Internet Association

Submission For The 2022 USTR National Trade Estimate Report

Docket No. USTR-2021-0016

Table of Contents

America's Digital Leadership and Foreign Barriers to Digital Trade

On behalf of America's leading internet companies, Internet Association (IA)[1] is pleased to submit the following comments to the Trade Policy Staff Committee (Docket Number USTR-2021-0016) for consideration as the Office of the United States Trade Representative (USTR) prepares the 2022 National Trade Estimate Report (NTE).

America's global technology leadership was built and depends upon a U.S. digital policy framework that provides certainty and flexibility for internet companies, large and small, to invest and develop innovative solutions that benefit American consumers, entrepreneurs, and workers.[2] Today, businesses and entrepreneurs in every state and every community across the U.S. use the internet to sell and export across the globe, with digitally enabled services accounting for nearly 60 percent of all U.S. services exports.[3]

Moreover, the U.S. response to the COVID-19 pandemic has further cemented the reliance of consumers and businesses, especially small and medium sized businesses, on internet services, platforms, and marketplaces to maintain economic stability and growth. Notably, one-third of small businesses report that they would not have survived the pandemic without digital tools.[4] And over 40 percent of small businesses report that digital tools helped them find new customers locally and outside the U.S.[5]

The digital economy is an American success story that is increasingly under threat as countries around the world seek to undermine U.S. leadership in the digital economy and the global nature of the free and open internet. In these comments, IA highlights examples of the concerning and increasing commercial and trade barriers worldwide that threaten the U.S. digital economy and a free and open internet, particularly in growing and innovative sectors, such as cloud, online marketplaces, social media, and financial services. Three key sets of issues merit a particular focus.

First, there is a growing trend of **digital protectionism** – with governments using 'techlash' as an excuse to restrict or exclude U.S. digital services and transfer value from U.S. to foreign businesses. For example, countries are developing new regulations – such as the EU's Digital Markets Act – that target U.S. platforms and depart from long-standing norms on due process, the rule of law, and the protection of privacy, security, and intellectual property. Notably, the EU's Digital Services Act and Digital Markets Act, as well as restrictions on cloud services, artificial intelligence, and increasingly narrow and restrictive interpretations of the General Data Protection Regulation (GDPR), are inhibiting U.S. digital companies from using personal data in innovative, pro-consumer ways. EU officials are also pursuing restrictions on cloud services, artificial intelligence, and data that have the stated purpose of achieving "digital sovereignty" and creating a "new empire" of European industrial powerhouses to resist American rivals.

Many other countries are also imposing or pursuing restrictive measures that target U.S. technology companies, leaving domestic competitors free to innovate. Notably, India is considering mandatory sharing of non-personal

[1] Internet Association is the only trade association that exclusively represents leading global internet companies on matters of public policy. The Association's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. More information at https://internetassociation.org/.

[2] Online platforms support 425,000 U.S. jobs and $44 billion in U.S. GDP annually. Internet Association, *Economic Value of Internet Intermediaries and the Role of Liability Protections*, (June 5, 2017), *available at* https://internetassociation.org/wp-content/uploads/2017/06/Economic-Value-of-Internet-Intermediaries-the-Role-of-Liability-Protections.pdf.

[3] Daniel S. Hamilton & Joseph Quinlan, *The Importance of Digital Services to the U.S. and European Economies*, The Wilson Center, (Apr. 8, 2021), *available at* https://www.wilsoncenter.org/article/importance-digital-services-us-and-european-economies.

[4] Connected Commerce Council, *How Digital Tools Power Small Businesses Amid COVID-19, available at* https://digitallyempowered.connectedcouncil.org/.

[5] *Id.*

data in their personal data protection bill, and Australia's News Media and Digital Platforms Mandatory Bargaining Code requires U.S. digital companies to carry domestic Australian news content, transfer revenue to Australian competitors and disclose proprietary information related to private user data and algorithms.[6] In Korea, the National Assembly banned mobile application platforms from requiring that in-app payments be made on their own payment systems, a global-first move that affected only two U.S. digital companies and none of their Korean competitors.

As another example of digital protectionism, an increasing number of foreign trading partners have imposed unilateral digital services taxes (DSTs), unfairly targeting U.S. digital companies with narrowly tailored tax measures that exclude domestic competitors from their scope. The OECD and nearly 140 countries' recent commitments to a new agreement to reform international taxation rules, which includes a commitment to roll back and halt the introduction of discriminatory DSTs, is a welcome step in the right direction.[7] The recent agreement that the U.S. reached with Austria, France, Italy, Spain and the U.K. to implement this framework, which includes commitments by these countries to revoke their DSTs, is also to be welcomed.[8] The U.S. should continue working actively to persuade countries with DSTs to repeal them, including through use of Section 301 for countries, such as India and Turkey, that have not committed to doing so. USTR should also be prepared to initiate new Section 301 investigations if additional countries impose their own DSTs.

Second, a proliferation of **online content regulation, censorship, and surveillance laws** is limiting freedom of expression and market access.[9] Some of these content restrictions mirror the Chinese internet regulatory framework, and sharply diverge from free and open internet principles long championed by the U.S. While issues such as online harms and misinformation are serious and legitimate public policy concerns, some countries have sought to use these concerns, or the COVID-19 pandemic itself, as an excuse for introducing invasive backdoor regulations to restrict speech and market access.

Across the globe –from Russia and Turkey to Vietnam, India, and Indonesia – countries have implemented laws with vague definitions, criminal penalties for employees of U.S. companies, and expanded powers for authorities that threaten freedom of information and undermine the rule of law. The censorship threats from these new laws can be both overt and more subtle – for example, Indonesia's new laws require digital services providers to provide the government with access to user data and systems without a need for a court order. Such laws, coupled with high civil and criminal penalties for non-compliance, are leading to over-removal and censorship of legitimate content, including political speech.

U.S. digital services companies are faced with increasingly difficult choices as to how to operate in these markets. These measures are resulting in reduced market access for U.S. digital services, impacting both U.S. commercial opportunity abroad and opportunities for values-based U.S. digital leadership.

---

[6] Comments of Internet Association, Submission on The Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2020, (Jan. 15, 2021) (noting that "[t]he Code is fundamentally discriminatory towards U.S. companies, sets a harmful global precedent, and undercuts critical principles of an open internet."), *available at* https://internetassociation.org/files/ia_comments-on-australian-news-media-bargaining-code_1-2021_trade-pdf/.

[7] OECD, *International Community Strikes a Ground-Breaking Tax Deal for the Digital Age*, (Oct. 8, 2021), *available at* *https://www.oecd.org/tax/international-community-strikes-a-ground-breaking-tax-deal-for-the-digital-age.htm* (last visited Oct. 16, 2021).

[8] US Department of Treasury, Joint Statement from the United States, Austria, France, Italy, Spain, and the United Kingdom, Regarding a Compromise on a Transitional Approach to Existing Unilateral Measures During the Interim Period Before Pillar 1 is in Effect, (Oct. 21, 2021), available at https://home.treasury.gov/news/press-releases/jy0419.

[9] Comments of Internet Association, U.S. International Trade Commission Investigation on Foreign Censorship, (July 22, 2021), *available at* https://internetassociation.org/files/ia_foreign-digital-censorship-usitc-investigation-no-332-585_july-2022_trade/ (noting that "[d]igital policies are increasingly being used by governments around the world to censor citizens, which harms U.S. digitial companies ability to operate.").

Finally, increased **digital fragmentation** is impacting U.S. businesses' ability to scale globally. Fragmented cross-border data transfer regimes are a core component of this problem. The lack of resolution on a meaningful U.S.-EU data transfer mechanism has put at risk the ability of transatlantic companies to transfer data between the U.S. and EU, threatening trillions in transatlantic trade.[10] At the same time, in Asia, the absence of a supranational body or multilateral forum has resulted in a patchwork of digital regulatory frameworks that is increasingly fragmented, including when it comes to regulation of cloud technology in the financial services industry. This presents significant regulatory challenges for U.S. technology firms and financial institutions as they seek to enter new markets in Asia.

To mitigate the threat these issues pose to the U.S. economy, including consumers, entrepreneurs, and workers, USTR and the Biden administration should continue to prioritize strategic engagement with U.S. trading partners, promote U.S. competitiveness through leadership on digital trade and reassert U.S. multilateral leadership.[11] Specifically, USTR should use trade and other bilateral agreements to fight for the adoption of America's digital framework across the world and ensure equal access to the internet for all people; pursue inclusive digital trade rules with trusted partners in the Indo-Pacific region[12]; use the U.S.-EU Trade and Technology Council as a forum to encourage the free flow of data, eliminate digital market access barriers, and identify future approaches to digital policy; and continue to use its Section 301 authority to mitigate the threat of DSTs and other discriminatory digital measures.

IA appreciates the strong steps that USTR took on these issues in the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Japan Digital Trade Agreement, as well as in its submissions to the World Trade Organization's e-commerce talks, but there is more to be done. IA looks forward to continuing to support USTR and the Biden administration's efforts to maintain U.S. digital leadership by driving a values-based approach to digital trade that protects American workers, consumers, and businesses by making digital trade a top priority in the 2022 NTE Report and in its overall trade agenda.

---

[10] Thousands of companies from all industries and of all sizes are potentially affected, across technology, financial services, healthcare, transportation, and many other sectors – ultimately threatening to undermine $7.1 trillion in transatlantic trade and investment. *See* U.S. Dept. of Commerce, *U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows*, (July 16, 2020), *available at* https://2017-2021.commerce.gov/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.html; *See also*, Hamilton, Daniel S., and Quinlan, Joseph P., *The Transatlantic Economy (2021): Annual Survey of Jobs, Trade and Investment between the United States and Europe*, (2021), II, *available at* https://www.amchameu.eu/sites/default/files/publications/files/transatlanticeconomy2021_fullreporthr.pdf (reporting that the total transatlantic "commercial sales" were $6.2 trillion in 2020).

[11] Letter from BSA | The Software Alliance, Computer and Communications Industry Association, Information Technology Industry Council (ITI), Internet Association, and the National Foreign Trade Council, *Promoting U.S. Global Leadership and Innovation: Digital Trade Priorities for the first 180 days*, (Jan. 21, 2021), *available at* https://internetassociation.org/news/coalition-of-tech-business-groups-offer-recommendations-to-biden-harris-administration-to-advance-u-s-global-leadership-through-digital-trade/.

[12] Multi-Association Letter to USTR Ambassador Tai on Pacific Digital Trade Agreements, (Sept. 10, 2021), *available at* https://internetassociation.org/files/multiassn_letter-ustr-amb-tai_pacific-digital-trade-agreements_09102021/.

Foreign Digital Trade Barriers by Issue

Data Flow Restrictions

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 foreign jurisdictions.

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.[13] These and other foreign governments frequently cite concerns about security, privacy, and law enforcement access to justify their localization measures, but other countries – including the U.S. – 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.

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. Specifically, the U.S. should 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.

Discriminatory Digital Sales Taxes (DSTs)

An increasing number of foreign trading partners are proposing or maintaining discriminatory revenue taxes on digital services provided by U.S. technology firms. These digital services taxes are narrow in scope and are specifically designed to target U.S. digital companies while insulating foreign competitors from the scope of taxation. In many cases, these taxation measures contradict longstanding global consensus-based practices (e.g., by taxing gross revenues instead of income) and result in double taxation on American businesses. Unfortunately, these tax regimes are on the rise globally.

Most 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. In addition, by taxing gross revenue instead of profits, DSTs do not account for real costs of doing business, such as research and development or capital expenditures. DSTs increase the cost of capital and discourage investment and innovation for all in-scope companies and particularly those in loss positions or with low margins. The DSTs are often arbitrary not just in their scope and rate but also their taxable base, as many DSTs focus on user participation which results in taxation of activity that does not generate any actual realized or recognized income. Such a departure from fundamental concepts like taxing net profit or realized income is a concerning precedent that further supports the need for international consensus.

[13] In 2018, for example, 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.

IA agrees with policymakers that global tax rules should be updated for the digital age, but discriminatory go-it-alone taxes targeted against U.S. firms are not the right approach. Consequently, IA welcomed the recent agreement by the OECD and the nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights. When fully implemented, the agreement will provide certainty for internet companies and improve the digital economy for internet users worldwide. Unilateral DSTs are inconsistent with this multilateral initiative and the U.S. should continue to press governments and jurisdictions that are currently maintaining DSTs to repeal them.

In this connection, the Section 301 investigations that USTR conducted with respect to DSTs adopted or under consideration by France, Austria, Brazil, the Czech Republic, the EU, India, Indonesia, Italy, Spain, Turkey, and the UK played an important role in driving the OECD talks to conclusion. The recent agreement that the U.S. reached with Austria, France, Italy, Spain and the U.K. to implement this framework, which includes commitments by these countries to revoke their DSTs, is a welcome step to ending this discriminatory practice.[14] The U.S. should continue working actively to persuade countries with DSTs to repeal them, including through use of Section 301 for countries, such as India and Turkey, that have not committed to doing so. USTR should also be prepared to initiate new Section 301 investigations if additional countries impose their own DSTs.

Online Content Restrictions and Surveillance

Countries around the world are increasingly proposing and enacting digital laws intended to censor their citizens and push back on the global nature of the free and open internet. Many of these policies are in direct conflict with Article 19 of the Universal Declaration of Human Rights– which states that everyone has the right to seek and receive news and express opinions– as well as Article 20, and the general international requirements of legality, necessity, and proportionality. [15]

Over the past year, some foreign governments have devised new ways of targeting U.S. digital companies as a way to limit their citizens' access to information. Other countries are adopting policies at odds with the U.S. digital economy, and these nations are also actively pressuring their trading partners to adopt such policies. China's recent "Global Initiative on Data Security" is one example of China's desire to promulgate a vision of the internet and digital trade that runs contrary to U.S. interests and values. African nations have increasingly taken to blocking social media access during protests and contentious elections. Countries such as India, Brazil, and Egypt have moved forward with website blocking, or even shutting down internet access, as a way to censor citizens.[16] In 2021, countries such as Uganda and Nigeria have been at the forefront of partial platform bans and total internet shutdowns.

The digital industry is also finding increasing censorship pressure coming from traditional allies. Over the last few years, censorship laws have been introduced in places such as Germany with the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG), the UK with the Online Harms bill, Australia with its Sharing of Abhorrent Material law, the EU with the DSA, and most recently Canada's proposed online safety bill. This proliferation of censorship laws by major U.S. allies is deeply concerning to the digital industry and has a significant economic and operational impact on U.S. businesses of all sizes.

In the global race to set the rules for the digital economy, the U.S. government should use trade and other bilateral deals to fight for the adoption of America's digital framework across the world and ensure equal access to the internet for all people.

---

[14] US Department of Treasury, Joint Statement from the United States, Austria, France, Italy, Spain, and the United Kingdom, Regarding a Compromise on a Transitional Approach to Existing Unilateral Measures During the Interim Period Before Pillar 1 is in Effect, *(*Oct. 21, 2021*), available at* https://home.treasury.gov/news/press-releases/jy0419.

[15] United Nations, *Universal Declaration of Human Rights*, *available at* https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[16] In 2020, there were at least 155 documented internet shutdowns in 29 countries. This follows 33 countries that shut down the internet in 2019 and 25 in 2018. Access Now, *Internet shutdowns report: Shattered dreams and lost opportunities — a year in the fight to #KeepItOn*, (Mar. 3, 2021), *available at* https://www.accessnow.org/keepiton-report-a-year-in-the-fight/.

Discriminatory Competition Regulations

An increasing number of countries are enacting discriminatory competition regulations that effectively target U.S. technology companies in service of industrial policy goals. Germany has enacted a new competition law that allows the German Federal Cartel Office to subject U.S. platforms to prohibitions and penalties even if there has been no showing of an abuse of a dominant market position. Chinese competition regulators continue to use the Anti-Monopoly Law (AML) to intervene in the market against foreign companies, including in cases where there is no evidence of abuse of market power or anti-competitive harm. The proposed EU Digital Markets Act – which the EU describes as "complementary" to competition law – would impose unprecedented new rules solely or primarily on prominent U.S. technology companies, while failing to impact rivals in Europe, China, and other markets. These types of protectionist measures depart from global competition norms, and IA urges the U.S. government to identify them in the 2022 NTE Report.

