers	40
Sharing Economy Barriers	40
Unilateral Or Discriminatory Digital Tax Measures	41
Germany	42
Copyright-Related Barriers	42
Discriminatory Or Opaque Application Of Competition Regulations	43
Non-IP Intermediary Liability Restrictions	43
Overly Restrictive Regulation of Online Services	44
Restrictions on U.S. Cloud Service Providers	44
Sharing Economy Barriers	44
Greece	44
Copyright-Related Barriers	44
Sharing Economy Barriers	45
Hungary	45
Filtering, Censorship, And Service-Blocking	45
Unilateral Or Discriminatory Digital Tax Measures	45
Italy	45
Copyright-Related Barriers	45
Sharing Economy Barriers	46
Unilateral Or Discriminatory Digital Tax Measures	46
Poland	46
Copyright-Related Barriers	46
Portugal	47
Sharing Economy Barriers	47
Spain	47
Copyright-Related Barriers	47
Sharing Economy Barriers	48
Unilateral Or Discriminatory Digital Tax Measures	48
Sweden	49
Copyright-Related Barriers	49
Restrictions on U.S. Cloud Service Providers	49
Sharing Economy Barriers	49
United Kingdom	50
Copyright-Related Barriers	50
Non-IP Intermediary Liability Restrictions	50
Unilateral Or Discriminatory Digital Tax Measures	50



Hong Kong	51
Copyright-Related Barriers	51
Sharing Economy Barriers	52
India	52
Copyright-Related Barriers	52
Divergence From Privacy Best Practices	52
Data Flow Restrictions And Service Blockages	53
Discriminatory Or Opaque Application Of Competition Regulations	54
Barriers To Mobile Payments	54
Blocking Foreign Direct Investment	54
Duties On Electronic Transmissions	55
Filtering, Censorship, And Service-Blocking	55
Non-IP Intermediary Liability Restrictions	55
Infrastructure-Based Regulation Of Online Services	56
Unilateral Or Discriminatory Digital Tax Measures	57
Indonesia	58
General	58
Data Flow Restrictions And Service Blockages	58
Discriminatory Or Opaque Application Of Competition Regulations	58
Disciplining Digital Platforms (OTT)	59
Excessive Government Access on Cybersecurity	59
Duties On Electronic Transmissions	59
Overly Restrictive Regulation of Online Services	60
Unilateral Or Discriminatory Digital Tax Measures	60
Jamaica	60
Divergence From Privacy Best Practices	60
Japan	60
Infrastructure-Based Regulation Of Online Services	60
Sharing Economy Barriers	61
Copyright-Related Barriers	62
Jordan	62
Sharing Economy Barriers	62
Kenya	63
Burdensome or Discriminatory Data Protection Regimes	63
Copyright-Related Barriers	63
Data Flow Restrictions And Service Blockages	63
Infrastructure-Based Regulation Of Online Services	64
Korea	64
Copyright-Related Barriers	64
Burdensome or Discriminatory Data Protection Regimes	64
Data Flow Restrictions And Service Blockages	64
Discriminatory Or Opaque Application Of Competition Regulations	64



Overly Restrictive Regulation of Online Services	65
Restrictions On Cloud Service Providers	65
Networking Charges	65
Sharing Economy Barriers	65
Malaysia	66
Infrastructure-Based Regulation Of Online Services	66
Mexico	66
Infrastructure-Based Regulation Of Online Services	66
Sharing Economy Barriers	66
Copyright-Related Barriers	67
New Zealand	67
Copyright-Related Barriers	67
Intermediary Liability	68
Unilateral Or Discriminatory Digital Tax Measures	68
Nigeria	68
Copyright-Related Barriers	68
Data Flow Restrictions And Service Blockages	68
Pakistan	69
Overly Restrictive Regulation of Online Services	69
Unilateral Or Discriminatory Digital Tax Measures	69
Panama	69
Burdensome or Discriminatory Data Protection Regimes	69
Sharing Economy Barriers	69
Peru	70
Copyright-Related Barriers	70
Qatar	70
Restrictions On Cloud Service Providers	70
Russia	71
Copyright-Related Barriers	71
Data Flow Restrictions And Service Blockages	71
Filtering, Censorship, and Service-Blocking	72
Saudi Arabia	72
Customs Barriers To Growth In E-Commerce	72
Data Flow Restrictions And Service Blockages	73
Restrictions On Cloud Service Providers	73
Senegal	73
Infrastructure-Based Regulation Of Online Services	73
Singapore	74
South Africa	74
Duties On Electronic Transmissions	74
Sharing Economy Barriers	74



Taiwan	75
Discriminatory Of Non-Objective Application Of Competition Regulations	75
Sharing Economy Barriers	75
Unilateral Or Discriminatory Digital Tax Measures	75
Thailand	76
Data Flow Restrictions And Service Blockages	76
Non-IP Intermediary Liability Restrictions	76
Turkey	76
Data Flow Restrictions And Service Blockages	76
Non-IP Intermediary Liability Restrictions	76
Restrictions On Cloud Service Providers	76
Unilateral Or Discriminatory Digital Tax Measures	77
Ukraine	77
Copyright-Related Barriers	77
United Arab Emirates	77
Infrastructure-Based Regulation Of Online Services	77
Sharing Economy Barriers	78
Uruguay	78
Overly Restrictive Regulation of Online Services	78
Vietnam	78
Copyright-Related Barriers	78
Cybersecurity Law	79
Video on Demand Regulation (VOD)	79
Data Flow Restrictions And Service Blockages	79
Non-IP Intermediary Liability	80
Infrastructure-Based Regulation Of Online Services	80
Zimbabwe	81
Overly Restrictive Regulation of Online Services	81
Other Geographic Regions	82
East African Region	82
Copyright-Related Barriers	82
Latin America Regional	82
Burdensome or Discriminatory Data Protection Regimes	82
Unilateral Or Discriminatory Digital Tax Measures	82



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-2019-0012) for consideration as the Office of the United States Trade Representative (USTR) prepares the 2020 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.

Over the past year, internet businesses have continued to face significant challenges around the world that are undermining the United States' (U.S.) leadership in the digital economy. Countries such as Vietnam, Indonesia, and India are adopting 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. Countries in the EU and elsewhere are proposing discriminatory digital services taxes that disproportionately impact U.S. technology firms by design. The recent 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. 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 three years, 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 2019 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, and otherwise restrict the ability of American internet companies to compete globally. IA welcomes USTR's leadership and encourages the continued 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 2020 NTE Report and its trade agenda.

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

² <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/march/fact-sheet-2019-national-trade-estimate>



American Digital Trade Leadership

The U.S. is the global internet and digital content leader. Americans are enjoying a digital revolution that has led to amazing products, lower prices, and new jobs, and American has spearheaded digitally driven export growth across borders, with digital trade now accounting for more than 55 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. Each year, U.S. manufacturers export \$86.5 billion of products and services through digital trade. Figures from BEA show that the 2018 U.S. digital trade surplus increased 4.3 percent to \$178.3 billion³ from \$172 billion in 2017.⁴

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.

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.

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.⁵ 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 This filing previously stated totals for “total digital service exports” and “digital service trade surplus” that summed together ICT-enabled service exports and potential ICT-enabled service exports. These figures should not have been summed together as potential ICT-enabled service exports includes ICT-enabled service exports. The correct totals are approximately \$439 billion in digital service exports and a surplus of \$172.6 billion for digital service trade balance. The previous, incorrect figures were \$470 billion in digital service exports and \$196.1 for for digital service trade balance.