Unbalanced Copyright Restrictions

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

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

USTR should highlight these issues to encourage the adoption of the U.S. copyright framework abroad, and discourage countries from using 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.[17] Unfortunately, foreign trading partners lack these innovation-oriented rules, which limit the export opportunities for U.S. industries in those markets.

In addition, Section 512 of the Copyright Act, as enacted by the DMCA, is a foundational law of the U.S. internet economy. It provides a 'safe harbor' system that protects the interests of copyright holders, online service providers, and users, imposing responsibilities and rights on each. Safe harbors are critical to the functioning of cloud services, social media platforms, online marketplaces, search engines, internet access providers, and many other businesses. Weakening safe harbor protections would devastate the U.S. economy, costing nearly half a million U.S. jobs.[18] And yet, key trading partners that have expressed obligations to enact ISP safe harbors under trade agreements have failed to do so, including Australia, Colombia, and Peru.

---

[17] CCIA, *Fair Use in the U.S. Economy*, 2011, http://www.ccianet.org/wp-content/uploads/library/CCIA-FairUseintheUSEconomy-2011.pdf (noting that 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).

[18] Internet Association, *Eliminating Internet Safe Harbors Would Hurt the Economy,* http://internetassociation.org/wp-content/uploads/2017/06/NERA-Intermediary-Liability-Two-Pager.pdf (last visited Oct. 20, 2021).

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

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

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, many of which provide their services to a global audience, and across jurisdictions, believe trust is fundamental to their relationship with their users and customers.[19] 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. Therefore, 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. Additionally, they have developed numerous tools and features to enable internet users to manage the personal information they share, as well as their online experiences.

In order to ensure that U.S. companies can continue to provide their products and services to users and consumers anywhere in the world, IA urges USTR to ensure that privacy and data protection regulations are implemented in an objective and non-discriminatory way. A good example on this matter is the reference to the APEC Privacy Framework in the USMCA, to ensure that the parties will take these privacy principles into account when facilitating the cross-border transfer of data in an informed (to the data subjects) and secure way.

In addition, it is important to encourage mechanisms that promote compatibility between different privacy regimes, as opposed to unilateral regulations that fragment the global data regulatory landscape and act as de-facto non-tariff trade barriers for US companies. Where regulations fall short of this standard, IA encourages USTR to identify these issues in the 2022 NTE as key impediments to digital trade.

[19]Internet Association, *IA Privacy Principles for a Modern National Regulatory Framework*, (Nov. 13, 2018), *available at* https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/.

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.

USTR should identify these complex customs regimes as key impediments to digital trade in the 2022 NTE and work with foreign countries to modernize these antiquated and overly burdensome systems. USTR should also work to fully implement the USMCA, including provisions related to tax and duty collection and procedures for low value shipments that do not lead to additional obstacles for small businesses exporting to Canada and Mexico.[20]

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 and moderate 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. The situation has not yet improved, even while 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 previous NTE reports. 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.

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

Traditional 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.

While "over-the-top" (OTT) services play key roles in the digital economy,[21] 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 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,

[20] Internet Association, *Statement on the U.S.-Mexico-Canada Agreement,* (Oct. 3, 2018), *available at* https://internetassociation.org/us-mexico-canada-agreement/.

[21] Each 10 percent increase in the usage of these services adds approximately $5.6 trillion to U.S. GDP. WIK, *The Economic and Societal Value of Rich Interaction Applications (RIAs),* (2017), *available at* http://www.wik.org/fileadmin/Studien/2017/CCIA_RIA_Report.pdf.

and a variety of regulatory fees. Such special regulation is not always appropriate for online services, where there are few barriers to new market entrants and low switching costs. While often couched as “level playing field” proposals, these initiatives serve to protect incumbent businesses, impede trade in online services, and make it substantially more difficult for U.S. internet firms to export their services.

To maintain U.S. leadership in this area, USTR should 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. USTR should also continue working to introduce disciplines on OTT regulations into its trade negotiations.

Foreign Digital Trade Barriers By Country

Argentina

Copyright-Related Barriers

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

Customs Barriers To Growth In E-Commerce

In recent years the government of Argentina ("GOA") has sought to reform the customs agency and has made positive strides. In 2016, the GOA implemented the Comprehensive Import Monitoring System (SIMI) in order to promote competitiveness and facilitate trade, while maintaining sufficient controls to manage risks. The SIMI established three different low-value import regimes (Postal, Express, 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. This creates serious roadblocks for U.S. companies seeking to export to Argentina, because 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. In addition, while import certificates/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 import regime and the inability to know how many shipments a customer has already received.

Extended Timelines for Pre-Shipment Licenses

Imports to Argentina are subject to pre-shipment licenses for certain IT and telecommunication goods. There are two types of licenses: automatic licenses, approved within 2-3 days; and non-automatic licenses, approved within 7-10 days. On September 17, 2021, the GOA published a regulatory change through the Federal Administration of Public Revenue and Customs (AFIP) and Secretary of Industry, Economy and Foreign Trade Administration (SIECyGCE) that established an increase of response time for non-automatic licenses from 10 days to 60 days. This change threatens to result in delays to the issuance of such licenses, and in turn to delays in inbound shipments.

Sharing Economy Barriers

Some cities in Argentina, such as Buenos Aires, are creating barriers to sharing economy services. For example, drivers seeking to provide app-based transportation services outside of the traditional taxi industry may be required to be licensed under the for-hire vehicle category, among other restrictions.[22] 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.

Unilateral Or Discriminatory Digital Tax Measures

In recent years, the GOA has applied a series of capital controls and new tax measures to the consumption of imports in an effort to make it more challenging for Argentine citizens to import goods and services. On October

[22] Other restrictive examples include a supply cap of 2,500 for-hire vehicles, requiring all for-hire vehicles to be affiliated with a for-hire agency and work exclusively for that agency, requiring for-hire vehicles to return to their registered place of business between trips, and permitting for-hire vehicles only to be solicited by either a phone call or email.

28, 2019, the Central Bank established a limit of $200 per month that citizens were able to access through their bank accounts, limiting the amount of money those citizens could use to import goods and services. On December 23, 2019, the executive branch issued Decree 99/2019, implementing a temporary 30percent tax ("PAIS tax") on the purchase of foreign currency and purchases made online invoiced in a foreign currency, among other things. And in August 2020, AFIP issued a revised opinion stating that a non-resident provider can be deemed of Argentine source even if its services are not performed in Argentina. This new opinion is contrary to a previous ruling by AFIP, in December of 2017, and conflicts with Article 5 of the Income Tax Law (ITL) and Article 9 of its Regulations. Based on this new opinion, services rendered by non-resident entities now fall within Article 14 of the ITL's scope and therefore an effective withholding rate of 17.5 percent applies to payments made by local customers for such services. In addition, on September 16, 2020, the Central Bank introduced a new 35percent tax on foreign currency purchases, including on cross-border transactions made with credit cards, to "discourage the demand for foreign currency."

In combination, these controls and taxes are making it increasingly difficult, and at times impossible, for foreign companies to sell to Argentine customers. For example, if the price of a digital service is 100 pesos, the customer pays at least 164 pesos, while the service provider receives only 82.5 pesos (not including transaction fees).

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 (analogous to 17 U.S.C. § 512). Australia has failed to comply with this commitment. Australia's implementation of this obligation is far narrower than required — notably, 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).[23] Instead, only a narrower subset of "service providers" are covered under Australian law,[24] rather than the broader definition of "internet service providers" in the AUSFTA. The lack of full coverage under this safe harbor framework creates significant liability risks and market access barriers for internet services seeking access to the Australian market. As a consequence, the law's application of intermediary protection is mainly limited to Australia's domestic broadband providers. IA urges USTR and others in the U.S. government to engage with Australian counterparts to make necessary adjustments to Division 2AA of the Copyright Act to bring this safe harbor into compliance with AUSFTA requirements.

In June 2018, the Australian Parliament amended the Copyright Act's provisions on safe harbors. The amendments expand the intermediary protections to some service providers including organizations assisting persons with a disability, public libraries, archives, educational institutions, and key cultural institutions —

[23] Copyright Act (1968), Part V Div. 2AA.

[24] Section 116ABA of the Copyright Amendment (Service Providers) Act (2018).

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.[25] 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.[26] 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.[27] The Australian Government has indicated that it anticipates these changes will only affect two U.S. companies.[28] 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 (well-established) principles-based fair use exception."[29]

Non-IP Intermediary Liability Restrictions

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

The Criminal Code Amendment (Sharing of Abhorrent Material) Act was rushed through Australia's Parliament in early 2019 with no public consultation, putting in place disproportionate and ambiguous provisions targeting the removal of online terrorism content.[30] The Act applies to an excessively broad range of technology companies, and has increased compliance risks for U.S. based social media, 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.[31]

---

[25] Copyright Amendment (Service Providers) Act (2018), *available at* https://www.legislation.gov.au/Details/C2018A00071.

[26] Copyright Amendment (Service Providers) Bill (2017), Second Reading, *available at* 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.

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

[28] The Copyright Amendment (Online Infringement) Bill (2018), Explanatory Memorandum, *available at* https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6209_ems_b5e338b6-e85c-4cf7-8037-35f13166ebd4/upload_pdf/687468.pdf;fileType=application/pdf.

[29] Australian Productivity Commission, Productivity Commission Inquiry Report, No. 78, 2, (Sept. 23, 2016), *available at* https://www.pc.gov.au/inquiries/completed/intellectual-property/report/intellectual-property.pdf.

[30] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill (2019), *available at* https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf.

[31] NYTimes, Australia *Passes Law to Punish Social Media Companies for Violent Posts*, (April 3, 2019), *available at*

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

Online Content

In June 2021, Australia passed the *Online Safety Act 2021*, which will become effective in January 2022. The Act authorizes the eSafety regulator to demand that Internet service providers remove content that is deemed "harmful." Under the Act, companies falling under eight different sectors of the online industry must develop codes of conduct regarding how they will proactively prevent access to both illegal and legal but harmful content. The eSafety Commissioner has also made clear that the enforceable industry codes, which will apply to all international services accessible by Australians, need to include companies' obligations for *preventing* harm, and also for conducting regular mandatory transparency reporting. Further, the Act's "Basic Online Safety Expectations"[32] imposes certain reporting obligations on international service providers regarding steps they take to, among other things, 1) provide Australian-specific safety information to the regulator; 2) identify people behind anonymous accounts; and 3) monitor encrypted communications for harmful content. Failure to comply with the Act could result in severe civil penalties (up to AUD$555,000 for each violation), and a company deemed to systemically disregard eSafety's notices could face a Federal Court order to cease providing relevant services in Australia. In addition to the significant regulatory burden, implementation of these obligations poses technical challenges and privacy concerns. Industry has mobilized around the scope of services caught by this legislation (social media services, user-generated content platforms, search engines, app distribution marketplaces and enterprise hosting services), concerned that turnaround times for content removal are too short (24 hours), lack of transparency and accountability of decisions made by the regulator and that the ill-defined concept of "harm" will lead to lawful content being censored.

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.[33]

---

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

[32] Online Safety Act 2021: Fact Sheet, (July 2021), https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf.

[33] Australian Tax Office. *Combating Multinational Tax Avoidance – A Targeted Anti-Avoidance Law*, *available at* 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/.

Audiovisual Services

In November 2020, the Australian Government issued the Media Reform Green Paper (Green Paper). The Green Paper proposes setting the "expectation" that subscription and advertising video-on-demand (SVOD) services invest a percentage of their Australian revenue in Australian content, in the form of commissions, co-productions, and acquisitions. Under the Green Paper proposal, if service suppliers fail to meet investment expenditure "expectations" for two consecutive years, the Minister of Communications would be authorized to implement relevant regulatory requirements. As drafted, the proposal would not apply to Australian SVODs that have a free-to-air TV broadcaster within their corporate group of companies. At the same time the Australian Government established a voluntary reporting framework administered by Australian Communications and Media Authority (ACMA) under which SVOD services report to ACMA on their level of investment in Australian content. ACMA's first report, published in August 2020, showed SVODs had invested AUD$268 million in Australian content. If the Australian Government indeed mandates SVODs to invest a percentage of their Australian revenue in Australian content, as proposed by the Green Paper, it would be a *prima facie* breach of Australia's obligations under the AUSFTA, under which Australia is obligated to accord to service suppliers of the other Party treatment no less favourable than that it accords, in like circumstances, to its own service suppliers.

News Media and Digital Platforms Mandatory Bargaining Code

In February 2021, the Australian Government passed the News Media and Digital Platforms Mandatory Bargaining Code. Under the Code, designated platform services companies are required to engage in negotiations with Australian news publishers for online content. The Bargaining Code specifies that the Australian Treasurer is responsible for designating platforms. When designating platforms, the Treasurer must consider whether the platform holds a significant bargaining power imbalance with Australian news media businesses. The Treasurer must also consider if the platform has made a significant contribution to the sustainability of the Australian news industry through agreements relating to news content of Australian news businesses. If negotiations break down, or an agreement is not reached within three months between a news business and designated platform, the bargaining parties would be subject to compulsory mediation. If mediation is unsuccessful, the bargaining parties would proceed with arbitration, with arbitrators seeking to determine a fair exchange of value between the platforms and the news businesses. In addition to the negotiation and arbitration requirements, the Bargaining Code imposes information sharing requirements, including a requirement that platforms provide advance notice of forthcoming changes to algorithms if the change is likely to have a significant effect on the referral traffic for covered news content. To date, no platform has been designated, although the Code is subject to an annual review by the Treasurer commencing February 2022. In view of the impending Federal election and that news publishers are integral to the election; the process is politicized. USTR should continue to play close attention to the implementation of the Code and its adherence to the principles of transparency, fairness and non-discrimination as consistent with the AUSFTA.

Telecommunications (Assistance and Access) Act

The Australian Parliament passed the Telecommunications (Assistance and Access) Act at the end of 2018, granting the country's national security and law enforcement agencies additional powers when dealing with encrypted communications and devices.[34] The legislation authorizes the Australian government to use three new tools to compel assistance from technology companies in accessing information within electronic communications. These tools are technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs). These tools call upon providers to do one or more specified acts which could include building new technical capabilities as required by the Attorney General. While the legislation specifically forbids a notice to provide a "systemic weakness or vulnerability" into an encrypted system, it does provide sufficiently broad authority to undermine encryption for all users through other technical means with little oversight. The broad language and failure to address concerns during the initial drafting process remain of concern to US service providers.

[34] Parliament of Australia, Telecommunications (Assistance and Access) Bill (2018), *available at* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

Government-Imposed Content Restrictions And Related Access Barriers

Australia amended its Criminal Code in April 2019 to establish new penalties for internet and hosting services who fail to provide law enforcement authorities with details of "abhorrent violent material" within a reasonable time, or fail to "expeditiously" remove and cease hosting this material.[35] Criticism of the legislation was widespread, with particular concern about the rushed nature of the drafting and legislative process. The legislation applies to a broad range of technology and internet services, including U.S.-based social media platforms, user-generated content and live streaming services, and enterprise hosting services. However, the law does not take into account the varying business models of these services in scope of the law and their varying capabilities or roles in facilitating user-generated content. Australian officials have also indicated that the country will soon block access to internet domains hosting terrorist material and will pursue additional legislation that will impose new content requirements on digital services.[36]

Critical Infrastructure Reforms

Australia announced changes to its critical infrastructure framework, with the introduction of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 in late 2020.[37] The Government's stated objective of the Bill is to "protect the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure." The proposed legislation significantly expands the sectors considered critical infrastructure (including companies that provide "data storage or processing" services) and will impose additional positive security obligations for critical infrastructure assets (like risk management programs and cyber incident reporting), enhanced cyber security obligations and, most concerningly, government assistance measures that would enable Australian government agencies to require critical infrastructure entities to install monitoring software on their networks, to 'take control' of an asset or to follow directions of the Australian Signals Directorate. U.S. companies have actively opposed the extent of the reforms, particularly the government assistance measures, arguing they go above and beyond what is necessary for action and support by the government in the data storage or processing sector.

Hosting Strategy Certification Framework

In 2019, the Australian Government released the Hosting Strategy,[38] providing policy direction on how government data and digital infrastructure would enable the Digital Transformation Strategy, focused on data center facilities, infrastructure, data storage and data transmission. In March 2021, the certification framework for the policy was released[39] to operationalize the Hosting Strategy. The certification requires hosting providers, data center operators and cloud service providers to allow the government to specify ownership and control conditions. The framework has the effect of imposing data localization and data residency requirements, plus personnel requirements, on all protected-level data and data from whole-of-government systems.