⁴ <https://apps.bea.gov/iTable/iTable.cfm?reqid=62&step=9&isuri=1&6210=4#reqid=62&step=9&isuri=1&6210=4> (Table 3.1)

⁵ <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.⁶ 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.

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.

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 DMCA (“ISP safe harbors”) to create jobs, foster innovation, and promote economic growth. The U.S. internet sector – as well as small businesses that rely on the internet to reach customers abroad – require balanced copyright rules to do business in foreign markets.

⁶ <http://www.cciainet.org/wp-content/uploads/2017/06/Fair-Use-in-the-U.S.-Economy-2017.pdf>



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.

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.⁷ 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 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.⁸ And yet key trading partners have failed to implement ISP safe harbors, including three countries (Australia, Colombia, and Peru) that 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. 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 use upcoming trade negotiations to promote a strong and balanced copyright framework that benefit all U.S. stakeholders. Without these business-critical protections, internet services – and the industries they enable – face troubling legal risks, even when they follow U.S. law.

⁷ Capital Trade. "Fair Use in the U.S. Economy." <http://www.ccianet.org/wp-content/uploads/library/CCIA-FairUseintheUSEconomy-2011.pdf>.

⁸ <http://internetassociation.org/wp-content/uploads/2017/06/NERA-Intermediary-Liability-Two-Pager.pdf>



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 2020 NTE and work with foreign countries to modernize these antiquated systems and overly burdensome systems. When it comes to USMCA, IA understands that USTR must undertake intensive work during the implementation phase of 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.⁹

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.

⁹ <https://internetassociation.org/us-mexico-canada-agreement/>



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 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.¹⁰ 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 number of countries have started moving forward with laws that are problematic in this respect.

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 2020 NTE as key impediments to digital trade.

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.¹¹

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.

¹⁰ https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/

¹¹ “The Economic and Societal Value of Rich Interaction Applications (RIAs).” WIK, 2017. http://www.wik.org/fileadmin/Studien/2017/CCIA_RIA_Report.pdf



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.

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 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.

Unilateral Or Discriminatory Digital Tax Measures

An increasing number of foreign trading partners – particularly but not exclusively in the EU – are proposing discriminatory 2 to 7 percent revenue taxes on digital services that U.S. technology firms provide. These digital services taxes (DSTs) are narrow in scope and are specifically designed to target U.S. digital companies. In many cases, these taxation measures contradict longstanding global consensus-based practices (e.g., by taking 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. 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.

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 DSTs, countries are taking 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.¹² 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 2020.¹³

USTR's initiation of a Section 301 investigation into France's DST was an important step in exercising American leadership to stem the tide of new discriminatory taxes in Europe and the rest of the world, and to push countries towards a multilateral OECD solution. The industry appreciates the prioritization of this issue by the U.S. government, and notes the bipartisan support in Congress for U.S. engagement. In order to fully stem the tide of new discriminatory taxes across the world, the U.S. will need to continue to exercise leadership. The U.S. is key to ensuring a global consensus around modern, global tax reform and in going forward it must continue sending a strong message to trading partners that targeted discriminatory taxes against U.S. firms are not an appropriate solution.

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 2020 NTE.

¹² <http://www.oecd.org/tax/beps/>

¹³ <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>



Foreign Digital Trade Barriers

Argentina

Divergence From Privacy Best Practices

Argentine President Mauricio Macri submitted to National Congress Bill No. MEN-2018-147-APN-PTE, aiming to replace in its entirety the Personal Data Protection Law No. 25,326, in force since 2000, which together with the Argentine Constitution sets forth general principles regarding data protection and habeas data. This bill includes a problematic provision regarding the extraterritorial application of the 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 creates 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.

Restrictive Regulation Of Online Services

In Argentina, the telecommunications reform commission recently issued 17 principles that would inform a “convergence” bill, aimed at unifying the telecommunications and audiovisual content laws that were enacted by the previous government.¹⁴ These principles do not explicitly leave information services, content services, and apps out of the scope of the bill, and may include new obligations both to register applications and satisfy intermediary liability requirements. In particular, the obligation to register an application would entail a set of complex administrative procedures that developers would need to follow before making their app widely available. Such obligations could create clear market access barriers for internet services that do not face registration requirements in other markets.

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

¹⁴ *New Rules of the Game in Telecommunications in Argentina*, OBSERVACOM. <http://www.observacom.org/new-rules-of-the-game-in-telecommunications-in-argentina/>



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.

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.

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

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

¹⁶ Section 116ABA of the Copyright Amendment (Service Providers) Act 2018.



internet services seeking access to the Australian market. IA urges USTR and others in 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 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

Non-IP Intermediary Liability Restrictions

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.²² The act applies to an excessively broad range of technology companies, and has increased compliance risks for U.S. based social media,

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

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 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.²³

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.

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.²⁴

Bahrain

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.

²³ <https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html>

²⁴ *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/>.



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.²⁵ 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.

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; 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

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.²⁶

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.²⁷ 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.

²⁵ <https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf>

²⁶ *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>.

²⁷ 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.²⁸

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 and competition 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.

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); it does not recognize the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks (ANATEL's Resolution 323).

The GSI (Institutional Security Office) revised its cloud guidelines and determined that government data should have some types of data localized. While this is only applicable to government data and these are just guidelines, this precedent raises serious concerns.

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.²⁹

²⁸ Cross Border Privacy Rules System, CBPRS, <http://www.cbprs.org/> (last visited Oct. 25, 2016).

²⁹ 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>; 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/>.



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.

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.³⁰ 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.

Copyright-Related Barriers and Non-IP Intermediary Liability Restrictions

Historically, the ‘Marco Civil’ law³¹ has offered legal certainty for domestic and foreign online services and has created conditions for the growth of the digital economy in Brazil.³² 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.³³

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.

³⁰ *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.rapidthvnews.com/2016070543482/brazil-s-creators-demand-vod-regulation.html#axzz4O8DTZE5y>.

³¹ Brazilian Civil Rights Framework for the Internet, Law No. 12.965 (2014).

³² Angelica Mari, *Brazil Passes Groundbreaking Internet Governance Bill*, ZDNET, <http://www.zdnet.com/brazil-passes-groundbreaking-internet-governance-bill-7000027740/>.

³³ Andrew McLaughlin, *Brazil’s Internet is Under Legislative Attack*, MEDIUM, <https://medium.com/@mcandrew/brazil-s-internet-is-under-legislative-attack-1416d94db3cb#.dy4aak1yk>.



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 Netflix, 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." 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. 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 United States-Mexico-Canada Agreement (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.³⁴

Non-IP Intermediary Liability Restrictions

The Liberal platform calls for new rules regulating online content and expands the role of internet companies in addressing content posted online.³⁵ The plan includes significant penalties for social-media companies that fail to address online harms within 24 hours. The plan runs counter to USMCA Article 19.17, and IA urges USTR to engage with Canadian officials on this issue.

³⁴ https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/

³⁵ <https://2019.liberal.ca/wp-content/uploads/sites/292/2019/09/Forward-A-real-plan-for-the-middle-class.pdf>



Unilateral Or Discriminatory Digital Tax Measures

Canadian Prime Minister Justin Trudeau has proposed a digital services tax similar to the French DST.³⁶ 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.³⁷ IA urges USTR to 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 rules³⁸ 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 (Recopilación 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 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 and enforced. These draft pieces of legislation 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.

³⁶ <https://2019.liberal.ca/wp-content/uploads/sites/292/2019/09/Forward-A-real-plan-for-the-middle-class.pdf>

³⁷ https://www.pbo-dpb.gc.ca/web/default/files/Documents/ElectionProposalCosting/Results/32977970_EN.pdf?timestamp=1569835806287

³⁸ Law No. 17.336 on Intellectual Property (as amended 2014), Art. 71.



China

Data Flow Restrictions And Service Blockages

China imposes numerous requirements on internet services to host, process, and manage data locally within China, and places significant restrictions on data flows entering and leaving the country.³⁹ China continues to moderate the public's access to websites and content online. On June 4, 2019, access to CNN was blocked⁴⁰ 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.

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 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 license 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.

³⁹ Data localization, AmChamChina, <http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization>

⁴⁰ <https://techcrunch.com/2019/06/04/china-blocks-cnn-website-and-reuters-stories-about-tiananmen-square/>



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.⁴¹ China actively censors – and often totally blocks – cross border internet traffic. It has been estimated that approximately 3,000 internet sites are totally blocked from the Chinese marketplace, including many of the most popular websites in the world. High-profile examples of targeted blocking of whole services include China's blocking of Facebook, Picasa, Twitter, Tumblr, Google search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare. This blocking has cost U.S. services billions of dollars, with a vast majority of U.S. companies describing Chinese internet restrictions as either “somewhat negatively” or “negatively” impacting their capacity to do business in the country.

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

Restrictions On U.S. Cloud Service Providers

U.S. cloud 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 transfer valuable U.S. intellectual property, 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.

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

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

⁴¹ Data localization, AmChamChina, <http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization>



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.

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 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.

Colombia

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, but while this bill contains a number of new copyright enforcement provisions, it lacks both fair use limitations and exceptions and intermediary liability safe harbor provisions that are required under the FTA.⁴² 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.

⁴² 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).



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.

Unilateral Or Discriminatory Digital Tax Measures

Colombia's Tax Authority includes a Permanent Establishment obligation for foreign companies that "have significant economic activities in the country." The bill appears to be designed to require digital economy companies to pay taxes on the same income that is taxed in the United States.

Ecuador

Burdensome or Discriminatory Data Protection Regimes

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. Key topics for the bill include strict requirements on express consent and a right to be forgotten provision.

Egypt

Filtering, Censorship, And Service-Blocking

On August 19, 2018, Egypt President Abdel Fattah al-Sisi signed a cybercrime law which makes it illegal to operate and to visit websites considered threats to the country, under threat of fines. Critics state that the law increases censorship and silences political opposition. During March 2019, Egypt's top media regulator the Supreme Media Regulatory Council, 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.⁴³ State censorship continues, and in April 2019, internet service providers in Egypt blocked 34,000 internet domains to prevent the public from accessing a 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.⁴⁴

⁴³ <https://www.haaretz.com/middle-east-news/egypt/egypt-can-now-block-websites-social-media-accounts-deemed-a-threat-1.7041232>

⁴⁴ <https://madamasr.com/en/2019/04/16/news/u/egypt-blocks-over-34000-websites-in-attempt-to-shut-down-constitutional-amendments-opposition-campaign/>



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.

European Union (EU)

Broad, Unclear, And Intrusive Monitoring And Filtering Obligations

The European Union's (EU) recent 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 17⁴⁵ 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.

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 the provisions of 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

⁴⁵ Article 15 was previously known as Article 11 and Article 17 was previously known as Article 13.



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.⁴⁶ 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.

Divergence From Privacy Best Practices

The E.U. General Data Protection Regulation is now in effect.⁴⁷ There is still considerable ambiguity in the text. Specifically, how E.U. data protection authorities choose to interpret the law will have a significant impact on companies’ ability to operate in the E.U. and offer consistent services and products across the globe.

Privacy Shield is indispensable to many U.S. companies, the U.S. economy, and the U.S.-EU economic relationship. The program provides companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the U.S. in support of transatlantic commerce. Its usefulness may be threatened by future court challenges and modifications arising out of the annual review process – such as potential restrictions on automated processing/profiling.⁴⁸ Standard Contractual Clauses (SCCs) may also be threatened by ongoing litigation.⁴⁹ Significant challenges to these transfer mechanisms threaten the viability of billions of dollars in EU-U.S. data transfers.

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 basic technological function of webpages and other online media.

⁴⁶ <https://www.techdirt.com/skyisrising/>

⁴⁷ 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>.

⁴⁸ <http://www.computerweekly.com/news/450302513/Slow-response-to-Privacy-Shield-EU-US-data-transfer-programme>.

⁴⁹ See, e.g., Allison Grande, *Irish Regulator Says Data Transfer Row Will Deliver Clarity*, LAW 360 (Sept. 30, 2016), <https://www.law360.com/articles/846924?sidebar=true>.



Copyright-Related Barriers And Other Issues

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 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 quotations or snippets 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.”⁵⁰ 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.⁵¹

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

⁵⁰ 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”).

⁵¹ The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, art. 9.



disadvantage internet services from offering services otherwise protected under copyright law by raising barriers to market entry.

As discussed below, 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.⁵² The EU's directive, like those earlier provisions, runs afoul of international obligations in the Berne Convention by giving some publishers the right to block internet services from making quotations from a work.⁵³

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.⁵⁴ 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

Finally, 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.⁵⁵ Another U.S.-based platform was found liable because it

⁵² *EU Lawmakers Are Still Considering This Failed Copyright Idea*, FORTUNE (March 24, 2016), <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).

⁵³ 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>.

⁵⁴ *C-GS Media BV v. Sanoma Media Netherlands BV et al.*, [ECLI:EU:C:2016:644](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016J0644&from=EN), European Court of Justice (8 September 2016).

⁵⁵ *RTI v. Kewego* (2016).



engaged in indexing or other organization of user content.⁵⁶ 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.”⁵⁷ All of these activities represent increasingly 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 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 admin 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

⁵⁶ Delta TV v. YouTube (2014).

⁵⁷ RTI v. TMFT (2016).



market. Furthermore, under the current regime, sellers on online marketplaces are often faced with double payments issue where the vendor pays the relevant EPR fee in the country where it places the goods on the market originally, and the sellers is 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.

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,⁵⁸ as well as local content quotas relating to the Audiovisual Media Services Directive (AVMS).⁵⁹

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 ranking.”⁶⁰ 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.

⁵⁸ 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](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)569979) (last visited Oct. 25, 2016).

⁵⁹ <https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd>

⁶⁰ <https://ec.europa.eu/digital-single-market/en/news/regulation-promoting-fairness-and-transparency-business-users-online-intermediation-services>.



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 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.



Sharing Economy Barriers

Ridesharing companies face two general categories of barriers that prohibit them from effectively competing across EU member states: market access restrictions and operational restrictions. While many of these restrictions may directly apply to drivers using ridesharing networks, they directly affect the provision of ridesharing companies' software application services by limiting the scale, raising the cost, undermining the efficiency, and eroding the quality that business models using these technologies can otherwise generate. These restrictions go beyond what is necessary to advance any legitimate public interest objective and instead serve to prevent competition with domestic traditional transportation providers.

Unilateral Or Discriminatory Digital Tax Measures

In March 2019, the European Union scrapped a plan to introduce an EU-wide digital tax as some states opposed it. However, similar taxes are being introduced at the EU state-level. Austria, France, Italy, the UK, and Spain, are proposing or have adopted discriminatory 2 to 7 percent revenue taxes on digital services that U.S. technology firms provide.

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.