---

[35] Criminal Code Amendments (Sharing of Abhorrent Violent Material) Bill (2019), *available at* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201.

[36] Alison Bevege, *Australia to Block Internet Domains Hosting Extremist Content During Terror Attacks*, Reuters (Aug. 25, 2019), *available at* https://www.reuters.com/article/us-australia-security-internet/australia-to-block-internet-domains-hosting-extremist-content-during-terror-attacks-idUSKCN1VF05G.

[37] Security Legislation Amendment (Critical Infrastructure) Bill (2020), *available at* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657.

[38] Digital Transformation Agency, Hosting Strategy, *available at* https://www.dta.gov.au/our-projects/whole-government-hosting-strategy.

[39] Digital Transformation Agency, Hosting Certification Framework (March 2021), *available at* https://www.dta.gov.au/sites/default/files/files/digital-identity/Newpercent20Accreditationpercent20Templates/Hostingpercent20Certificationpercent20Frameworkpercent20-percent20Marchpercent202021.v2.pdf.

Bahrain

Divergence From Privacy Best Practices

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

Restrictions On Cloud Service Providers

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

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

Bangladesh

Data Flow Restrictions And Service Blockages

The Bangladesh Government is reportedly planning to enact laws to institute data localization requirements on foreign companies. To that end, it has released a draft Personal Data Protection Bill but has yet to go into public consultation or introduce the bill in its legislature. The draft bill contains a 'mirroring' requirement, which obliges data controllers to store a copy of personal data collected in Bangladesh on locally situated servers. Moreover, it is also understood that data can only be transferred outside the country on fulfilment of certain arbitrary conditions, under approved standard contractual clauses or intra-group agreements, or to white-listed countries, or pursuant to approval of the GoB, or with the data subject's consent. These requirements are not only inconsistent with International Standards, but they also impose overly restrictive conditions that will be prohibitively expensive for U.S businesses.

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 solidarity, financial activities, security, defence, religious values or public discipline of the country or any part thereof" and created new criminal provisions prohibiting publication of content online that may be defamatory, harmful to religious values, or critical of the government.[40] Many of these

[40] Government of the People's Republic of Bangladesh Legislative and Parliamentary Affairs Division Ministry of Law, Justice and Parliamentary Affairs, Digital Security Act, (2018), *available at* https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf.

provisions are vague and overbroad and pose considerable operational challenges for U.S. based intermediaries in the market.

Additionally, service providers may only defend themselves if they can prove that they took all possible steps to try to prevent publication of specific material that violates the law. Otherwise, they will be subject to criminal penalties, including fines and/or imprisonment. While theoretically internet intermediaries have safe harbor under the Digital Security Act, in practice, this can be easily lost, providing internet intermediaries with insufficient protection from liability for third-party user content. The lack of adequate safe harbor protections poses a significant barrier for internet intermediaries in the market. The Bangladesh Telecommunication Regulatory Act of 2001 is currently undergoing revisions and the amended Act will grant the Bangladesh Telecommunication Regulatory Commission extraterritorial jurisdiction over internet companies that will have far reaching consequences for U.S-based businesses.

Unilateral Or Discriminatory Digital Tax Measures

Bangladesh has a 15 percent value-added tax (VAT) on digital sales. However, unlike resident taxpayers where online direct payment of tax dues is available, the National Board of Revenue (NBR) has not implemented a mechanism to allow non-resident service providers to remit tax dues online, directly into the government exchequer. This makes it costlier for non-resident service providers to comply with the VAT law as compared to resident taxpayers.

Filtering, Censorship and Service Blocking

Bangladesh has blocked Facebook several times, including during the pandemic in March 2021, citing national security interests, thereby cutting off access to a U.S-based communication service for more than 40 million Bangladeshis.

Digital Security Act

The Digital Security Act of 2018 criminalizes a wide range of online activity, creating challenges for Internet-based platforms and digital media firms. The Act criminalizes publication of information online that hampers the nation, tarnishes the image of the state, spreads rumors, or hurts religious sentiment. The Act provides for criminal penalties up to $120,000 and up to 14 years in prison for certain infractions.

Information and Communication Technology Act

The Information and Communication Technology Act of 2006 (the Act), amended in 2013, authorizes the government of Bangladesh to access any computer system for the purpose of obtaining any information or data, and to intercept information transmitted through any computer resource. Under the Act, Bangladesh may also prohibit the transmission of any data or voice call and censor online communications. The Bangladesh Telecommunication Regulatory Commission (BTRC) ordered mobile operators to limit data transmissions for political reasons on several occasions in 2019 and in 2020 ahead of politically sensitive events, including local and national elections. The BTRC ordered mobile operators to block all services except for voice calls in the Rohingya refugee camps in Cox's Bazar from September 2019 until August 2020. In November 2018 the BTRC instructed all international internet gateway licensees to temporarily block a U.S. voice over IP service supplier; the block lasted for one day. Such interference, even on a temporary basis, undermines the value of internet-based services, decreasing the incentive to invest, and raises costs for firms in the market.

Brazil

Copyright-Related Barriers And Non-IP Intermediary Liability Restrictions

Historically, the 'Marco Civil' law[41] has offered legal certainty for domestic and foreign online services and has created conditions for the growth of the digital economy in Brazil.[42] 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.[43]

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

There is also a bill on the Brazilian Senate[44] that includes a provision that requires digital platforms to "pay news publishers for use of their content (other than hyperlinks)," distorting fair play and placing unfair burden on digital platforms.

Customs Barriers To Growth In E-Commerce

Brazil's de minimis threshold with respect to imported items not subject to duty or tax charges applies only to customer to customer (C2C) transactions under $50 and sent through Post (Decree No. 1804 of 1980 and Ministry of Finance Ordinance No. 156 of 1999). 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. Brazil should address this barrier to trade by extending the de minimis threshold to business to customer (B2C) and business to business (B2B) transactions, for both Post and express delivery shipments, and increasing the threshold to a commercially meaningful level. As a reference, OECD members have an average of USD$70 for taxes and USD$194 for duties. A change in the de minimis policy can lead to an increase in consumption, since consumers will have more products available in the market. Studies have shown that this increase in consumption will positively impact the Brazilian economy, adding R$157 million to the GDP, besides increasing wages by R$ 82.7 million per year, and generating more than 3,000 jobs.

Brazil has already moved forward in its trade facilitation policy, by implementing the new Single Window project for imports and exports. The project's goal is to reduce the average time for customs procedures by implementing one integrated system, and cutting bureaucracy and paper requirements. Part of the project's proposal to recede import times is the creation of the Product Catalog, a database of products and foreign operators. The database's main objective is to increase the quality of the product descriptions, with information organized in attributes, and allow the attachment of documents that help the administrative treatment, inspection, and risk analysis. The e-commerce particularities should be considered within this process to guarantee a simplified process for products bought online. It is also crucial that the government ensures that businesses have adequate time to adapt to any new requirements.

---

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

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

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

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

Tariff Reduction

The Ex-Tariff regime consists of the temporary reduction of the tax rate for the import of capital goods and information technology and telecommunications, as classified in the Common External Tariff of Mercosur, when there is no national production equivalent. In order for this regime to continue to attract more investments, it is critical that the Brazilian government ensures Mercosur's approval to extend the Ex Tariff regime, which is currently scheduled to end in December 2021. Otherwise, all products that benefit from this regime, including cutting-edge technology for Brazilian consumers, will be subject to their original import tariffs. The Brazilian import tariff for information and communication technology (ICT) products, for example, is one of the highest in the world.

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 ICT goods and equipment (Basic Production Process (PPB) – Law 8387/91, Law 8248/91, and Ordinance 87/2013); it offers government procurement preferences for local ICT hardware and software (2014 Decrees 8184, 8185, 8186, 8194, and 2013 Decree 7903); and it does not recognize the results of conformity assessment procedures performed outside of Brazil for equipment connected to telecommunications networks (ANATEL's Resolution 323). Industry reports that cloud services are also required to have some types of government data localized under recent revisions to the Institutional Security law. The Presidency Institutional Security Group (GSI) published a Normative Instruction which established new rules for the contracting of cloud services by the Federal Public Administration. It established requirements for data and metadata residency exclusively in national territory in a few situations that are red flags for U.S. digital services providers. These requirements disadvantage firms that provide services to the Brazil public sector but do not have the capacity to store data locally, and these guidelines set concerning precedents.

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

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

Divergence From Privacy Best Practices

On August 15, 2018, Brazil's President Michel Temer signed the General Data Protection Law Lei Geral de Protecao de Dados (LGPD), inspired by the EU's GDPR. Businesses had 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.[45]

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.[46] These developments conflict with Brazil's strong commitment to freedom of expression and

[45] *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.

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

access to information, and would present market access barriers for both small and large U.S. services seeking to enter the Brazilian market.

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.[47]

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.[48]

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.[49] However, this approach risks raising costs for online entrepreneurs and halting Brazil's innovation due to increased bureaucracy and artificial limits on services, harming both local consumers and foreign providers of internet services.

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

Good Regulatory Practices

Brazil took a significant step towards good regulatory practices when the Brazilian Foreign Trade Council (CAMEX)'s published Resolution 90 in 2018, thereby establishing good practices for the preparation and review of regulatory measures affecting foreign trade. The resolution encourages Brazilian regulatory bodies to develop regulatory agendas, conduct regulatory impact analysis, evaluate regulatory alternatives, use international standards, conduct transparent public consultations of a minimum of 60 days for all regulations with international trade effects, ensure all regulations comply with Brazil's international trade commitments, notify regulations to the

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

[48] *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/.

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

WTO via the inquiry point, use evidence-based decision making, coordinate with other relevant regulators to ensure coherence and compatibility with other regulations, and review and manage regulatory stock. Despite this development, however, recent consultations notified by ANATEL through the WTO TBT inquiry point included very short timeframes for response. We appreciate ANATEL extending the deadlines for comments on a case-by-case basis, but we encourage all agencies in Brazil to notify consultations with a minimum 60-day comment period. Agencies are also encouraged to consider the regulatory impact imposed by requirements and whether the benefits are commensurate with the impacts. For example, the recent operational procedures published for Resolution No. 715 contain a number of submission procedures and additional bureaucratic steps that increase burden to industry without providing additional assurance of conformity. We encourage ANATEL to consider the impacts of regulations in comparison to the benefits provided and to provide an explanation of these benefits in any proposed regulation.

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

National AI Strategy

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

Restrictions On Cloud Service Providers

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

Unilateral Or Discriminatory Digital Tax Measures

The Brazilian Congress is considering a variety of bills that seek to implement or raise taxes on digital services. Currently, the most relevant bill creates the Social Contribution on Digital Services (CSSD), with a rate of three percent on the gross revenue from digital services, and ten percent on the revenue from online betting. The bill targets companies domiciled in Brazil or abroad that have earned in Brazil a gross revenue greater than R$ 100 million (USD 17 million). The bill has support from traditional members of Congress, from both the opposition and the government support base. On the other hand, neither the speakers of the House and Senate nor the Ministry of Economy endorsed any of the proposals. Brazil's proposals share characteristics with the French DST enacted in

July 2019, in that they contravene long-standing international taxation principles and present significant burdens for companies in the tech sector as well as the companies that rely on these services.

Brazil is also an expansion of its existing CIDE (contribuição de intervenção no domínio econômico) regime. The CIDE-Digital tax (PL 2,358/2020) would apply progressively from 1 percent to 5 percent on gross revenues derived from (1) digital advertising; (2) operating a digital service that permits users to interact with each other for the sale of goods and services; and (3) collection of user-generated data in the operation of a digital platform.[50] There is also pending legislation (PL 131/2020) to raise payments under the existing COFINS regime (contribuição para o financiamento da seguridade social) for companies in the digital sector.[51]

Given the recent agreement at the OECD, the Brazilian Government should abandon any consideration of unilateral DSTs.

Import Licenses

The import of products that require import licenses in the current Brazilian licensing system face challenges. These challenges are mainly related to the time it takes to issue licenses, which does not keep up with the agility for shipments. Furthermore, air shipments are consolidated with thousands of other products that do not have an import license, and as the License is per product and per shipment, a product that requires licensing could interrupt the shipment and delivery of several other products to consumers. Brazil should consider issuing import licenses by product, through a process that requires only information similar to that in the product catalog: informing the product manufacturer, without the need to specify commercial data. It is also crucial to extend the validity of import licenses from six months to one year, and to allow their use in several shipments, with no limit of quantity (only time).

Privacy Law

In 2018, Brazil passed a privacy law, Lei Geral de Proteção de Dados (LGPD). It came into force in August 2020 and enforcement of its penalties and sanctions provisions one year later, in August 2021.[52] The law is closely modeled after the EU's General Data Protection Regulation (GDPR) and has extraterritorial scope. However, the LGPD lacks a number of provisions in the GDPR designed to lessen the burden on smaller firms.[53] Further, the LGPD does not permit cross-border data transfers based on the controller's legitimate interests, but rather lists ten instances in which cross-border data transfer under the LGPD is permitted.[54] In addition, the national authority is tasked with determining whether a foreign government or international organization has a sufficient data protection scheme in place before any data is authorized to be transferred to the government or organization. The national authority released its regulatory agenda and included "International transfer of data" as part of "Phase 2", meaning that the issue is expected to be subject to public consultation by mid-2022. Brazil's data protection

[50] *Brazil Congressman Proposed Digital Services Tax*, EY, (May 8, 2020), https://taxnews.ey.com/news/2020-1246-brazilian-congressman-proposes-digital-services-tax.

[51] *Brazil: Proposed COFINS Regime for Digital Sector Taxpayers*, KPMG (July 7, 2020), https://home.kpmg/us/en/home/insights/2020/07/tnf-brazil-proposed-cofins-regime-digital-sector-taxpayers.html ("The proposal (COFINS-Digital) would, if enacted, affect companies that operate in the digital sector and would focus on the gross monthly revenue earned in relation to digital services from: [1] Electronic communications and digital interface that allows interaction between users with regard to the delivery of goods or provision of services [and 2] Marketing to advertisers or agents for placing targeted advertising messages on a digital interface based on user data.").

[52] Kate Black *et al.*, *Brazil's Data Protection Law Will Be Effective After All, But Enforcement Provisions Delayed Until August 2021*, GreenbergTraurig, (Aug. 28, 2020), https://www.gtlaw.com/en/insights/2020/8/brazils-data-protection-law-effective-enforcement-provisions-delayed-august-2021.

[53] Erin Locker & David Navetta, *Brazil's New Data Protection Law: The LGPD*, Cooley Policy & Legislation, (Sept. 18, 2018), *available at* https://cdp.cooley.com/brazils-new-data-protection-law-the-lgpd.

[54] Chris Brook, *Breaking Down LGPD, Brazil's New Data Protection Law*, Data Insider (June 10, 2019) (noting that the instances where cross-border data transfer is allowable are found in articles 33-36 of the LGPD), *available at* https://www.digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law .

authority will release guidelines to define what constitutes the international transfer (for example, storage on international servers contracted for cloud service) and the content of standard contractual clauses.

Copyright Liability Regimes for Online Intermediaries

The Ministry of Citizenship held a consultation in 2019 on Brazil's Copyright Law.[55] Industry reports that officials are considering what approach to take with respect to intermediary liability protections, which do not currently exist within the existing statute for copyrighted content. The Marco Civil da Internet, Federal Law No. 12965/2014, granted limited intermediary protections that do not include copyrighted content. Brazil should adopt an approach consistent with DMCA notice-and-takedown provisions that will allow legal certainty for Internet services in Brazil. There is also the pressure to change the Brazilian copyright regime in order to create a press publishers' right, a similar movement to the EUCD Article 15 implementation.

Cambodia

National Internet Gateway

Reports of censorship and mandated Internet filtering and blocking continue to rise in Cambodia.[56] A sub-decree signed in February 2021 established the National Internet Gateway, which would create a single point of entry for internet traffic regulated by a government-appointed operator. While the specifics of the implementation remain unclear, there is potential that this could be abused and misused to block online content and keep out certain foreign digital services, akin to China's "Great Firewall".

Draft Cybercrime Bill

The Cambodian Interior Ministry has come up with a draft Cybercrime bill,[57] which includes provisions that could make intermediary platforms liable for content uploaded by third parties. It also includes broad provisions that mandate data localization to facilitate access by government authorities. There has thus far not been any consultation with industry on the draft bill.

Canada

Discriminatory Or Opaque Application Of Competition Regulations

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

---

[55] Ministério Do Turismo, Secretaria Especial da Cultura, Ministério da Cidadania abre consulta pública sobre reforma da Lei de Direitos Autorais, (June 28, 2019), *available at* http://cultura.gov.br/ministerio-da-cidadania-abre-consulta-publica-sobre-reforma-da-lei-de-direitos-autorais/.

[56] *Freedom on the Net 2020: Cambodia* (2020), *available at* https://freedomhouse.org/country/cambodia/freedom-net/2020.

[57] Voice of America, Activists: Cambodia's Draft Cybercrime Law Imperils Free Expression, Privacy, (Oct. 11, 2020), *available at* https://www.voanews.com/a/east-asia-pacific_activists-cambodias-draft-cybercrime-law-imperils-free-expression-privacy/6196959.html

Non-IP Intermediary Liability Restrictions

The Liberal platform and government mandate letters call for new rules regulating online content and expands the role of internet companies in addressing content posted online.[58] The plan includes significant penalties for social-media companies that fail to address online harms within 24 hours. There will also be legislation introduced to address civil remedies for victims of online hate. The plan runs counter to USMCA Article 19.17, and IA urges USTR to engage with Canadian officials on this issue.

Unilateral Or Discriminatory Digital Tax Measures

Late in 2019, Canadian Prime Minister Justin Trudeau has proposed a digital services tax similar to the French DST.[59] 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.[60] There have been renewed calls for this tax in the wake of the COVID pandemic. Given the recent agreement at the OECD, the Canadian Government should abandon any consideration of unilateral DSTs. IA urges USTR to seek to prevent Canada from implementing this unilateral tax measure concerning digital products and services.

After the recent OECD agreement, the government of Canada agreed to pause on implementing a Digital Services Tax until January 2024, but also indicated that it would proceed in designing and passing this tax via legislation before 2022. Minister Freeland confirmed that "we intend to move ahead with legislation finalizing the enactment" of the DST. It appears that this legislation will include a provision that will retroactively impose a digital levy for the previous two years if a final OECD agreement "has not come into force" by the beginning of 2024. There is a risk that this legislation will provide a blueprint for other countries to move forward with similar DSTs while creating similar retroactive mechanisms to bank revenues from 2022 forward in the event that the OECD agreement does not come into force.

Extraterritorial Regulations And Judgments

Rulings regarding intermediary liability that have extraterritorial effects present a significant barrier to trade by creating significant market uncertainty for companies seeking to host user content and communications on a global basis. In *Equustek Solutions v. Jack*, Google was compelled by the Supreme Court of British Columbia to remove—from all its domains worldwide—indexes and references to the website of Datalink, a competitor to Equustek that had been found to have violated Canadian trade secrets and consumer protection laws.[61]

Following two unsuccessful Canadian appeals, Google successfully obtained permanent injunctive relief in the United States District Court for the Northern District of California, which held that the Canadian order could not be enforced in the United States because it undermined U.S. law and free speech on the Internet. While an injunction was granted, the principle that Canadian courts can dictate to Americans what they can read online is itself a trade barrier. Further, the Equustek decision has since been cited by other foreign courts to justify world-wide injunctions for online content.[62]

---

[58] Liberal Party of Canada, Forward: A Real Chance for Middle Class, (2019), *available at* https://2019.liberal.ca/wp-content/uploads/sites/292/2019/09/Forward-A-real-plan-for-the-middle-class.pdf

[59] *Id.*

[60] Office of the Parliamentary Budget Officer, *Cost Estimate of Election Campaign Proposal*, (Sept. 29, 2019), *available at* https://www.pbo-dpb.gc.ca/web/default/files/Documents/ElectionProposalCosting/Results/32977970_EN.pdf?timestamp=1569835806287.

[61] *Equustek Sols. v. Jack,* [2014] B.C.S.C. 1063, *available at* https://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc1063/2014bcsc1063.pdf.

[62] *Swami Ramdev & Anr. v. Facebook, Inc.*, High Court of Delhi at New Delhi, (Oct. 23, 2019), *available at* http://lobis.nic.in/ddir/dhc/PMS/judgement/23-10-2019/PMS23102019S272019.pdf, infra note 274.

Restrictions On Cross-Border Data Flows

Industry had raised concerns with the Office of Privacy Commission (OPC) during consultation on the review of its official policy position on cross-border data flows under the Personal Information Protection and Electronic Documents Act.[63] After industry concerns, the OPC determined that it would not amend the guidelines.[64] Rather, it intends to direct lawmakers to reevaluate existing law and determine whether legislative changes are needed. Industry is following these proceedings. Abrupt changes to procedures that enable data transfer between the U.S. and Canada may conflict with provisions in the Digital Trade Chapter of USMCA and Canada's commitments under CPTPP, which both contain commitments for all parties to enable cross-border data flows.

Online Harms Bill

The Canadian government recently announced plans to combat online hate speech with a new bill dealing with "online harms" (C-36), as well as a forthcoming consultation on new obligations for online platforms to remove harmful content. The broad nature of the proposal means it can include content that is legal but still judged to be harmful, such as abuse that doesn't reach the threshold of criminality, and posts that encourage self-harm and misinformation. It is also expected that the proposal will include a NetzDG-style model requiring removal of harmful content within specified timeframes, to be administered by a new regulator empowered to fine and block non-compliant sites and services, along with new mandatory reporting obligations to Canadian law enforcement. The overly broad nature of the proposal will likely result in censorship of Canadian speech and collateral harm to U.S. companies carrying such speech.

The Canadian government also introduced Bill C-10, which extends Canada's broadcasting regulations to online platforms. Under Bill C-10, the Canadian Radio-Television and Telecommunications Commission is empowered to apply new "discoverability" obligations to any site of service hosting audio or audio-visual content (including "social media services") which would compel the service to give preferential treatment to Canadian content and creators. This has profound censorship and digital trade implications, as it necessarily means non-Canadian audio and audio-visual communications will be demoted.

Chile

Copyright-Related Barriers

Chile does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Chilean Intellectual Property Law includes a long but inflexible list of rules[65] that does not clearly provide for open limitations and exceptions that are necessary for the digital environment – for example, flexible limitations and exceptions that would enable text and data mining, machine learning, and indexing of content. This handful of limitations leaves foreign services and innovators in a legally precarious position. In order to reduce market access barriers to U.S. services, IA urges USTR to work with Chile to implement a multi-factor balancing test analogous to fair use frameworks in the U.S and Singapore, to enable copyright-protected works to continue to be used for socially useful purposes that do not unreasonably interfere with the legitimate interests of copyright owners.

Divergence From Privacy Best Practices

Under Chile's Comisión para los Mercados Financieros, its compilation of updated rules (Recopilacion Actualizada de Normas Bancos or "RAN") Chapter 20-7 requires that "significant" or "strategic" outsourcing data be held in

[63] CCIA Comments, In re Request for Public Comments To Compile the National Trade Estimate Report on Foreign Trade Barriers, Docket. No. 2019-0012, filed (Oct. 31, 2019) at 33, *available at* https://www.ccianet.org/wp-content/uploads/2019/10/USTR-2019-CCIA-Comments-for-NTE.pdf [hereinafter "2019 CCIA NTE Comments"].

[64] Office of the Privacy Commissioner of Canada, Commissioner Concludes Consultation on Transfer for Processing (Sept. 23, 2019), https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.

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

Chile. The same requirement is outlined in Circular No. 2, which is addressed to non-banking payment card issuers and operators. In effect, these regulations can apply to any confidential records. In the case of the international transfer of such data, transfer may occur but duplicate copies of such records must be held in Chile.

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

China

The Chinese market continues to be hostile to foreign competitors, and in recent years the focus on U.S. information technologies and internet services has intensified. An influx of anticompetitive laws directed at information infrastructure and cloud services combined with an uptick in Internet shutdowns have businesses growing more concerned and hesitant to enter the Chinese market, costing American firms.

USTR should remain vigilant and discourage policies restricting foreign companies' ability to enter the Chinese technology sector, and to promote policies focused on allowing free and open competition within China's borders. This is increasingly critical as China's global dominance in technology services continues to rise.[66] U.S. policy should target unfair practices by foreign trade partners, while ensuring any U.S. offensive measures or regulations do not have the adverse effect of disadvantaging U.S. firms.

Lack Of Intellectual Property Protection/Digital Trade And E-Commerce

In recent years, the protection of intellectual property rights (IPR) has become an area of increasing focus to USTR. The government of China should strengthen relevant law enforcement, effectively protect the legitimate rights and interests of U.S. tech companies, and establish an open and fair market environment. The major challenge to IPR protection in China is insufficient efforts by the government of China against cross-border counterfeit crimes.

We recommended that the government of China proactively enhance international cooperation on IPR protection, fully utilize multilateral or bilateral mechanisms to strengthen cross-border judicial assistance, and work closely with judicial agencies in the U.S., EU, UK, ASEAN, among others, to achieve consensus on the fight against online crimes, and build common rules for digital forensics across borders.

Government Procurement Restrictions

China's Government Procurement Law (GPL) was implemented in 2002 and revised in 2014. It stipulates that government procurement should purchase domestic products, services, and engineering projects, with exceptions made only when the targeted products are not available in the Chinese market or are not used within China's territory. In late-2020, an amendment draft calling for comments on the GPL did not result in any changes. It is noteworthy that in the draft for public opinion of the Implementing Regulations of Government Procurement Law, in 2010, the term "domestic products" was clearly defined as goods physically manufactured in Chinese territory, with a certain proportion of domestic production costs, while "domestic services and engineering projects" were defined as being supplied by Chinese nationals, legal persons, or organizations. Nevertheless, these definitions were nowhere to be found in the formal Implementing Regulations of GPL released in 2015. This absence puts government procurement of foreign-invested and domestically manufactured or assembled products at a competitive disadvantage. Further, while the government of China has wide discretion in determining whether a product is considered "domestic."

[66] Richard Bowman, *Rise of China's Tech Giants – What to know when investing in Chinese tech companies*, Catana Capital (Aug. 3, 2020), *available at* https://catanacapital.com/blog/investing-chinese-tech-companies/.

Restrictions On Cloud Services

China seeks to further restrain foreign cloud service operators, in concert with its national plan to promote the Chinese cloud computing industry. U.S. cloud service providers (CSPs) are worldwide leaders and strong U.S exporters, supporting tens of thousands of high-paying American jobs and making a strong contribution toward a positive balance of trade.[67] 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 will 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 implement fully these restrictions, effectively barring U.S. CSPs from operating or competing fairly in China.

China's Ministry of Industry and Information Technology (MIIT) proposed two draft notices – Regulating Business Operation in Cloud Services Market (2016) and Cleaning up and Regulating the Internet Access Service Market (2017). These measures, together with existing licensing and foreign direct investment restrictions on foreign CSPs operating in China under the Classification Catalogue of Telecommunications Services (2015) and the Cybersecurity Law (2016), would require foreign CSPs to turn over essentially all ownership and operations to a Chinese company, forcing the transfer of incredibly valuable U.S. intellectual property and know-how to China.[68]

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.

The United States must 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 remain free to operate and compete in the U.S. market, and U.S. CSPs should benefit from the same opportunity in China.

Cybersecurity

Over the past year, the government of China has expedited the implementation of cybersecurity measures, including the Cybersecurity Review Measure, the Personal Information Protection Law, the Critical Information Infrastructure Protection Measure, and a series of auto data related regulations. There are also many laws and regulations currently being consulted or discussed, including Data Security Management Measures in the Field of Industry and Information Technology, Administrative Measures for the Filing of Network Product Security Vulnerability Collection Platforms, Provisions on Administration of Algorithm-based Recommendation in Internet Information Services, Data Categorization and Classification, just to name a few. These laws and regulations raise various requirements for market players, and may set hurdles for MNCs to participate in specific sectors and add additional compliance burdens.

---

[67] Synergy Research Group, *Amazon Dominates Public IaaS and Ahead in PaaS; IBM Leads in Private Cloud* (Oct. 30, 2016), *available at* https://www.srgresearch.com/articles/amazon-dominates-public-iaas-paas-ibm-leadsmanaged-private-cloud.

[68] 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.

- **Critical Information Infrastructure**. The *Critical Information Infrastructure Protection Measures ("Measure")* was released on August 17, 2020. The Measure provides a non-exhaustive list of the sectors for Critical Information Infrastructure (CII), including public communications and information services, energy, transportation, water utilities, finance, public services, e-government, and national security. The ever-expanding scope of CIIs and the cybersecurity review create compliance cost and potential entry barrier to certain sectors. It is important that the various relevant regulatory mechanisms be transparent and narrow in scope. This includes ensuring that terms such as "national security," "national economy and people's livelihood," and "public interests" are not interpreted broadly.

- **Data policy.** Data localization and restrictions on cross-border data flows are existent in various Chinese laws and regulations. According to the Cybersecurity Law, effective in 2017, "Personal information and important data collected and generated by critical information infrastructure operators during their operations in the People's Republic of China should be stored in the country." The Data Security Law, effective in 2021, carries out the concept of important data and core data, and further subjects non-CII operators that collect or produce important data to cross-border security review regulations. The Personal Information Protection Law, effective in 2021, sets requirements on the cross-border transfer of personal data. Besides the general data regulations, we have also seen data localization and cross-border data flow restrictions in various industry regulations, such as financial services, auto, ride hailing, internet publication, mapping, and pharmaceutical sectors. The lack of necessary clarifications on the term "data" and unclear procedures for cross-border data review as well as for triggering a data security review increase the already complex and uncertain compliance burdens. In addition to posing heavy operational burdens, these requirements can essentially act as market access barriers for foreign invested enterprises, due to their high frequency of cross-border data transfer for normal operational reasons and in response to their headquarters' requests, among other reasons.

- **Industry standards.** The Cybersecurity Review Measures, effective in 2020, puts in place a review process to regulate the purchase of ICT products and services by CII operators in China. In addition, the draft revision of Information Security Technology - Security Capability Requirements of Cloud Computing Services (GB/T 31168) and Basic Rules for the Regulation of Financial Cloud Services propose a community cloud model with physical separation of the servers for critical workloads in the public sector and financial services sector. In October 2019, China adopted a Cryptography Law that includes restrictive requirements for commercial encryption products that "involve national security, the national economy and people's lives, and public interest," which must undergo a security assessment, arising concerns that the new Cryptography Law will lead to unnecessary restrictions on foreign ICT products and services.

Copyright-Related Barriers

Online piracy remains rampant in China, for example with respect to e-books and software. At the same time, China has not expedited amendments to its Copyright Law, which have been under review since 2011. The latest draft proposes increased penalties that would provide a greater deterrent to copyright violators. For example, under the current law, there is no criminal provision for digitalization of written works and circumvention of digital technological protection measures, and pirates can only be pursued for criminal liability with the purpose of making profits. The cost of selling pirated eBooks or software remains unreasonably low in China as online shops are immune from criminal charges if they sell pirated copies valued under a significant threshold $7,365) or the online works being transmitted have been accessed less than 50,000 times. As industry has repeatedly communicated to authorities, piracy would be improved if China's Criminal Law introduced new crimes of online piracy, lowered the criminal threshold, increased criminal liability for piracy, implemented stronger civil remedies, and expressly criminalized the commercial use of pirated content.

Data Flow Restrictions And Service Blockages

China imposes numerous requirements on internet services to host, process, and manage data (personal information and other important data gathered or produced within China) to be stored locally within China, and places significant restrictions on data flows entering and leaving the country. China continues to moderate the

public's access to websites and content online. On June 4, 2019, access to CNN was blocked[69] after the media company published a story on Tiananmen Square prior to the anniversary of the event.

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

China's restrictive requirements on data localization and cross-border information flows will significantly impact foreign companies' ability to operate in the online space, create extra burdens, and hurt related business prospects. The data localization requirement would extend the scope of CII to all internet business players, and mandates all original users' information be retained within China only, with no copies being transmitted beyond the country, unless an authority's approval is obtained. Expanding the scope of CII requirements will make ordinary data transfers much more complicated and inflict unnecessary burdens on foreign companies.