EU Member State Measures

Austria

Sharing Economy Barriers

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

- *Vehicle requirements:* For-hire vehicles must be of a minimum length of 4.2 meters, width of 1.56 meters, height of 1.3 meters, and be equipped with air conditioning.
- *Capital requirements:* In Vienna, vehicle fleet owners must meet a capital requirement of €7,500 for every car that they want to operate.
- *This requirement is cumulative:* if someone wants to add a fifth car to a fleet of four cars, she would have to produce proof of additional available funds of €37,500 (5 x €7,500) and not merely an additional €7,500.
- *Professional experience requirement:* To become a for-hire driver, one needs at least three years of relevant work experience.
- *Return-to-garage rule:* For-hire vehicles must return to their company's place of business after completion of the trip unless they receive a new request during their return to the company's place of business. The request itself, however, must be accepted at the company's place of business.

Unilateral Or Discriminatory Digital Tax Measures

In April 2019, Austria published a draft bill introducing a 5 percent tax on digital advertising revenues (an increase from the 3 percent in previous proposals). Then-Chancellor Kurz announced that “Austria will now introduce a national tax on digital giants like Google or Facebook to ensure that they also pay their fair share of taxes.” Like other national tax proposals, a revenue threshold ensures that only large U.S. companies fall within the scope of the proposed tax. The tax could receive a favorable vote prior to elections in fall 2019.



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 €31,133.29 (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 €90.

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.



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.⁶¹ 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.⁶² 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

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, member 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 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

⁶¹ 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>.

⁶² Open Letter to Minister Azoulay, March 2016, available at <http://www.cccanet.org/wp-content/uploads/2016/03/OpenLetter-to-Minister-Azoulay-Image-Index-Bill-on-Creation-Eng.pdf>.



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

France adopted a ‘Cloud First’ policy last year. This momentum has been followed rapidly by a tender to reference public CSPs. The outcomes regarding the decision of the French procurement office will be known in December 2019. However, despite this good momentum, cloud adoption is still fragile in France from a 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.

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 cars used by independent licensed drivers who work on the platform 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.⁶³

The French DST will be applicable to gross revenues derived from certain digital services provided in France in which there is user involvement.⁶⁴ The rate is set at 3 percent of “qualifying” revenues and will concern companies with worldwide revenues of at least €750 million and French “qualifying” revenues of at least €25 million.⁶⁵ 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.⁶⁶ 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 2020.⁶⁷

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.⁶⁸ 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.⁶⁹ 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 2017.⁷⁰

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

⁶³ <https://www.dentons.com/en/insights/articles/2019/july/15/french-digital-services-tax-dst>

⁶⁴ <https://www.ev.com/gl/en/services/tax/international-tax/alert-frances-parliamentary-commission-agrees-on-digital-services-tax>

⁶⁵ <https://www.gouvernement.fr/en/gafa-tax-a-major-step-towards-a-fairer-and-more-efficient-tax-system>

⁶⁶ <http://www.oecd.org/tax/beps/>

⁶⁷ <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>

⁶⁸ <https://taxfoundation.org/digital-taxes-europe-2019/>

⁶⁹ <https://www.gouvernement.fr/en/tax-on-digital-services-an-efficacious-fiscal-justice-measure>

⁷⁰ <https://2016.export.gov/france/doingbusinessinfrance/index.asp>



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.⁷¹

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 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.⁷²

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.⁷³ 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.”⁷⁴ 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.

⁷¹ France Country Commercial Guide (CCG 2018), U.S. Commercial Service, <https://2016.export.gov/france/doingbusinessinfrance/index.asp>

⁷² <https://tai-strategie.fr/content/uploads/2020/03/dst-impact-assessment-march-2019.pdf>

⁷³ 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.

⁷⁴ Id.



On December 24, 2018, the Higher Regional Court of Saarbrücken, 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 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.

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 Tübingen 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 extends film funding levies from German to 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.

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. 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.⁷⁵

Unilateral Or Discriminatory Digital Tax Measures

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

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 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.

⁷⁵ 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>.



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).
- *Return-to-garage rule*: For-hire drivers have an obligation to return to the garage before and after each trip and are prohibited from parking their vehicle anywhere but in its designated garage.

Unilateral Or Discriminatory Digital Tax Measures

Italy's 2019 Budget included a 3 percent digital services tax closely aligned with the EU's original proposal. The tax is expected 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 gerrymandered around large U.S. tech firms. The new Italian government has also included the digital tax in its priorities. The implementation of the tax is merely administrative and could happen at any moment.

Poland

Copyright-Related Barriers

In January 2017 the CJEU in the case of *OTK v. SFP*⁷⁶ 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.

⁷⁶ C-367/15 Stowarzyszenie 'Oławska Telewizja Kablowa' v. Stowarzyszenie Filmowców Polskich, ECLI:EU:C:2017:36, European Court of Justice (January 25, 2017).



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 propiedad 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.”⁷⁷ 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.⁷⁸

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.⁷⁹ An economic study prepared by the Spanish Association of Publishers of Periodical Publications found that the result of ley de propiedad 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.⁸⁰

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

⁷⁷ 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 Propiedad 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.

⁷⁸ https://www.elconfidencial.com/tecnologia/2017-02-07/canon-aede-meneame-internet-facebook-agregadores_1327333

⁷⁹ *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>.

⁸⁰ *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>.



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.
- *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

A digital services tax of 3 percent, closely modeled after the EU proposal, was included in Spain’s budget bill for 2019. Following the G7 Finance Ministers meeting in July, Spanish officials indicated the intention to start deliberations on the digital tax bill “as soon as there is a government.”



Sweden

Copyright-Related Barriers

A recent Supreme Court ruling⁸¹ 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

In Sweden, there is uncertainty surrounding the use of U.S. cloud service providers (CSPs) because of negative legal analysis on the impact of the U.S. CLOUD Act. A quasi-governmental group (eSam) has published a series of legal analyses deeming the use of American CSPs incompatible with Swedish/EU law, suggesting that Swedish organizations are prohibited from using and procuring cloud services from foreign (mostly U.S.) providers. The effect of these statements and the associated backlash has led to a slowdown of the use of U.S. CSPs in the Swedish public sector.

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.

⁸¹ April 4, 2016, case Ö 849-15, Bildupphovsrätt i Sverige ek. för v. Wikimedia Sverige.



United Kingdom

Copyright-Related Barriers

While there is significant uncertainty related to Brexit, if the UK were to implement the just passed EU measures, 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 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 Paper⁸² that would create significant compliance issues for U.S. companies operating in the UK if it is enacted into law.

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 is continuing to pursue problematic digital tax legislation. In the UK's October 2018 Budget, the government proposed a Digital Services Tax (DST) that would apply a 2 percent tax on gross revenue linked to UK users of three types of business models: search engines, social media platforms, and online marketplaces. This proposal is narrowly targeted at U.S. technology companies. For example, the legislation excludes ads on UK news websites, but includes ads shown to UK users of social media websites or online search engines.

IA believes that a UK DST sends a strong signal to internet companies of all sizes – from SMEs to major organizations – that the UK 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

⁸² https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf



business, legal, and regulatory environment, the UK had rightly earned a reputation as a great place for U.S. firms to invest in and export to, especially internet companies aiming to export to not only UK but also European markets.

The DST puts this position at risk. Companies are likely to either reduce their exports to and investment in the UK, or divert their focus to more welcoming jurisdictions.

While the UK Treasury has indicated it recognizes the potential impact on SMEs, and has proposed a system of thresholds and exceptions designed to exempt certain companies from the DST, the proposed thresholds and exemptions will not fix the underlying problems with the proposed measure and its impact on American businesses.