A new draft Measures for Security Assessment of Personal Information Cross-border Transfer released for comments in 2019 focuses on cross-border transfer of "personal information"— imposing cross-border data transfer restrictions on ordinary network operators and requiring companies to obtain customer consent for cross-border transfers of their sensitive personal information. On May 28, 2019, draft Measures for Data Security Management were released that set out requirements for the treatment of "important data" which was not clearly defined in the Cybersecurity Law.[70] "Important data" is defined as "data that, if leaked, may directly affect China's national security, economic security, social stability, or public health and security."[71] Draft amendments were also published in 2019 to amend the Personal Information Protection Standard, which became effective in 2018 and sets out best practices regarding enforcement of the data protection rules outlined in the Cybersecurity Law.[72] The draft amendments released on February 1, 2019, set out the following: enhanced notice and consent requirements, new requirements on personalized recommendations and target advertising, requirements on access by third parties and data integration, revised notification requirements for incident response, and requirements to maintain data processing records.[73] These two draft Measures are reportedly being submitted for deliberation during the National People's Congress term ending in 2023.[74]

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.

---

[69] Catherine Chu, *China blocks CNN's website and Reuters stories about Tiananmen Square*, Tech Crunch, (June 3, 2019), *available at* https://techcrunch.com/2019/06/04/china-blocks-cnns-website-and-reuters-stories-about-tiananmen-square/.

[70] Yan Luo, Nicholas Shepherd & Zhijing Yu, *China Releases Draft Measures for Data Security Management*, Covington Inside Privacy (May 28, 2019), https://www.insideprivacy.com/uncategorized/china-releases-draft-measures-for-the-administration-of-data-security/.

[71] *Id.*

[72] Yan Luo & Phil Bradley-Schmieg, *China Issues New Personal Information Protection Standard*, Covington Inside Privacy (Jan. 25, 2018), https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/.

[73] Yan Luo, *China Releases Draft Amendments to the Personal Information Protection Standard*, Covington Inside Privacy (Feb. 11, 2019), https://www.insideprivacy.com/international/china/china-releases-draft-amendments-to-the-personal-information-protection-standard/.

[74] Graham Webster & Rogier Creemers, *A Chinese Scholar Outlines Stakes for New 'Personal Information' and 'Data Security' Laws (Translation)*, New America (May 28, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation/.

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

Electronic Payments

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

Filtering, Censorship, And Service-Blocking

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

China imposes numerous requirements on internet services to host, process, and manage data locally within China, and places significant restrictions on data flows entering and leaving the country. China actively censors – and often totally blocks – cross border internet traffic. It has been estimated that approximately 3,000 internet sites are totally blocked from the Chinese marketplace, including many of the most popular websites in the world. High-profile examples of targeted blocking of whole services include China's blocking of Facebook, Picasa, Twitter, Tumblr, Google Search, Foursquare, Hulu, YouTube, Dropbox, LinkedIn, and Slideshare.

Infrastructure-Based Regulation Of Online Services

China's revised Telecommunications Services Catalog released in 2015 expands regulatory oversight of new services not typically regulated as telecom services. China's classification of cloud computing, online platforms, and content delivery networks as Value Added Telecom Services (VATS) not only has far-reaching consequences for market access and the development of online services in China, but also runs counter to China's WTO commitments. For example, cloud computing is traditionally classified as a Computer and Related Service, not a Telecommunications Service. Applying licensing obligations to 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

Data Localization

While Colombia has a legal regime that allows cross-border data flows (law 1581 2012 and Circular externa SIC 02/18) and a cloud friendly environment, the ministry of defense issued a regulation in March 2021 with data localization requirements for the sector. This regulation is in tension with the national digital transformation plan adopted by the National Government. Among other matters, it does not follow the guidelines and standards issued by the Presidential Council for Economic Affairs and Digital Transformation and the ICT Ministry, such as the Cloud Computing Manual (February 2021) and the Cloud Computing Guide G.ST.02. (May 2018), especially in relation to the definitions and scope of cloud services, as well as the absence of data localization requirements. It is also in tension with the Presidential Directive 03 of 2021, which defined the guidelines for the use of cloud services, artificial intelligence, digital security and data management in public entities of the executive branch of national order.

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.[75] 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

Article 5.7(g) of the U.S.-Colombia Free Trade Agreement establishes a de minimis threshold of $200, below which no customs duties or taxes are charged on imported goods. In December 2012, a tax reform implemented the VAT benefit, but the Colombian government only fully implemented it regarding customs duties in August 2020. Colombia is applying the de minimis threshold to all express and postal shipments arriving in Colombia, no matter the country of origin.

On Sept. 8, the Colombian Congress approved a new tax reform that adjusted the application of the de minimis threshold. The VAT exemption for shipments under $200 will be limited to Free Trade Agreement partners whose agreements explicitly include such VAT exemption (i.e., US) and for shipments with no commercial use. It remains to be seen how the government will define 'shipments with no commercial use;' depending on how it does, it could impact the ability of companies to leverage this shipment method and comply with the Agreement.

Non-IP Intermediary Liability Restrictions

This fall, legislation is moving in Colombia targeting U.S. digital platforms. The draft bill "Por el cual se modifica la Ley General de Turismo y se dictan otras disposiciones" was drafted by the Vice Minister of Tourism Julian Guerrero at the urging of traditional hotel associations. The bill proposes regulations against digital platforms' responsibilities. It would hold digital platforms legally liable for any user's violation of terms of service (Article 21), which will be impossible to implement. The bill would require digital platforms to register with the National Tourism Registry (Article 20), which would make U.S. companies subject to local law and further sanctions beyond the user's violation of terms of service. It would also require digital platforms to create a permit field and obligate Colombian hosts to submit a permit number from the National Tourism Registry (Article 20), which would burden those who share their space for income, and require home sharing platforms achieve the impossible task of confirming all listings are registered. Any company incorporated in the U.S. or abroad that participates as an intermediary in the travels and tourism sector is subject to the Bill, including online travel agencies, metasearch companies, short-term rental platforms and Global Distribution Systems. The Bill also poorly defines an electronic or digital platform broad enough to account for a wide swath of IA member companies.

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services outside of the traditional taxi industry must be licensed under the for-hire vehicle category. In addition, for-hire vehicles face market access restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of for-hire vehicles. For example, 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.

Copyright Liability Regimes For Online Intermediaries

Colombia has failed to comply with its obligations under the U.S.-Colombia Free Trade Agreement to provide protections for Internet service providers.[76] Revision to the legislation in 2018 that sought to implement the

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

[76] *See* US-Colombia Free Trade Agreement, (Nov. 22, 2006), art. 16.11, para. 29.

U.S.-Colombia FTA copyright chapter includes no language on online intermediaries.[77] Without such protections required under the FTA, intermediaries exporting services to Colombia remain exposed to potential civil liability for services and functionality that are lawful in the United States and elsewhere. The recent legislation also does not appear to include widely recognized exceptions such as text and data mining, display of snippets or quotations, and other non-expressive or non-consumptive uses.

National Strategy On Artificial Intelligence

The Colombian Government presented the approved version of its Ethical Framework for AI, which is at the core of the national strategy on AI. The document put children at the center, introducing a set of recommendations to guarantee that the use of AI would impact children in a positive way. While the Framework adopted some good practices such as taking a risk-based approach for AI solutions, it also included several obligations that might lead to unique standards, onerous certifications, audit of algorithms, among other concerning matters which would add undue burden to US companies operating in the Colombian market.

Ecuador

Divergence From Privacy Best Practices

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

Data Localization Requirements

The personal data protection bill establishes that public sector entities that contract software services or others that involve the location of data, must do so with providers that guarantee that the data remains in the country and is located in data centers that comply with international standards on security and protection.

Pursuant to the bill, all data related to national security and strategic sectors (the Ecuadorian Constitution defines a list of strategic sectors: energy in all its forms, telecommunications, non-renewable natural resources, transportation and refining of hydrocarbons, biodiversity and genetic heritage, the radioelectric spectrum and water) should be located in computer centers located in Ecuadorian territory.

The bill also states that data that is not related to national security or strategic sectors, but is nonetheless relevant to the state, should preferably be found in computer centers located in Ecuadorian territory or in countries with data protection standards equal to or more demanding than those established in Ecuador.

Egypt

Divergence From Privacy Best Practices

In July 2020, Egypt enacted its first general privacy law, the Data Protection Law. The law, which imposes significant regulatory burdens on entities operating in Egypt, is expected to go into full effect following imminent passage of Executive Regulations. The law diverges from privacy best practices in several areas including onerous licensing and record keeping requirements, strict requirements for cross border data transfers, broad definitions of personal data and sensitive personal data, and criminal liability for violations.

[77] José Roberto Herrera, *The Recent and Relevant Copyright Bill in Colombia Law (1915-2018)*, Kluwer Copyright Blog (Sept. 5, 2018), http://copyrightblog.kluweriplaw.com/2018/09/05/recent-relevant-copyright-billcolombia-law-1915-2018/.

Cybercrime Law

Egypt President Abdel Fattah al-Sisi ratified a cybercrime law which obliges ISPs to block websites, whether hosted in Egypt or internationally, which are deemed to have committed a cybercrime that threatens national security, under threat of fines and/or imprisonment. Critics state that the law increases censorship and silences political opposition.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of for-hire vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

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

Unilateral Or Discriminatory Digital Tax Measures

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

Social Media Law

In 2018, Egypt passed a new law that requires all social media users with more than 5,000 followers to procure a license from the Higher Council for Media Regulation. Reports continue to show the government's increased use of censorship, website blocking, and mandated content filtering.[78]

In May 2020, Egypt's top media regulator issued Decree no. 26 of 2020 that enforces a strict licensing regime on Media and Press outlets.[79] This includes online platforms. Under the regulation, there is a 24-hour timeline for removing harmful content. Further, international companies are obligated to open a representative office within the country, while naming a liable legal and content removal point of contact. There are no safe harbor protections for foreign companies, and the regulation stipulates an average of $200,000 in licensing fees (which could conflict with the existing Media law of 2018).

European Union (EU)

Since the European elections in 2019, EU leaders have actively promoted a multi-pronged approach towards "technological sovereignty" or "digital sovereignty" as a main policy objective.[80] In updates to the EU's digital and

[78] Freedom House, *Freedom on the Net 2020: Egypt* (2020) ("At the end of the first quarter of 2020, 546 websites were reported blocked by the authorities."), *available at* https://freedomhouse.org/country/egypt/freedom-net/2020.

[79] Lexology, *The New Press and Media Regulation Era in Egypt* (May 16, 2020), *available at* https://www.lexology.com/library/detail.aspx?g=36e4982b-40ef-4fb5-9ee6-f4912a7271ac.

[80] Ursula von der Leyen, European Commission, Mission Letter, (Dec. 1, 2019), *available at* https://ec.europa.eu/commission/commissioners/sites/default/files/commissioner_mission_letters/president-elect_von_der_leyens_mission_l

industrial agenda calls for "technology sovereignty" have been advanced with regards to data, artificial intelligence, cloud services, as well as on the responsibility of online platforms and competition policy with the latter two packaged as the Digital Services Act and Digital Markets Act.

While the precise meaning of sovereignty or autonomy in the realm of technologies remains ambiguous, EU leaders have emphasized the desire to limit the market position of U.S. providers. For example, some EU officials have called for a range of policies to support "a European way of digitization, to reduce our dependence on foreign hardware, software and services."[81]

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

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

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

However, in the trade negotiation context, it is unfortunate that the EU's proposed text to facilitate cross-border data flows and digital trade includes self-judging provisions that risk increasing the likelihood of data localization, rather than reducing barriers.[82] The EU has presented this text within the context of the WTO Joint Statement Initiative on Electronic Commerce.

In its proposed AI Act, the European Commission has proposed a complicated bureaucratic structure that will threaten innovation and significantly raise the costs of bringing AI technologies to market in Europe. First, unlike the GDPR, there is no lead regulator. Instead, under the AI Act each Member State is directed to designate their own national supervisory authority, creating a risk of 27 different sets of standards and regulations. Second, although the Commission appropriately focuses on high-risk AI systems, the high-risk categories can be easily expanded to cover all kinds of AI systems without any clear process for stakeholder consultation. Third, the standards set for high-risk systems are incredibly high and under-specified, requiring that the systems achieve "an appropriate level of accuracy, robustness [and] cybersecurity", without any meaningful guidance on what this means. And some of the standards are nearly impossible to satisfy, such as "data sets shall be… free of errors and

Letter_to_thierry_breton.pdf.

[81] Axel Voss, A manifesto for Europe's digital sovereignty and geo-political competitiveness, *available at* https://www.politico.eu/wp-content/uploads/2020/01/Axel-Voss-Digital-Manifesto-2.pdf.

[82] Christian Borggreen, *How the EU's New Trade Provision Could End Up Justifying More Data Localisation Globally*, Disruptive Competition Project (May 14, 2018) ("The risk, as recently highlighted by the European Parliament, is that third countries will justify data localisation measures for data protection reasons. Unfortunately, the European Commission's proposed text will encourage exactly that. Its article B2 states that "each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy." This is essentially a carte blanche for non-EU countries to introduce data protectionism under the guise of "data protection". It doesn't even require that countries can demonstrate that such laws are necessary and done in the least trade restrictive way, as under existing international trade law, which the EU has long been a party to."), *available at* http://www.project-disco.org/european-union/051418eus-new-trade-provision-end-justifying-data-localisation-globally/ .

complete." And fourth, while the AI Act as originally introduced applies ex-ante third party conformity assessment to only a small subset of high-risk AI systems, European stakeholders are already urging the European Parliament to go further. The EU should be encouraged to create clear, consistent rules that focus on high-risk AI systems and provide sufficient predictability to companies investing in AI technologies through limiting expansion of high-risk areas and limiting the application of ex-ante third-party conformity assessments in the EU for non-EU AI products.

Digital Markets Act

The European Commission published its Digital Markets Act (DMA) proposal in December 2020. The DMA includes an array of extraordinary prohibitions that will apply exclusively to a small group of U.S. platforms. EU officials have been clear that they aim to use the DMA to reduce "dependence" on U.S. services and to support local industry, furthering the EU's current agenda of digital sovereignty.[83]

As proposed, the DMA would impose sweeping competitive restrictions on companies labeled as "gatekeepers," which the EU has defined narrowly to refer to a specific subset of U.S. technology providers, while excluding European digital rivals and other EU industries that compete with the U.S. technology sector. If enacted, US companies would be forced to comply with new obligations and regulatory restrictions that would damage their competitiveness with foreign firms, while the EU – as well as Russia, China, and other foreign rivals – would be entirely free of these restrictions.

Specifically, the DMA imposes a large number of restrictions on business activities that have previously been permissible under U.S. and EU law. Further, U.S. companies would have to meet a number of new requirements and restrictions under the DMA, including obligations to provide foreign rivals with access to proprietary and private information, ranking data, and internal tools; and restrictions on offering integrated services regardless of consumer welfare, security, and privacy considerations. For example, one of the most striking requirements under the DMA is an obligation for U.S. search engine providers to "provide access, on fair, reasonable and non-discriminatory terms, to search ranking, query, click and view data to other providers of such services." This sort of obligation has no parallel in any other national law, and would present significant privacy, security, and intellectual property concerns to consumers and business users of search services, while appropriating highly valuable trade secrets from U.S. companies. The DMA's enforcement provisions would also lower the bar for EU officials to impose structural remedies on U.S. companies. In addition to potential fines of up to 10% of global turnover, the DMA includes a long list of potential sanctions, divestment requirements, structural separation requirements, and broader remedies for "systemic non-compliance." This framework gives the EU substantial new authority to potentially restructure the operations of U.S. companies.

Finally, the DMA breaks with longstanding transatlantic regulatory and competition norms. The DMA recites a long list of per se harms and irrebuttable regulatory conclusions, and takes a "shortcut" around competition investigations and depriving in-scope companies of due process. Further, the DMA lacks meaningful standards or processes on fact-finding, evidence, economic analysis, and other due process and substantive legal protections associated with competition law. It appears that the EU's goal in circumventing competition norms is to lower evidentiary standards, shift burdens of proof, and eliminate opportunities to rebut findings—making it faster and simpler to issue crippling penalties and structural remedies on U.S. companies.

Copyright Liability Regimes for Online Intermediaries

The EU's passage and adoption of the Copyright Directive (Directive) in 2019 serves as a market access barrier for U.S. technology companies doing business in Europe, and underscores the industry's position that the strong and balanced U.S. copyright system has continued vitality in promoting the strongest content and technology sectors in the world. The principles behind Articles 15 and 17[84] are at odds with fundamental principles of U.S. law and

[83] Barbara Moens and Paola Tamma, *Macron and Merkel defy Brussels with push for industrial champions, Politico,* (May 18, 2020), *available at* https://www.politico.eu/article/macron-and-merkel-defy-brussels-with-push-for-industrial-champions/

[84] Article 15 was previously known as Article 11 and Article 17 was previously known as Article 13.

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 Copyright Directive is vague, untested, and creates significant risk for companies that are seeking to comply. Online services would be directly liable unless they did all of the following: (1) made best efforts to obtain a license, (2) made best efforts to "ensure the unavailability of specific works and other subject matter" for which the rightsholders have provided to the online service, and (3) "in any event" acted expeditiously to remove content once notified by rightsholders and made best efforts to prevent their future uploads. The last requirement effectively creates an EU-wide "notice and staydown" obligation. The other requirements are not mitigated by the inclusion of a "best efforts'' standard, in part because "best efforts" is a subjective but still mandatory standard open to abuse and inconsistent interpretations at the member state level.

Member States are currently working on implementation, with many Member States in final stages of legislation. It is important that Member States implement Article 17 in a harmonized fashion by transposing the text verbatim, rather than creating bespoke requirements, as is the case in Member States such as Germany.

The USTR should work with EU counterparts to ensure the Directive is implemented in a technologically neutral and future proof manner. EU countries should not in their implementing laws mandate either the use of a technological solution nor impose any specific technological solutions on service providers in order to demonstrate best efforts. Any requirement to render content unavailable must be proportionate and allow platforms the latitude needed to manage their systems without negatively impacting lawful user expression and legitimate uses of creative content.

It is imperative that national implementation does not impact on the freedom of contract and therefore diverge from the terms of the Directive by imposing mandatory licensing, "must carry and must pay" obligations.

As Member States craft legislation and guidance, a service provider which is made primarily liable for copyright infringements must be able to take steps to discharge this liability, otherwise this will ultimately lead to the demise of user-generated content services based in Europe — as it is materially impossible for any service to license all the works in the world and rightsholders are entitled to refuse to grant a license or to license only certain uses. Accordingly, mitigation measures are absolutely necessary in order to make Article 17 workable. Moreover, any measures taken by a service provider for Article 17 should be based on the notification of infringing uses of works, not just notification of works. A functional copyright system requires cooperation between information society service providers and rightsholders. Rightsholders should provide robust and detailed rights information (using standard formats and fingerprint technology where applicable) to facilitate efforts to limit the availability of potentially infringing content.

Last, but not least, EU Member States should refrain from inserting new payment obligations for authors and performers into their national laws (such as recently adopted in Germany) which would create commercial confusion that affects all stakeholders in the value chain.

Imbalanced Copyright Laws and "Link Taxes"

There remain concerns with the Copyright Directive on Article 15 and the creation of a press publishers' right.[85] Contrary to U.S. law and current commercial practices, Article 15 grants press publishers the exclusive right to either authorize or prohibit the use of their publications, impacting search engines, news aggregators, applications, and platforms that include snippets of content in search results, news listings, and other formats.

[85] *See TCO Joint Letter Ahead of the 4th Trialogue Negotiations, available at* https://www.ccianet.org/wp-content/uploads/2020/09/2020-09-21-TCO-joint-letter-ahead-of-the-4th-trialogue-negotiations.pdf.

As EU countries are now moving forward with the implementation, they should ensure that national legislation follows the terms of the Directive as closely as possible in order to ensure the maximum harmonization of rules in the EU and respect the exceptions and limitations inserted in the Directive (including the exceptions inserted in the Directive in Article 15 which allow linking and short news extracts to be posted without the need for a license) in order to maintain a fair balance between the various fundamental rights. Moreover, it is imperative that national implementation does not impact on the freedom of contract and therefore diverge from the terms of the Directive by imposing mandatory licensing, "must carry and must pay" obligations.

The Copyright Directive also does not harmonize the exceptions and limitations across the EU. The freedom of panorama exception (the right to take and use photos of public spaces) was left out of the proposal entirely. Moreover, while a provision on text and data mining is included, the qualifying conditions are too restrictive. The beneficiaries of this exception are limited to "research organizations," excluding individual researchers and startups.

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 visualization and indexing" to users.[86] Another U.S.-based platform was found liable because it engaged in indexing or other organization of user content.[87] 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."[88] 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.

Restrictions on Cross-Border Data Flows and Data Localization

As part of the EU-wide push for "technological sovereignty" there are proposals to craft EU industrial policy measures that will facilitate data localization and force out U.S. cloud providers. New measures would build and promote European cloud services at the expense of market-leading U.S. cloud services, with many policymakers calling for a "trusted" European cloud.

This has been supported by a number of European policy makers including, but not limited, to the following:

→ Internal Market Commissioner Thierry Breton has explicitly called for localization of European data on European soil as well as exclusive application of EU law on European data.[89]

→ French President Macron stated that Europe should not rely "on any non-European power" for data security.[90]

[86] *RTI v. Kewego* (2016).

[87] *Delta TV v. YouTube* (2014).

[88] *RTI v. TMFT* (2016).

[89] POLITICO Virtual Brussels Playbook Interview with Thierry Breton (Sept. 1, 2020), *available at* https://www.youtube.com/watch?v=L6qWkdq9xSQ&t=1445.

[90] *France's Macron says Europe has "lost" the global battle in cloud computing*, Reuters (Sept. 14, 2020), https://uk.reuters.com/article/us-france-tech-macron/frances-macron-says-europe-has-lost-the-global-battle-in-cloud-computing-idUSKBN26532N.

- European Council Conclusions from October 2, 2020 note that "the need to establish trusted, safe and secure European cloud services in order to ensure that European data can be stored and processed in Europe, in compliance with European rules and standards."[91]

- A declaration signed by 25 Member States on October 15, 2020 stated the need to develop "a truly competitive EU cloud supply" to reverse the current trend towards cloud infrastructure market convergence "around four large non-European players," and address "concerns over cloud users' ability to maintain control over strategic and sensitive personal and non-personal data." The Declaration recommends excluding providers of cloud services from the so-called European Cloud Federation if they are subject to "laws of foreign jurisdictions," unless they can demonstrate they have put in place "verified safeguards" to ensure that any foreign request to access EU (personal and non-personal) data is compliant with EU law.[92]

- U.S. cloud providers have been relegated to observers in the Franco-German GAIA-X cloud project.

There have already been attempts to establish an EU-wide cloud that would localize data within EU borders. Following the original announcement in 2019 by Germany, this June German Federal Minister of Economic Affairs and Energy Peter Altmaier and the French Minister of Economy and Finance Bruno Le Maire unveiled details on plans to create Europe's own cloud services, titled "GAIA-X".[93] According to the documents made available, the goal of the project is the "development of a trustworthy and sovereign digital infrastructure for Europe" and "GAIA-X will support the development of a digital ecosystem in Europe, which will generate innovation and new data-driven services and applications."[94]

At the same time, European criticisms of (non-EU) extraterritorial government data access laws and practices are at odds with Member States' support for the EU's proposed e-Evidence Regulation,[95] EU legislation akin to the U.S. CLOUD Act that would allow European law enforcement to request access to data irrespective of the location of the data.

Data Flow Restrictions And Service Blockages

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

In addition, the EU and some Member States have been proposing various restrictions on cloud services. As of this submission, the EU was preparing a Joint Declaration on cloud services that would erect protectionist barriers to entry into the European market. According to the leaked draft, providers *"must fulfil the need of cloud users to*

[91] General Secretariat of the Council, Special meeting of the European Council (Oct. 2, 2020), https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

[92] Declaration, Building the next generation cloud for businesses and the public sector in the EU, *available at* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70089.

[93] Liam Tung, *Meet GAIA-X: This is Europe's bid to get cloud independence from US and China giants*, ZDNet (June 8, 2020), https://www.zdnet.com/article/meet-gaia-x-this-is-europes-bid-to-get-cloud-independence-from-us-and-china-giants; *Germany Economy Minister Plans a European Cloud Services "Gaia-X"*, Financial World (Aug. 25, 2019), https://www.financial-world.org/news/news/economy/3046/german-economy-minister-plans-a-european-cloud-service-gaiax/; *Europa-Cloud Gaia-X Startet Im Oktober*, Handelsblatt (Sept. 3, 2019), https://www.handelsblatt.com/politik/deutschland/datenplattform-europa-cloud-gaia-x-startet-im-oktober/24974718.html.

[94] Federal Ministry for Economic Affairs and Energy (BMWi), *GAIA-X - the European project kicks off the next phase* (June 4, 2020), https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=13.

[95] Press Release, EU Council, Regulation on cross-border access to e-evidence: Council agrees its position, (Dec. 7 2018), https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

maintain control over strategic and sensitive data, including by ensuring that cloud capacities and services are not subject to the laws of foreign jurisdictions that could oblige access to be granted to EU data."[96]

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

Divergence From Privacy Best Practices

The European high court on July 16, 2020, issued a major decision that severely limits mechanisms for data flows to the United States and that, if not addressed, will seriously impede U.S.-EU digital trade and U.S. exports. In the *Schrems II* case, the European court invalidated the EU-U.S. Privacy Shield framework which more than 5,000 companies relied on for the transatlantic commercial data transfer.[97] The ruling created immediate legal uncertainty for thousands of companies, a majority of which are SMEs. Industry encourages the European Commission and the U.S. Administration to finalize a durable new framework to restore certainty on data flows between the world's most important trading partners.[98]

The EU also has been working on amending the existing ePrivacy Directive and proposed the "ePrivacy Regulation" in 2017.[99] The proposal seeks to expand the existing Directive, which only applies to telecommunication services, to all "electronic communication services" including over the top services.[100] Rules that were originally created for traditional telecommunication services would then apply to a variety of online applications from those that provide communications and messaging services to personalized advertising and the Internet of Things. The Commission justifies this scope expansion by observing that since the enactment of the ePrivacy Directive, services entered the market that "from a consumer perspective are substitutable to traditional services, but do not have to comply with the same set of rules."[101] This is based on a flawed understanding of the services at issue, and it is ignoring that the internet has flourished largely due to not treating over-the-top services like traditional telecommunications providers.

In addition, the EU General Data Protection Regulation[102] still contains considerable ambiguity and, as illustrated by the *Schrems II* case, described above, we are witnessing an increase in restrictive interpretations of its provisions which is hampering the ability for U.S. companies to operate in the EU. How EU data protection authorities choose to interpret the law will continue to have a significant impact on companies' ability to operate in the EU and offer consistent services and products across the globe.

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

---

[96] Council of the European Union General Secretariat, Working Paper (Sept. 8, 2020), *available at* https://www.politico.eu/wp-content/uploads/2020/09/Draft-cloud-declaration.pdf?.

[97] *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, case C-311-18, CJEU, *available at* https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[98] Press Release, *EU Top Court Strikes Down Privacy Shield, CCIA Calls for Urgent Legal Certainty and Solutions* (July 16, 2020), *available at* https://www.ccianet.org/2020/07/916160/.

[99] Proposal for a Regulation on Privacy and Electronic Communications 2017/003, *available at* http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241 [hereinafter "Proposal for ePrivacy Regulation"].

[100] *Id*. at art. 4 (CCIA is further concerned that the definition of an "electronic communication service" is not final and dependent on the also pending Electronic Communications Code).

[101] *Id*. at recital 6.

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

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,[103] as well as local content quotas relating to the Audiovisual Media Services Directive (AVMS).[104]

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. The new regulation would impose disproportionate requirements that are likely to create market access barriers for developers, platforms, and SMEs seeking access to the EU market.

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

Non-IP Intermediary Liability

In June 2021, a new terrorism regulation came into force that includes 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. [105] The regulation will become effective on June 7, 2022 and, *inter alia,* includes an obligation for hosting service providers exposed to terrorist content to implement "specific measures to protect its services against the dissemination to the public of terrorist content." While it will primarily rest with the host providers to determine the type and scope of specific measures, it remains to be seen whether the coordination mechanism between national enforcers in the EU will avoid impractical hurdles for U.S. companies, particularly resulting from conflicting assessments by different national authorities on the suitability of implemented measures."

---

[103] *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), *available at* http://europa.eu/rapid/press-release_MEMO-16-3009_en.htm; *Report On OTT Services,* BEREC (Jan. 29, 2016), *available at* 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), *available at* http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)569979 (last visited Oct. 25, 2016).

[104] European Commission, *Revision of the Audiovisual Media Services Directive (AVMSD), available at* https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd

[105] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, *available at* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32021R0784.

The internet industry supports the EU's goal of tackling terrorist content online and notes that hosting services remain committed to this goal through multiple efforts. However, the one-hour removal deadline, coupled with draconian penalties, will incentivize hosting services to take down all reported content, thereby chilling freedom of expression online.[106] Broad implementation of mandated proactive measures across the Internet is likely to also incentivize hosting services to suppress potentially legal content and public interest speech. This law applies broadly to platforms of all sizes, and could put a lot of burden on small and medium-sized players. Some might not have the resources needed to comply which could force them out of the EU market.

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.

The current proposal generally maintains clear safe harbors for intermediaries under the e-Commerce Directive. In addition, the proposal retains an important prohibition on general monitoring. Maintaining these principles will further foster innovation and protect fundamental rights. This is vital for companies of all sizes, including for small businesses, that stand to lose more than 23 billion EUR if a more stringent revision of liability rules is adopted.[107]

However, there are some proposed European Parliament amendments to the DSA that would severely limit customized or personalized online advertising and make it harder for European businesses and American exporters to reach new customers. U.S. government surveys show that new forms of online advertising have significantly reduced advertising costs for businesses throughout the economy, while giving customers wider choices and lower costs. The EU Parliament's amendments would damage US and EU interests by reducing the quality of advertising, making it harder for advertisers to find the right audience, and harming news publishers that rely on personalized advertising.

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.

---

[106] *See TCO Joint Letter Ahead of the 4th Trialogue Negotiations, available at* https://www.ccianet.org/wp-content/uploads/2020/09/2020-09-21-TCO-joint-letter-ahead-of-the-4th-trialogue-negotiations.pdf.

[107] Oxera, The impact of the Digital Services Act on business users: Policy Report (Oct. 23, 2020), *available at* https://alliedforstartups.org/wp-content/uploads/2020/10/Impact-of-DSA-on-EU-business-policy-paper-2020-10-23.pdf.

Restrictions On Cloud Service Providers

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

Cybersecurity Regulations

Secure network and information systems in the EU are needed in order to keep the online economy resilient. The first pillar of the EU cybersecurity strategy is the EU Cyber Security Act, which entered into force in June 2019.[108] It provides a cybersecurity certification framework as part of which the European Commission and the European Union Agency for Cybersecurity (ENISA) will develop and adopt an EU-wide cloud computing cybersecurity scheme by mid-2021. Industry is concerned that this scheme may set market access conditions to favor local providers. The second pillar of the EU strategy is the revision of the Directive on security of networks and information systems (NIS) and the critical infrastructure protection Directive (CI) that could lead to a significant increase in indirect oversight on cloud providers in Europe. These measures may constitute technical barriers to trade that would prevent non-EU companies from accessing the EU market.

Sharing Economy Barriers

EU treaties establish fundamental principles to ensure an adequate level of competition within the EU Single Market. The European Commission is the guardian of these treaties and is responsible for their enforcement between and within Member States. Across the EU, app-based service providers face barriers aimed at protecting incumbents, affecting the level of typical competition and infringing on principles such as the freedom of establishment, equality, non-discrimination and access to the profession. These shortcomings have been acknowledged in EU-funded sectoral studies but without any action by the EU.[109] The failure to enforce EU principles and to ensure effective competition in a level playing field creates barriers for new entrants, lowers the quality of services provided and raises prices for consumers.

Unilateral Or Discriminatory Digital Tax Measures

Since the introduction of a now-abandoned, digital services tax by the European Commission in 2018, national measures proliferated but then slowed as the OECD negotiations picked up. The EU is supportive of the OECD outcome and poised to implement the frameworks in the coming years.