Consideration must also be given to the small businesses and consumers who ultimately bear 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 SMEs and consumers, and it is those SMEs and consumers who will suffer the incidence of the tax.

The design of the DST also creates complexity in the UK tax system and leaves uncertainty for U.S. companies as to whether or not their exports would be captured by the tax, either directly or indirectly. Consequently it places a new compliance burden on companies, even if they are ultimately exempt from the tax, as significant work would be required of them to produce bespoke financial information to confirm that fact. As drafted, the DST further makes the UK a less attractive place to operate an internet business. In addition, the thresholds will also create a disincentive to grow for firms who are at the margin for exemption. IA encourages USTR to ensure that the UK and other trading partners focus their 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.

The UK's diverted profits tax⁸³ is another example of a unilateral approach to international tax policy, diverging from international treaties and the agreed rules for apportioning profits among different countries. This tax was a major step outside of the multilateral tax system, designed to privilege the UK over its trading partners. Under this policy, the UK can levy taxes on structures and payments that are not related to the UK activities, creating an impediment to cross-border investment and a significant source of uncertainty among small and medium companies with any ties to the UK market. The SMEs have to spend a disproportionate time complying with this tax policy.⁸⁴

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.

⁸³ <https://www.gov.uk/government/publications/diverted-profits-tax-changes/diverted-profits-tax-amendments>

⁸⁴ <https://www.bna.com/insight-uk-diverted-n73014483427/>



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,⁸⁵ 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

India's draft bill for a new, comprehensive data protection law, the Personal Data Protection Bill 2018 (PDPB) seeks to define principles and parameters for the Indian data economy.⁸⁶ However, in a number of respects, the bill is far more restrictive than the EU's recently enacted GDPR, which is widely considered to be the most comprehensive regulation in the data protection sphere. Along with data localization requirements, other excessive restrictions in the bill include:

- New discretionary powers to local data protection authorities (DPAs), including the ability to impose draconian penalties on foreign companies, unilaterally suspend data transfers, engage in search and seizure activities, cancel the registration of "data fiduciaries," and order the discontinuation of certain businesses or activities.
- Onerous obligations on "significant data fiduciaries," including data audits and impact assessments by DPAs; the assignment of "data trust scores" to companies and the publication of ratings on the DPA's website; and mandatory registration and record-keeping requirements.
- Potentially destructive monetary penalties linked to global turnover, uncapped compensation, and inclusion of criminal penalties and non-bailable offences.
- Definition of "sensitive personal data" to include financial data and passwords (in conflict with global best practices on privacy), and definition of a "child" to include anyone under 18 years old.

⁸⁵ 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 . . .").

⁸⁶ https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf



- An unduly tight timeline for companies (and the government itself) to implement this new law.
- Imposition of an EU-style “right to be forgotten” to be adjudicated by DPAs.

IA strongly encourages 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.

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 “personal data” in India, while subjecting “sensitive” personal data to even stricter requirements and mandating that “critical” personal data can only be processed within India. These definitions of personal data all remain very unclear and, if not addressed, will create significant market access barriers for U.S. firms doing business in India.

India is using data localization requirements to address concerns about security and law enforcement access to data. But these requirements will be counterproductive to India’s security objectives. Data localization has been shown to increase security risks and costs by requiring storage of data in a single, centralized location, making companies more vulnerable to natural 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 March 2017, the Reserve Bank of India released new guidelines that require mobile payment product providers to establish a local entity in order to access the market. This requirement isn't limited to financially regulated entities, and applies even to companies that are serving as a platform for licensed partners.

Blocking Foreign Direct Investment

The Ministry of Commerce, Government of India formed a think tank (or committee) to frame the E-Commerce Policy for India, a draft of which was released in July 2018. The think tank that drafted the policy did not have any representation of foreign companies. Indian promoted companies (comprising largely of companies which were Indian startups but now have substantial foreign equity invested in them) such as Snapdeal, Paytm, and Ola Cabs are represented on this think tank and aim to make the policy favorable to Indian companies in order to protect their interests. Some of the proposed clauses in the policy included provisions to enable founders to retain control of companies they have minority stakes in, mandatory disclosure of source codes to the government under domestic law, 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.⁸⁷

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"),

⁸⁷ 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.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=0 (reporting on the practices of the Jammu and Kashmir governments to "increasingly [use] a communication blackout to prevent unrest in the valley.").



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, proactive filtering, and compressed timelines for content removal.⁸⁸

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.⁸⁹ The government has informed the Supreme Court that it is likely to complete the 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, TRAI, issued a consultation paper on "Regulatory Framework for Over-the-Top (OTT) services."⁹⁰ There has been no response from the regulator on this paper after comments were submitted, yet it appears that the matter is still under consideration. In 2016, there were additional consultation papers on issues including net neutrality,⁹¹ VoIP,⁹² and cloud service.⁹³

⁸⁸ http://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf

⁸⁹ <https://www.livemint.com/news/india/sc-flags-tech-pitfalls-asks-centre-to-curb-social-media-misuse-1569350515906.html>

⁹⁰ 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.

⁹¹ TRAI, *Consultation Paper on Net Neutrality* (May 30, 2016), http://www.trai.gov.in/Content/ConDis/20775_0.aspx.

⁹² TRAI, *Consultation Paper on Internet Telephony (VoIP)* (June 22, 2016), http://www.trai.gov.in/Content/ConDis/20779_0.aspx.

⁹³ TRAI, *Consultation Paper on Cloud Computing* (Oct. 6, 2016), http://www.trai.gov.in/Content/ConDis/20777_0.aspx.



Many of these consultations have sought feedback on whether there is a need for regulation of OTT providers that offer such services. However, again, regulators have provided little feedback or response to industry submissions. Finally, the Ministry of Telecommunications recently released draft registration guidelines for machine-to-machine (M2M) service providers in India, with a focus on increasing regulation of M2M service providers.⁹⁴ Restrictions on U.S. Cloud Service Providers

Cloud computing services require a highly reliable, low latency underlying network. Cloud service providers face significant regulatory challenges in operating and managing data centres in India including 1) inability to buy dark 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.

Unilateral Or Discriminatory Digital Tax Measures

The industry is deeply concerned about India's adoption of an "equalization levy," which imposes an additional 6 percent withholding tax on outbound payments to nonresident companies for digital advertising services.⁹⁵ These provisions do not provide credit for tax paid in other countries for the service provided in India. In addition, the levy targets business income even when a foreign resident does not have a permanent establishment in India, and even when underlying activities are not carried out in India, in violation of Articles 5 and 7 of the U.S.-India tax treaty. And it does this by singling out one particular activity provided through one particular mode of supply: online advertising.

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

India has enacted a "substantial economic presence" tax measure that seeks to unilaterally change the definition of Permanent Establishment. It is effectively targeted at the digital sector, but may also impact other transactions outside the digital economy. This measure preempts the outcomes of the multilateral OECD process and may expose U.S. companies to double taxation.

⁹⁴ 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.

⁹⁵ Madhav Chanchani et al., *Equalisation Levy of 6% On Digital Ad: Government Finds a Way to Tax Companies Like Google, Facebook*, THE ECONOMIC TIMES (Mar. 2, 2016), <http://economictimes.indiatimes.com/news/economy/policy/equalisation-levy-of-6-on-digital-ad-government-finds-a-way-to-tax-companies-like-google-facebook/articleshow/51216310.cms>.



Indonesia

General

Indonesia's "Draft Regulation Regarding the Provision of Application and/or Content Services through the Internet" targets online services and would require platforms to take responsibility for a very broad list of content types, including content that "ruins reputation," "is contradictory to the Indonesian constitution," and "threatens the unity of Indonesia."⁹⁶ This regulation, which is part of the broader package of OTT regulations discussed below, will present significant market access barriers to U.S. providers in Indonesia.

Data Flow Restrictions And Service Blockages

The government of Indonesia has introduced a series of forced data localization measures through Ministry of Communication and Informatics Regulation 82/2012 and the more recent Draft Regulation Regarding the Provision of Application and/or Content Services Through the Internet. These measures contain numerous market access barriers, including requirements for foreign services to "place a part of its servers at data centers within the territory of the Republic of Indonesia."⁹⁷

Indonesia's GR82 data localization policy, or its revisions, continues to be a significant barrier to digital trade, and is inhibiting foreign firms' participation in Indonesian e-commerce. Indeed, U.S. firms have lost, and continue to lose, business in Indonesia from customers being told they must store their data locally. Indonesia is planning to take important steps to reform its data localization policy, including by replacing it with a data classification policy whereby only national security and intelligence data must remain onshore. This approach would be a positive step for Indonesia. However, the industry is concerned that there are no clear commitments to finalizing this revision, creating tremendous business uncertainty and increased compliance risks. IA urges USTR to strongly encourage Indonesia to move swiftly in finalizing this revision.

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.

⁹⁶ <https://www.telegeography.com/products/commsupdate/articles/2016/05/05/mcit-issues-draft-regulation-on-ott-in-indonesia/>

⁹⁷ Alexander Plaum, *The Impact of Forced Data Localisation on Fundamental Rights*, Access Now (June 4, 2014), <https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/>.



Disciplining Digital Platforms (OTT)

Indonesia plans to revive its draft regulation on Over-the-Top (OTT), renaming it a “Digital Platform” regulation. The ICT Ministry plans to issue the policy by the first half of 2020. They have begun policy research to develop a definition of “digital platform,” with the intent to classify e-commerce, fintech, healthtech, transport and travel apps, and cloud services as digital platforms. The regulation will seek to create an equal playing field between local and foreign platforms, likely requiring foreign providers to locally register, submit to screening of content, provide law enforcement access, and respect local taxation laws and regulations. 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, that 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 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 2017.

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



Overly Restrictive Regulation of Online Services

Indonesia introduced a draft law in 2016 focused on online services (“Draft Regulation Regarding the Provision of Application and/or Content Services through the Internet”) that would require data localization, creation of a local entity or permanent establishment, forced cooperation with local telecom operators offering similar services, new intermediary liability and monitoring requirements, exclusive use of a national payment gateway, and numerous other barriers that would severely impact or cripple the ability of many internet services to do business in Indonesia.⁹⁸ The compliance and enforcement provisions of these regulations would impose significant costs on both companies and the government, ultimately hampering the development of Indonesia’s digital economy.

Unilateral Or Discriminatory Digital Tax Measures

Indonesia has taken steps on taxation that significantly deviate from global norms, bilateral tax treaties, and WTO commitments. These steps include proposed requirements that would compel foreign services to create a permanent establishment in order to do business in Indonesia.⁹⁹ This process would require significant resources from online service providers, many of which are small companies that lack the necessary legal and technical resources to comply with such processes, and could have significant tax consequences that conflict with OECD multilateral principles. Furthermore, this requirement would likely violate Indonesia’s WTO commitments to allow computer and other services to be provided on a cross-border basis.

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) is considering a proposal that would extend 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, MIC is proposing that 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). A bill is likely to be submitted in the next Diet, which convenes in January 2020.

⁹⁸ 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/>.

⁹⁹ Victoria Ho, Indonesia Tells Google and Other Internet Firms to Pay Tax or Risk Getting Blocked, MASHABLE (Mar. 1, 2016), <http://mashable.com/2016/03/01/indonesia-tax-google/#bmVYs96AfsqF>.



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 US 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 2 hours.
- *Price controls*: Regulations set a minimum price floor and a maximum price ceiling for both taxis and hire cars.
- *"Return-to-garage" rule*: Hire car drivers must return to their registered place of business after completing every trip.
- *Barriers to independent taxi operators*: In order to receive a license to work as an independent taxi driver—as opposed to an affiliate of a larger taxi firm—a driver must first have 10 years of experience driving for the same taxi firm and be at least 35 years old.
- *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 engines¹⁰⁰ and some data mining activities,¹⁰¹ Japanese law today does not clearly provide for the full range of limitations and exceptions necessary for the digital environment¹⁰² – 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.

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.
- *Platform liability*: Regulations place full liability for all driver actions on the app provider company through which the driver is sourcing work.
- *Data-sharing requirement*: App providers regularly face demands to share data in real time from security and judicial agencies and without clear due process.
- *On-shoring requirements*: Technology companies seeking to operate in Jordan are required to have significant local physical presence (staff).

¹⁰⁰ Copyright Law of Japan, Section 5 Art. 47-6, <http://www.cric.or.jp/english/cli/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”).

¹⁰¹ Copyright Law of Japan, Section 5 Art. 47-7, <http://www.cric.or.jp/english/cli/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).

¹⁰² 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 snipping 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.



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.

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 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 problematically, 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

Recent draft legislation includes ambiguous requirements related to data localization.



Infrastructure-Based Regulation Of Online Services

The Ministry of ICT has started drafting a new national ICT policy in response to, among other things, the need to provide clarity on how to treat online services.¹⁰³ IA encourages USTR to monitor the development of this policy and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach.

Korea

Copyright-Related Barriers

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

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.

Data Flow Restrictions And Service Blockages

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

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

Discriminatory Or 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 frequently heavily redacted. It is also important to ensure that Korea is meeting the standards of Article 16.1.3 of the U.S.-Korea Free Trade Agreement, which requires that respondents have a reasonable opportunity to cross-examine any witnesses.

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

¹⁰³ 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>.



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, 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.

Restrictions On Cloud Service Providers

The Korean government continues to maintain a protectionist stance to keep global Cloud Service Providers (CSPs) out of the public sector market. In 2016, the Korean government and the Korea Internet and Security Agency (KISA) created a cloud security certificate (KCSC) system governing the sale of cloud into the public sector. The KCSC is a key barrier for U.S. CSPs in the Korean public sector market as U.S. companies are unable to meet four components of the certification. As a result, all central and local government ministries, affiliated public institutions, and educational institutions (from primary schools to universities) are prohibited from adopting cloud services provided by U.S. companies. In order to address the KCSC barrier, the KCSC system needs to be amended to allow Korea public sector institutions to adopt global CSPs’ services.

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.

Sharing Economy Barriers

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

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



Malaysia

Infrastructure-Based Regulation Of Online Services

In Malaysia, there have been proposals to include regulation of online services within the ambit of communications regulators. In addition, the Malaysian Communications and Multimedia Commission (MCMC) decided to assess the need for improvements to the Communications and Multimedia Act (CMA).¹⁰⁴ The U.S. government should monitor the development of these regulatory frameworks and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach. In particular, Malaysia should avoid creating market access barriers by subjecting foreign internet services and applications to telecom-specific or public utility regulations.

Mexico

Infrastructure-Based Regulation Of Online Services

To import certain products into Mexico, products must comply with certain technical regulations, or Normas Oficial Mexicana (NOMs), which contain the information, requirements, specifications, procedures, and methodologies that allow the government to set and measure parameters to avoid risks to people, animals, and the environment. As of 2010, for a small subset of products covering certain electronics, office equipment, and IT products (i.e., NOMs 001, 016, 019), Mexico is supposed to recognize lab testing from the country of export as “equivalent” to what is required by its NOMs for those three categories of products, thereby allowing those products to be imported without additional testing. However, for certain electronics products, Mexico is continuing to require additional testing prior to import. The U.S. government should work with Mexico to enforce existing equivalence agreements, as well as expand such agreement to cover additional NOMs, such as NOM-003 (Safety Testing for Electrical Products).