Despite their OECD support, the EU has indicated that it may pursue an EU-wide digital levy to support economic recovery plans.[110]

For background, the European Commission presented a package of two digital tax proposals in March 2018.[111] The package contains two legislative proposals, including a Directive introducing "an interim tax on certain revenue from digital activities." This controversial DST was to be set at 3 percent of companies' gross revenues

---

[108] European Commission, *Shaping Europe's digital future, available at* https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

[109]European Commission, *Mobility and Transport, available at* https://ec.europa.eu/transport/sites/transport/files/2016-09-26-pax-transport-taxi-hirecar-w-driver-ridesharing-final-report.pdf

[110] Matt Schruers, *To Fund Emergency Measures, Tax Collectors Tap Tech*, Disruptive Competition Project (May 18, 2020), https://www.project-disco.org/21st-century-trade/051820-to-fund-emergency-measures-tax-collectors-tap-tech/.

[111] *Proposal for a Council Directive on the Common System of A Digital Services Tax on Revenues Resulting from the Provisions of Certain Digital Services*, https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en.

from making available advertisement space, intermediation services, and transmission of user data.[112] As explained in other country sections of these comments, national DSTs largely reflect this framework, with variations on rate and covered digital activities.

Complex VAT Registration And Compliance Requirements In Intra-EU Trade

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

Foreign Subsidies Proposal

The European Commission published a proposed regulation on May 5, 2021, to address "*distortions caused by foreign subsidies received by companies operating in the EU".*[113] The scope of the proposal is greater than any existing subsidy regulatory tool, and the European Commission has broad discretion to utilize the tool freely or target specific industry sectors. The proposed regulation provides far reaching new powers to investigate and sanction a broad range of incentives, based on a definition of "subsidy" that is broader than the definition included in the WTO Agreement on Subsidies and Countervailing Measures, to include the purchase of goods and services by government bodies. The proposed regulation grants the Commission substantial discretion to deem distortion to exist when a foreign subsidy improves the competitive position of the beneficiary in the EU market. The regulation introduces three new regulatory tools, the first of which is general investigative tool giving the Commission the ability to investigate based solely on suspicion of distortion, and could also oblige firms to disclose foreign incentives received in the last 3 years when participating in public procurement and ahead of merger and acquisition transactions. If, as a result of an investigation, the EU determines that an incentive that a company receives distorts the internal market, the Commission may assess corrective measures on the beneficiary to rectify the distortion, including fines up to 10 percent of global turnover, exclusion from procurement activities, divestment from EU markets and assets, publication of R&D results, and acquisition denial. Any business operating in the EU that benefits from non-EU incentives is within the Proposal's scope.

Extraterritorial Regulations and Judgments

In September 2019, the EU Court of Justice ruled that removed or delisted URLs from search engines should not apply worldwide.[114] The ruling honors EU residents' "right to be forgotten" (RTBF) without compromising the constitutional rights of citizens outside of the EU. The decision concludes that a service provider subject to the RTBF is not obligated to de-index outside of the EU.[115] However, the decision does leave the possibility for a data protection authority or a national court to ask, on a case-by-case basis, for the delisting of all versions of the

---

[112] *See* CCIA's 2018 NTE Comments for full criticism of the EU's DST, at 50, *available at* http://www.ccianet.org/wp-content/uploads/2018/10/CCIA-Comments-to-USTR-for-2019-NTE.pdf.

[113] European Commission, Proposal for a Regulation of the European Parliament and of the Council on foreign subsidies distorting the internal market (May 5, 2021), *available at* https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

[114] *Google LLC v. CNIL*, Case C-507/17, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1092623.

[115] *Id.* at ¶ 74 ("On a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and of Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), where a search engine operator grants a request for de-referencing pursuant to those provisions, **that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States**, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.") (emphasis added).

search engine, even outside the EU.[116] Further, a subsequent decision issued in October 2019 authorizing national courts to issue global content takedown injunctions indicates that EU courts may be trending in a direction that would conflict directly with the U.S. 2010 SPEECH Act, which was designed to combat libel tourism abroad.[117]

The GDPR also includes a "right to erasure" provision, which codifies the "right to be forgotten" and applies it to all data controllers. Under Article 17, controllers must erase personal data "without undue delay" if the data is no longer needed, the data subject objects to the processing, or the processing was unlawful.[118] Under the GDPR, the fine for noncompliance with these and other provisions can be up to 4 percent of a company's global operating costs. Putting the onus on companies to respond to all requests in compliance with the "right to be forgotten" ruling and Article 17 of the GDPR is administratively burdensome. For example, popular U.S. services have fielded hundreds of thousands of requests since the policy went into effect.[119] Processing these requests requires considerable resources because each request must be examined individually. Small and medium-sized enterprises that also offer similar services but without similar resources to field these requests could find that the "right to be forgotten" and "right to erasure" pose a barrier to entry into the EU. USTR should monitor the outcome of these requirements for adherence with international commitments.

[116] *Id.* at ¶ 72.

[117] *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd.*, Case C-18/18, dec. (Oct. 3, 2019) (interpreting the EU E-Commerce Directive prohibition on general monitoring provisions not to preclude a court of a Member State from (1) ordering an online service from removing content worldwide, within the framework of relevant international law, and (2) as well as ordering the removal of content that is "equivalent" or "conveys a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality"), *available at* http://curia.europa.eu/juris/document/document_print.jsf?docid=218621&text=&dir=&doclang=EN&part=1&occ=first&mode=req&pageIndex=0&cid=1986464.

[118] GDPR art. 17.

[119] Alex Hern, *Google takes right to be forgotten battle to France's highest court*, The Guardian (May 19, 2016), *available at* https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court.

EU Member State Measures

Austria

Non-IP Intermediary Liability Restrictions

In September 2020, Austrian lawmakers presented a new law for platform accountability, the Kommunikationsplattformen-Gesetz (KoPl-G), or Communication Platforms Act, is a "draft federal act on measures to protect users on communication platforms."[120] The draft law is part of a larger package targeting "Hass im Netz" (online hate), amending the Austrian civil and penal codes — as well as media law — well beyond the introduction of the Communication Platforms Act itself. The draft law is a NetzDG-style law regarding intermediary liability.[121]

Unilateral Or Discriminatory Digital Tax Measures

Austria implemented a 5 percent digital tax on revenues from digital advertising services provided domestically.[122] The global revenue threshold is 750 million euro, and domestic revenue threshold is 25 million euro. The tax, implemented in the Digital Tax Act 2020 (Digitalsteuergesetz 2020), became effective on January 1, 2020. "Online advertisement services'' include advertisements placed on a digital interface, in particular in the form of banner advertising, search engine advertising and comparable advertising services.[123] Per officials, a covered service is deemed to have been provided domestically "if it is received on a user's device having a domestic IP address and is addressed (also) to domestic users in terms of its content and design."[124] The tax also provides for the use of an IP address or other geolocation technologies to determine the location of the service.

The discriminatory motivations underlying this tax are clear, with U.S. companies being singled out as targets of this online advertising tax. Upon introduction, 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."[125]

---

[120]Draft Federal Act on measures to protect users on communication platforms (Communication Platforms Act), *available at* https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2020&num=544.

[121] London School of Economics and Political Science Blog, *A primer on Austria's 'Communication Platforms Act' draft law that aims to rein in social media platforms*, *available at* https://blogs.lse.ac.uk/medialse/2020/09/14/a-primer-on-austrias-communication-platforms-act-draft-law-that-aims-to-rein-in-social-media-platforms/.

[122] Austria: Legislation Introducing Digital Services Tax, KPMG (Oct. 29, 2019), https://home.kpmg/us/en/home/insights/2019/10/tnf-austria-legislation-introducing-digital-services-tax.html.

[123] Federal Ministry Republic of Austria, Digital Tax Act (2020), *available at* https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html (last visited Oct. 29, 2020).

[124] *Id.*

[125] Sebastian Kurz (@sebastiankurz), Twitter (Apr. 3, 2019, 1:44 AM), *available at* https://twitter.com/sebastiankurz/status/1113361541938778112*; see also* Parliamentary Correspondence No. 914, National Council: digital tax on online advertising sales decided, (Aug. 20, 2019), ("Internetgiganten wie Facebook oder Google müssen künftig Online-Werbeumsetze abführen. Um mehr Steuergerechtigkeit zu erreichen, soll nun auch die seit längerem in der Öffentlichkeit diskutierte Digitalsteuer umgesetzt werden; das dazu von ÖVP und FPÖ vorgelegte Abgabenänderungsgesetz 2020 hatte die nötige Stimmenmehrheit. Nunmehr müssen Internetgiganten wie Facebook, Google oder Amazon ab dem Jahr 2020 eine fünfprozentige Steuer auf Online-Werbeumsätze abführen haben. Konkret sind jene Unternehmen betroffen, die einen weltweiten Umsatz von 750 Mio. € bzw. einen jährlichen Umsatz aus Onlinewerbeleistungen von mindestens 25 Mio. € erzielen, soweit diese in Österreich gegen Entgelt erbracht werden. Aus den aus der Digitalsteuer resultierenden Einnahmen sollen jährlich 15 Mio. € an österreichische Medienunternehmen gehen." [Internet giants like Facebook or Google will have to pay for online advertising sales in the future. In order to achieve more tax justice, the digital tax that has long been discussed in public should now be implemented; the Tax Amendment Act 2020 presented by the ÖVP and FPÖ had the necessary majority of votes. Internet giants like Facebook, Google or Amazon must now pay a five percent tax on online advertising sales from 2020. Specifically, those companies are affected that achieve a worldwide turnover of € 750 million or an annual turnover from online advertising services of at least € 25 million, as far as these are rendered in Austria for a fee. From the income resulting from the digital tax, € 15 million should go to

On January 14, 2021, USTR determined that Austria's DST is unreasonable and discriminatory and burdens or restricts U.S. commerce. On June 7, 2021, USTR determined to take action in response in the form of additional duties of 25 percent on certain products of Austria, and it also determined to suspend application of the additional duties for up to 180 days. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, Austria should repeal its DST.

Belgium

Asymmetry in Competition Frameworks

The Belgian, Dutch, and Luxembourg competition authorities have proposed amendments to their competition regimes allowing for the imposition of remedies without proving harm to consumers for digital companies. This will increase legal uncertainty and open a path to use competition to slow down successful U.S. companies operating in these regions.

Digital Taxation

After rejecting a similar proposal in 2019, Belgium reintroduced a DST in June 2020. The tax would be 3 percent and applies to revenue derived from the selling of user data. The newly elected government announced that they would wait for an OECD solution. Industry is monitoring political developments.[126]

Sharing Economy Barriers

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

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

Unilateral Or Discriminatory Digital Tax Measures

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

Austrian media companies every year.]), *available at* https://www.parlament.gv.at/PAKT/PR/JAHR_2019/PK0914/.

[126] David Gaier, *INSIGHT: Belgium and Digital Taxation—Where do we Stand?*, Bloomberg Tax (Sept. 30, 2020), *available at* https://news.bloombergtax.com/daily-tax-report-international/insight-belgium-and-digital-taxation-where-do-we-stand.

Czech Republic

Unilateral Or Discriminatory Digital Tax Measures

Announced by the Ministry of Finance in July 2019,[127] the Czech Republic has been contemplating a 7 percent digital services tax (DST).[128] The tax, which has a similar structure to the French DST, would apply to companies that meet the following thresholds, either individually or as part of a group: global revenue exceeding EUR750 million; and revenue from supplying covered services in the Czech Republic exceeding CZK 100 million and the revenue from the supply of covered services in the EU amounts to at least 10 percent of total revenue in the EU. The structure of the tax will expressly target U.S. companies while insulating Czech competitors in the advertising and digital markets from scope of coverage. IA believes that the Czech Republic's DST draft law would be unreasonable and would discriminate against U.S. digital companies by creating a targeted burden on U.S. commerce. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, the Czech Republic should abandon consideration of its DST.

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.

[127] Press Release, *The Ministry of Finance Sends Draft Law in Digital Tax to Comment Procedure* (July 4, 2019), *available at* https://www.mfcr.cz/cs/aktualne/tiskove-zpravy/2019/mf-posila-do-pripominkoveho-rizeni-navrh-35609.

[128] *Czech Republic to Delay Proposed Digital Tax, Cut Rate to 5%*, Bloomberg Tax (June 10, 2020), *available at* https://news.bloombergtax.com/daily-tax-report-international/czech-republic-to-delay-proposed-digital-tax-cut-rate-to-5.

Finland

Data Flow Restrictions And Service Blockages

In a communication issued in 2018, the Finnish Ministry of Finance announced its intention to introduce a requirement for companies in the financial sector to build back-up systems in Finland in the event of exceptional circumstances and serious disruptions. According to this, in-scope companies would be subject to precautionary measures to maintain in Finland such information systems and information resources that are necessary for the uninterrupted operation of the financial markets. In July 2020, in order to assess any gaps in preparedness capacity, the FIN-FSA requested entities under scope to submit by December 31, 2020 an entity-specific plan on how to ensure the operability and accessibility of critical services for end customers in circumstances where foreign service provision is completely unavailable. Firms' preparedness plans will then inform the work of the Ministry of Finance, with a view to issue legislation on this in 2021. Effectively, this could represent an indirect data localization requirement, presenting a market barrier and a risk to free market and competition in Finland for CSPs which don't have local data centers.

Financial Services/Cloud Services

In a communication issued in 2018, the Finnish Ministry of Finance announced its intention to introduce a requirement for companies in the financial sector to build back-up systems in Finland in the event of exceptional circumstances and serious disruptions. According to this, in-scope companies would be subject to precautionary measures to maintain in Finland such information systems and information resources that are necessary for the uninterrupted operation of the financial markets. Effectively, this could represent an indirect data localization requirement, presenting a market barrier and a risk to free market and competition in Finland for CSPs which don't have local data centers. In July 2020, the FIN-FSA requested entities under scope to submit by December 31, 2020, an entity-specific plan on how to ensure the operability and accessibility of critical services for end customers in circumstances where foreign service provision is completely unavailable. Firms' preparedness plans were requested to inform the work of the Ministry of Finance, with a view to issue legislation on this in 2021. Due to extensive resistance from both the financial services industry and CSPs, the issue is currently on hold with no new legislation communicated from the Ministry of Finance during this year. The issue has not, however, officially been put to the side and thus requires continuous monitoring.

Data Localization Requirements for Patient and Pharmaceutical Data

In September 2021, the Finnish Institute for Health and Welfare launched a consultation regarding additional restrictions for the processing and storage of Finnish healthcare data. According to the draft decrees issued, systems that involve the provision of health and care services, and systems that contain particularly sensitive data (i.e., patient and pharmaceutical data systems) would be subject to a localisation requirement. According to the draft decrees, systems handling data that is considered necessary in abnormal situations (contingency or emergency planning) must continue to operate even when network connections are limited to Finland. The physical location limitation also covers administration, backups and other maintenance solutions. Requirements also include a restriction on governance authorities of other countries having direct or indirect access to the data. If implemented, CSPs without local data centers will not be able to access and support the majority of the healthcare sector in Finland. The industry is currently working to change this requirement together with CSPs and there is a good possibility that this threat can be mitigated. If there is no mitigation, this will become a barrier that can harm competition in Finland and restrict the free operation of the healthcare market, in particular for international CSPs.

France

Copyright Liability Regimes for Online Intermediaries

France proposed legislation in October 2019 intending to implement the EU Copyright Directive, through the ongoing audiovisual reform.[129] Previously, French officials indicated that filters would be required under implementing legislation.[130] The proposal does not appear to reflect even the text of the Directive, omitting mention of protection of exceptions and limitations, the principle of proportionality, or that the actions required by the liability standard cannot amount to a duty to monitor. Specifically, the proposal replaces the prohibition on removal of safeguards that allow users to rely on exceptions granted in Article 17(7) of the Directive.[131] Instead, there is only an obligation to inform users about relevant exceptions in terms and conditions.

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.

Digital Taxation

In March 2019, the National Assembly proposed a very broad law on combating hate speech ("Lutte contre la haine sur internet").[132] The law would require designated Internet services to take down hateful comments reported by users within 24 hours. The law targeted any hateful attack on someone's "dignity" on the basis of race, religion, sexual orientation, gender identity, or disability. If platforms in scope do not comply, they could face an administrative penalty of 4 percent of their global revenue and penalties could reach tens of millions of euros.