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.

¹⁰⁴ *Amendment to Communications and Multimedia Act 1998 in March*, ASTRO AWANI (Feb. 22, 2016), <http://english.astroawani.com/malaysia-news/amendment-communications-and-multimedia-act-1998-march-95481>.



- *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.

Copyright-Related Barriers

Mexico currently does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Without the USMCA, digital creators and innovators in Mexico must rely on a general provision that allows the use of works where there is no economic profit,¹⁰⁵ which increases legal risk and costs for U.S. internet and technology companies seeking to offer commercial services in Mexico.

Without the USMCA, Mexico does not have a comprehensive ISP safe harbor framework covering the full range of service providers and functions and prohibiting the imposition of monitoring duties.

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.

¹⁰⁵ Mexico Federal Law on Copyright (as amended, 2016), Art. 148-151.



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 marketplace 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 of New Zealand's 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 U.S. law, 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.

Data Flow Restrictions And Service Blockages

The Guidelines for Nigerian Content Development in ICT require both foreign and local businesses to store all of their data concerning Nigerian citizens in Nigeria, and establish local content requirements for hardware, software, and services. These rules will significantly increase market access barriers for internet companies seeking to serve the Nigerian market.

On February 5, 2019, the Nigerian National Information Technology Development Agency (NITDA) released a draft of the Nigerian Data Protection Regulation, which applies to natural persons residing in Nigeria and Nigerians abroad, and has been described as being inspired by the GDPR. Under the draft, companies must comply with regulations that include publishing privacy policies for the public, publishing their data protection policies within three months, designating a Data Protection Officer, and conducting a detailed audit within six months after the issuance. Failing to comply can lead to fines under the following categories: More than 10,000 data subjects: 2 percent annual gross revenue or 10 million Naira (\$28,000) (whichever is greater) or less than 10,000 data subjects: 1 percent annual gross revenue or 2 million Naira (\$5,500) (whichever is greater).

IA urges USTR to engage with counterparts in Nigeria to highlight and resolve these barriers.



Pakistan

Overly Restrictive Regulation of Online Services

The Pakistan Telecommunications Authority published the final draft of a regulatory framework for online services.¹⁰⁶ The policy framework focuses on regulation of “payment infrastructure, taxation issues, consumer protection in the digital environment, issues relating to logistics, and data ownership/sovereignty and data localization.” IA encourages USTR to monitor the development of this policy and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach, and that encourages innovation and investment.

Unilateral Or Discriminatory Digital Tax Measures

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

Panama

Burdensome or Discriminatory Data Protection Regimes

In March 2019, Panama has 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 is, however, very broad. This could create a de facto data localization mandate for all data, even if this is not the objective 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.

¹⁰⁶ <http://www.commerce.gov.pk/wp-content/uploads/2019/07/Final-Draft-E-Commerce-Policy-Framework-of-Pakistan.pdf>



- *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.
- *Cash payment prohibition:* Drivers working with app-based transportation services are prohibited from accepting cash payment, although no other type of transportation provider is similarly prohibited.
- *Geographical restriction:* App-based transportation services cannot provide their services in six out of the 10 provinces. This restriction does not apply to other modes 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 environment¹⁰⁷ – 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.¹⁰⁸

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.¹⁰⁹ IA urges USTR to address this significant market access barrier for U.S. services and push for full implementation of the agreement.

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 utilise 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.

¹⁰⁷ Legislative Decree No. 822 of April 23, 1996, Title IV Chapter 1.

¹⁰⁸ Legislative Decree No. 822 of April 23, 1996, Title IV Chapter 1, Art. 50.

¹⁰⁹ https://ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file437_9548.pdf



Russia

Copyright-Related Barriers

Russia has taken additional steps to broaden the scope of an already unbalanced set of copyright enforcement measures. The “Mirrors Law,” which came into effect on October 1, 2017, extends Russia’s copyright enforcement rules into new domains by requiring search providers to delist all links to allegedly infringing websites within just 24 hours of a removal request. The law also applies to so-called “mirror” websites that are “confusingly similar” to a previously blocked website.

In practice, this law has resulted in overbroad removal and delisting requests for general-purpose websites that would not be subject to removal under Section 512 of the DMCA or other parts of U.S. copyright law. As USTR has noted elsewhere, 24 hours is an insufficient amount of time for service providers to review these types of requests. In addition, the principle of removing entire websites that include a proportionally minor amount of potentially infringing content was squarely rejected by the U.S. Congress during debate over the Stop Online Piracy Act in the 112th Congress.

IA urges USTR to engage with counterparts in Russia to address this measure, which is likely to generate market access barriers for U.S. internet services.

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.



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

Filtering, Censorship, and Service-Blocking

Russia has implemented a new site-blocking law, giving additional power to regulators over online services, including the power to demand that intermediaries block certain sites or certain types of content.¹¹⁰ 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 law No. 31-FZ “On Amending Article 15-3 of Federal Law” criminalizing users spreading misinformation online and criminalizes insults of government officials. The law targets 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. Critics specifically oppose Article 19 in the law, which allows public officials to decide what counts as “truth.”

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 provide the installation of network equipment that would be able to identify the source of web traffic and block banned content. The law will take effect November 1, 2019.

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.

¹¹⁰ 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.

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.¹¹¹ 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.

¹¹¹ 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/>.



Singapore

On May 9, 2019, Singapore signed into law the Protection from Online Falsehoods and Manipulation Bill (Bill No. 10/2019) as a measure to curb misinformation. It is reported that 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. 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.” The legislation was proposed after the Law Ministry stated that Facebook declined to take down a post that 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 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.

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:* Pending amendments to the National Land Transport Act would 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.



Taiwan

Discriminatory Of Non-Objective Application Of Competition Regulations

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

Sharing Economy Barriers

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

- *License cap:* Taxi licenses are capped for taxi companies and taxi fleets and the growth in their number is pegged to the growth of each city/county's population or road expansion. (There is no license cap for individual taxi operators' licenses or for rental car licenses.)
- *Minimum/maximum price restrictions:* Prices for taxis are regulated by local governments and constrained within a minimum price floor and maximum price ceiling. While taxis operating under the new Multi-Purpose Taxi scheme face only a price floor and not a price ceiling, access to the scheme is limited to only those taxi drivers who have an exclusive affiliation with a single taxi dispatch company and not those who operate independently or as members of a co-operative—forming a taxi dispatch company requires meeting a NTD \$5 million capital requirement.
- *Identification requirement:* Although a rider being driven by a rental car driver is not renting a car in the sense contemplated by legacy car rental regulations, the service is nevertheless governed by those regulations. As a result, the rider/renter must provide the rental car company with her/his national identification number, as if they were renting the car to drive herself/himself. The national identification number is a very sensitive piece of personal information, akin to the Social Security number in the U.S. Requiring riders to turn it over has a severe deterrent effect on the use of rental car driver services.

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.



Thailand

Data Flow Restrictions And Service Blockages

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

Non-IP Intermediary Liability 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 such they are assisting or facilitating the offense.¹¹² 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.¹¹³ Such rules have resulted in the blockage of U.S. online services in Thailand.

Turkey

Data Flow Restrictions And Service Blockages

The Communiqué 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.

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.

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. This CSPs 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

¹¹² <https://www.law.uw.edu/media/1423/thailand-intermediary-liability-of-isps-defamation.pdf>

¹¹³ <https://www.eff.org/deeplinks/2012/05/suspended-sentence-good-news-thai-webmaster-jiew-threat-freedom-expression-remains>



information – as well as genetic and biometric data shall be stored domestically in a safe environment. Another sector specific regulation that will bring localization requirements for companies in the financial services industry is the draft regulation on the Information System of Banks and Electronic Banking Services prepared by the Banking Regulation and Supervision Agency, an implementation period will run until January 2020. This regulation requires banks and financial services to keep their primary information systems (production data) within the country.

Unilateral Or Discriminatory Digital Tax Measures

The Ministry of Finance and Treasury is planning to send a digital service tax bill to the Turkish Parliament in 2019. The alleged digital service tax of 7.5 percent is expected to be applied to companies that do not have a permanent establishment in Turkey which provide their services through the internet. The bill taxes revenue from a wide range of digital services. It is the industry's understanding that the Ministry does not plan to wait for OECD negotiations to conclude before passing this bill.

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.¹¹⁴ These problems have not been effectively addressed in the past year.¹¹⁵ 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.¹¹⁶ 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.

United Arab Emirates

Infrastructure-Based Regulation Of Online Services

In 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.¹¹⁷ 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

¹¹⁴ <https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf>.

¹¹⁵ See Tetyana Lokot, New Ukrainian Draft Bill Seeks Extrajudicial Blocking for Websites Violating Copyright, Global Voices (Feb. 1, 2016), <https://advoc.globalvoices.org/2016/02/01/new-ukrainian-draft-bill-seeks-extrajudicial-blocking-for-websites-violating-copyright/>

¹¹⁶ Law of Ukraine “On State Support of Cinematography in Ukraine”

¹¹⁷ 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 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>.



to insist that only national providers can provide these forms of communications services.¹¹⁸ These restrictions are impeding 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.¹¹⁹

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.

- *Vehicle requirements:* In Dubai, for-hire vehicle companies must own a minimum of 20 vehicles and only 10 percent of their vehicles can have a value of less than \$50,000 USD. As a result, the minimum cost of setting up a for-hire vehicle company is approximately \$1 million.
- *Minimum price requirement:* For-hire transportation providers must charge 30 percent more than taxis.
- *Data-sharing requirement:* Companies providing transportation apps are required to share data in real time, via integration into government computer systems.

Uruguay

Overly Restrictive Regulation of Online Services

Uruguay is currently considering a bill to regulate digital platforms and services.¹²⁰ 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

¹¹⁸ See Mary-Ann Russon, *supra* note 98.

¹¹⁹ 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 ADVOC (Sept. 7, 2016), <https://advoc.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/>.

¹²⁰ 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/>.



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.¹²¹

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

The Law on Cybersecurity was passed by the National Assembly (NA) on June 12, 2018 containing vague data localization and representative office requirements. Vietnam's Ministry of Public Security has issued multiple draft versions of the Implementing Decree of the Cybersecurity Law that will specify which companies must locate their data in Vietnam. Under the latest draft, there are clauses requiring all companies to comply with data handover, content takedown, and domain name seizure requests. Companies who do not make efforts to comply could be served a data localization notice by the Ministry of Public Security (MPS). These requirements are concerning for service providers such as data processors and ISPs who do not have visibility into data stored on their platform, putting assets and data held by U.S. companies at risk of seizure, infringement of trade secrets and intellectual property rights, and loss of personal data of U.S. persons. The U.S. Government should encourage Vietnam not to use "data localization" as the punishment for non-compliance, to have law enforcement requests only apply to data controllers and required to be served through existing international legal processes.

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 below, Vietnam's Law on Cyber Security includes significant data localization requirements.

¹²¹ Law on Intellectual Property (as amended, 2009), Art. 25, 26.



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.¹²²

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 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.¹²³

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.¹²⁴

¹²² Draft Decree Amending Decree 72/2013-ND-CP on the Management, Provision and Use of Internet Services and Information Content Online.

¹²³ 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 its safe harbor framework does not include any requirements to monitor content and communications.

¹²⁴ Circular Regulates OTT Services, VIETNAM NEWS (Nov. 15, 2014), <http://vietnamnews.vn/economy/262825/circular-regulates-ott-services.html#qvpySzIcYMz25vCl.97>



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.

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.¹²⁵

¹²⁵ 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 seeks 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.

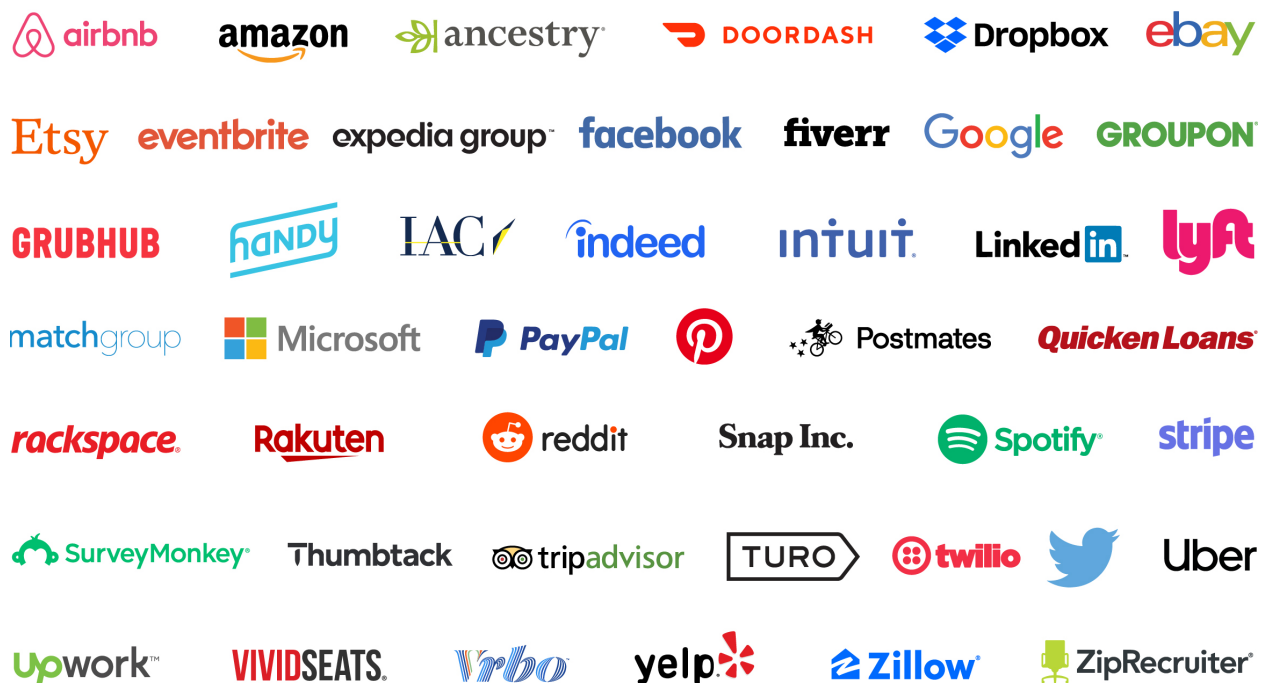
Unilateral Or Discriminatory Digital Tax Measures


Numerous countries in the region have already implemented or are in the process of putting place 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.





**We are the
unified voice
of the internet
economy**

www.internetassociation.org