The French National Assembly adopted the law on May 13, 2020. However, the French Constitutional Court released a decision pertaining to the constitutionality of the new law on June 18, 2020.[133] The Court determined the legislation "undermines freedom of expression and communication in a way that is not appropriate, necessary and proportionate to the aim pursued" making the text not compatible with the French constitution. The French law required platforms to take down manifestly illegal content upon notification within 24 hours. Among others, the law targeted any hateful attack on someone's "dignity" on the basis of race, religion, sexual orientation, gender identity or disability.[134] The Court also struck down the one-hour removal deadline for terrorist propaganda and child pornographic contents as it contradicts the French Penal code (Art 227-3 and 421-2-5).

---

[129] See source (French): http://electronlibre.info/wp-content/uploads/2019/10/2019-09-30-PJL-audio-complet.pdf.

[130] Mike Masnick, *After Insisting That EU Copyright Directive Didn't Require Filters, France Immediately Starts Promoting Filters*, Techdirt (Mar. 28, 2019), *available at* https://www.techdirt.com/articles/20190327/17141241885/after-insisting-that-eu-copyright-directive-didnt-requirefilters-france-immediately-starts-promoting-filters.shtml.

[131] *Article 17: Both French and Dutch implementation proposals lack key user rights safeguards*, Communia (Jan. 10, 2020), *available at* https://www.communia-association.org/2020/01/10/article-17-implementation-french-dutch-implementation-proposals-lack-key-user-rights-safeguards/.

[132] Lutte contre la haine sure internet, Assemblee National, *available at* http://www.assembleenationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.

[133] Conseil constitutionnel [CC] [Constitutional Court] decision No. 2020-801DC, (June 18, 2020) (Fr.), *available at* https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

[134] *See* Press Release, CCIA, *Court Ruling Rejects Core of French Hate Speech Law* (June 18, 2020), *available at* https://www.ccianet.org/2020/06/court-rules-rejects-core-of-french-hate-speech-law/.

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

France first indicated that it will direct resources to build a national "trusted cloud" in 2019.[135] This follows France's "Cloud First" policy adopted in 2018 and public statements of distrust of U.S. services. For example, the French Economy Minister has characterized the U.S. CLOUD Act as an overstep into France's sovereignty and is helping local industry players exclude U.S. industry from public procurements.[136]

However, despite this good momentum, cloud adoption is still fragile in France from the U.S. CSP perspective. Indeed, the French Minister of Finance recently announced France's intention to build a national "trusted cloud." French CSPs have been requested by the French government to invest in the project, which could constitute a protectionist obstacle to the use of U.S. CSPs cloud in the public sector in France. Moreover, France and Germany released a joint statement on October 29, 2019 indicating their commitments to collaborate on a European data infrastructure.[137]

SecNumCloud

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

Sovereign Cloud Program

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

Sharing Economy Barriers

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

---

[135] Leigh Thomas, *France Recruits Dassault Systemes, OVH For Alternative to U.S. Cloud Firms*, Reuters (Oct. 8, 2019) ("France has enlisted tech companies Dassault Systemes and OVH to come up with plans to break the dominance of U.S. companies in cloud computing, its finance minister said on Thursday. Paris is eager to build up a capacity to store sensitive data in France amid concerns the U.S. government can obtain data kept on the servers of U.S. companies such as Amazon and Microsoft."), *available at* https://www.reuters.com/article/us-france-dataprotection/france-recruits-dassault-systemes-ovh-for-alternative-to-u-s-cloud-firms-idUSKBN1WI189.

[136] *Id.*

[137] Press Release, *Franco-German Common Work on a Secure and Trustworthy Data Infrastructure* (Oct. 29, 2019).

- *Platform liability:* French law holds app-based dispatchers of licensed transportation liable for the transportation service provided by the drivers using the app. The app-based dispatcher of licensed transportation, or "platform," is also responsible for making sure that the independent drivers and vehicles comply with the specifications listed hereafter.

- *Vehicle requirements:* For-hire vehicles must be less than six years old and equipped with at least four doors. They must have a minimum length of 4.5 meters, a minimum width of 1.7 meters, and 115 horsepower (electric or hybrid vehicles are exempt from these restrictions).

- *Exams:* French law requires prospective for-hire vehicle drivers to pass stringent exams. The exams include both written and practical sections, covering topics such as general culture, business management, and English language. Examination slots are offered infrequently and there is a delay of approximately 3 months between the written and practical exams. As a result, prospective for-hire vehicle drivers require between six and 12 months to become licensed. The average pass rate in 2018 was below 50 percent due to the difficulty of the process.

- *Capital requirements:* Drivers must provide €1,500 in equity or a bank guarantee when registering their company with the Ministry of Transportation.

- *Return-to-garage rule:* Between trips, drivers must return either to their registered place of business or to an authorized off-street parking space, unless a new trip request is received on the way to either place.

- *Geolocation prohibition:* French rules forbid for-hire drivers and apps facilitating their services from informing consumers about the availability and the location of a for-hire vehicle prior to a booking request—taxis face no such restriction.

Unilateral Or Discriminatory Digital Tax Measures

France has adopted a DST that is applicable to certain digital services provided in France in which there is user involvement. The rate is set at 3 percent of "qualifying" revenues and applies to companies with worldwide revenues of at least €750 million and French "qualifying" revenues of at least €25 million.[138] On July 16, 2019, USTR initiated a Section 301 investigation of the French DST. On December 6, 2019, USTR determined that the French DST is unreasonable and discriminatory and burdens or restricts U.S. commerce. On July 16, 2020, USTR determined to take action in response in the form of additional duties of 25 percent on certain products of France, and it also determined to suspend application of the additional duties for up to 180 days. On January 12, 2021 USTR further determined to suspend the duties until further notice.

In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, France should repeal its DST.

Germany

Copyright-Related Barriers

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

[138] *GAFA tax: a major step towards a fairer and more efficient tax system* (Apr. 11, 2019), *available at* https://www.gouvernement.fr/en/gafa-tax-a-major-step-towards-a-fairer-and-more-efficient-tax-system.

Discriminatory Or Opaque Application Of Competition Regulations

A new competition law entered into force in Germany in January 2021 that allows the German Federal Cartel Office ("FCO") to subject certain companies to prohibitions and penalties even if there has been no showing of an abuse of a dominant market position, which would be flatly inconsistent with U.S., EU and global practice. The companies targeted are online platforms and other companies that German authorities accuse of "transcending" their market power in a given market because, for example, they are vertically integrated or control sensitive business data. After the new law became effective, the FCO immediately used its new powers and initiated investigations against US-based companies Facebook, Google, Amazon, and Apple alleging that these companies are of "paramount significance for competition across markets."

Other rules in the new law also target online platforms, including a rule that makes it easier for competition authorities to oblige platforms to provide access to data. Many of the rules include fuzzy definitions of longstanding concepts in competition law (such as "essential facilities") and depart from global competition norms, including by shifting the burden of proof away from the FCO and towards targeted companies. Together these rules come close to introducing a sector-specific regulation of online platforms by means of antitrust law and could serve as a model for other countries worldwide that are looking to challenge or undermine U.S. businesses operating in this sector. Overall, the new regime is likely to negatively affect U.S.-German digital trade.

Non-IP Intermediary Liability Restrictions

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

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

Further concerning is the potential domino effect of this policy on other regimes. This law has been used as the basis for a number of concerning content regulations including legislation in Russia, Singapore, Turkey, and Venezuela.[139] Cases arising under this law will also have implications on extraterritoriality.[140]

In a 2020 review of the law, the German government has acknowledged flaws and needs for improvement.[141] In June 2020, there were further amendments proposed.[142]

---

[139] Jacob Mchangama & Natalie Alkiviadou, *The Digital Berlin Wall: How Germany built a prototype for online censorship*, EURACTIV (Oct. 8, 2020), *available at* https://www.euractiv.com/section/digital/opinion/the-digital-berlin-wall-how-germany-built-a-prototype-for-online-censorship/.

[140] *See* EU Section of these comments.

[141] Bundesministerium der Justiz und für Verbraucherschutz, Evaluierungsbericht zum Netzwerkdurchsetzungsgesetz (NetzDG) vorgelegt (Sept. 9, 2020), *available at* https://www.bmjv.de/SharedDocs/Artikel/DE/2020/090920_Evaluierungsbericht_NetzDG.html.

[142] Madeline Earp, *Germany revisits influential internet law as amendment raises privacy implications*, Committee to Protect Journalists (Oct. 7, 2020), *available at* https://cpj.org/2020/10/germany-revisits-influential-internet-law-as-amendment-raises-privacy-implications/.

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

Restrictions On U.S. Cloud Service Providers

The German Economy Minister announced in 2019 that they were working on a plan to create Europe's own cloud services, titled "GAIA-X".[144] This project would connect existing central and decentralized infrastructure solutions via open-source applications and interoperable solutions. As noted above, France and Germany released a joint statement on October 29, 2019 indicating their commitments to collaborate on a European data infrastructure. U.S. cloud service providers could be disadvantaged from operating in these markets as a result of these protectionist measures.

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.

[143] German Federal Film Board, *Film Levy*, *available at* https://www.ffa.de/film-levy.html.

[144] Sourav D, *Germany Economy Minister Plans a European Cloud Services "Gaia-X"*, Financial World (Aug. 25, 2019), *available at* https://www.financial-world.org/news/news/economy/3046/german-economy-minister-plans-aeuropean-cloud-service-gaiax/; Barbara Gillmann, *Europa-Cloud Gaia-X Startet Im Oktober*, Handelsblatt (Sept. 3, 2019), https://www.handelsblatt.com/politik/deutschland/datenplattform-europa-cloud-gaia-x-startet-imoktober/24974718.html.

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 committee 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.[145]

Italy

P2B EU Regulation

Italy implemented the EU Regulation on Platform to Business ("P2B") by appointing the Communications Authority ("Agcom") as the national agency in charge of its application and enforcement. Agcom implemented the Regulation by imposing burdensome obligations on platforms that will be subject to the Regulation in Italy in a way that goes well beyond the scope of the P2B regulation and is something unique to Italy, as no other agencies across the EU are asking for similar obligations. Agcom passed two resolutions that implement the Regulation by: (i) forcing entities providing intermediation services to register on a national registry – which involves the payment of a yearly contribution to support Agcom's activities related to P2B ("ROC resolution"); and (ii) requesting registered entities to provide extensive disclosure of internal financial and accounting data, which goes well beyond the scope of the P2B Regulation. Agcom will soon also approve a resolution setting the amount of the yearly contribution, which will be capped at a maximum of 2 percent of the national turnover. As a result, the estimated annual contribution could amount to up to EUR 4 million based on 2020 turnover figures for Italy. The contribution, as well as such extensive data disclosure requirements, is unique to Italy, as no other agencies

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

across the EU are asking for similar obligations. Industry has challenged before the Administrative Court (TAR del Lazio) the two Agcom resolutions and we expect a final decision by the Administrative court by end of 2022 (that can be further appealed before the Council of State).

Ex-Ante Regulation On Digital Platforms

In March 2021, the Italian Competition Authority ("ICA") came forward with proposals for the Italian government to reform Italian competition law to more effectively tackle anticompetitive conducts by digital platforms. The Italian government could include the ICA's proposals into a draft annual law on competition bill that will be in place by late-2022. First, the ICA proposed to introduce a presumption of economic dependence in the commercial relationships of third-party business users with digital platforms that offer an intermediation service, where these platforms play a critical role in reaching end users and suppliers, including as a result of network effects and data accumulation. As this is a rebuttable presumption, digital platforms will have the opportunity to demonstrate that this relationship of economic dependence does not exist. Second, the ICA proposed to introduce new legislation, based on Germany's 10th amendment to its competition law, which would designate certain companies as "undertakings of primary importance for competition in more than one market." These companies would be prohibited from pursuing certain conduct, unless they can demonstrate that it is objectively justified. Prohibited conduct listed in the proposed amendment includes: (i) self-preferencing; (ii) strategically using data to erect barriers to entry; (iii) providing third party business users with insufficient information on their performance on the platform; and (iv) making the provision or quality of a service conditional upon data transfer. Failure to comply with these rules could lead the ICA to impose behavioral or structural remedies.

Audiovisual Services Directive Implementation

Italy is implementing the EU Audiovisual Media Services Directive ("AVMS-D"). The implementing measure in question envisages a significant increase in the mandatory investment quotas in local productions endangering international and local investments. Italy is implementing EU AVMS-D (Directive 2018/1808) through a Legislative Decree ("Dlgs") which delegates the Government to adopt the implementing measures. The Dlgs provides, among other things, the introduction of a mandatory investment quota in European works (a quota that includes Italian works) which would gradually (until 2025) grow up to 25 percent of the given company's net revenues of the previous year. As also underlined by other local/international players (TV broadcasters, Cable TV, streaming providers), such a high investment quota would jeopardize Italy's attractiveness for the audio-visual sector and create an environment hostile to investments in general. If the measure is approved in the current text, in 2025 Italy would have the highest mandatory investment quota in the whole of the EU.

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.

Italy is about to adopt its legislation transposing the European Copyright Directive. This law introduces problematic provisions introducing a "must negotiate must pay" obligation on platforms, therefore going far beyond the terms of the EU Directive. The law about to be adopted in November 2021, tilts rights in favor of just rights holders, in an approach that will significantly harm American businesses.

The industry therefore encourages USTR to reiterate the U.S. government's opposition to these measures and to encourage Italy to comply with its obligations through the upcoming U.S./EU bilateral trade negotiations. Departures by the EU from the proven, successful policies that both sides of the Atlantic have followed to date risks thwarting the continued growth of innovative and creative industries.

Sharing Economy Barriers

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

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

Unilateral Or Discriminatory Digital Tax Measures

Italy's 2020 Budget introduced a 3 percent digital services tax closely aligned with the EU's original proposal.[146] Covered services started accruing tax on January 1, 2020, and payments are due in 2021. The global revenue threshold is set at 750 million euros, and the local threshold is 5.5 million euros. The tax applies to revenue derived from the following digital activities: (1) the "provision of advertising on a digital interface targeted to users of the same interface"; (2) the "provision of a digital multilateral interface aimed at allowing users to interact (also in order to facilitate the direct exchange of good and services)"; and (3) the "transmission of data collected from users and generated by the use of a digital interface."[147]

The tax is expected to predominantly affect U.S. firms. 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.[148] It appears that this remains the case with the current tax.

On June 2, 2020, USTR initiated a Section 301 investigation into Italy's DST. On January 6, 2021, USTR determined that Italy's DST is unreasonable and discriminatory and burdens or restricts U.S. commerce. On June 7, 2021, USTR determined to take action in response in the form of additional duties of 25 percent on certain products of Italy, and it also determined to suspend application of the additional duties for up to 180 days. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, Italy should repeal its DST.

Poland

Copyright-Related Barriers

In January 2017 the CJEU in the case of *OTK v. SFP*[149]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

[146] Italy included a digital tax in the Italian Budget Law (2019), (Law no.145/2018), but never took the final steps to implement the tax.

[147] *Tax Alert: Italy Digital Services Tax Enters into Force*, EY, *available at* https://www.ey.com/en_gl/tax-alerts/ey-italys-digital-services-tax-enters-into-force-as-of-1%C2%A0january-2020 (last accessed Oct. 27, 2020).

[148] *Web tax in arrivo*, Adnkronos (Dec. 19, 2018), *available at* https://www.adnkronos.com/soldi/economia/2018/12/19/web-tax-arrivodi-maio-rassicura-solo-per-gigantirete_JEfFksy3wkwzPPJaG7vxuI.html.

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

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.

Restrictions On Cloud Service Providers

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

Problematic Laws And Proposed Legislation

Industry is concerned about the following laws and proposed legislation:

- → Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC – The Directive provides for measures aiming at improving the position of rights holders to negotiate and be remunerated for the exploitation of their content by online services giving access to user-uploaded content. The Directive has yet to be implemented.

- → The draft act on the protection of freedom of expression in online social networks (a legislative initiative currently under consultation) – The draft introduces a new authority to ensure respect for freedom of expression, obtaining information, dissemination of information, expression of religious and philosophical beliefs and freedom of communication through online social networking services. There are concerns that the new law may be used for online censorship.

- → The draft act on book market protection (an industry initiative currently under consultation) – The draft act sets out an obligation on publishers and importers to set fixed prices for books, eBooks and audiobooks, which will be valid for a period of 6 full calendar months. This significantly limits the free pricing of these products and can be problematic for websites that provide access to eBooks and audiobooks for a specific monthly subscription.

- → Proposal of an income tax for the largest companies (minimum tax) included in the draft act of comprehensive tax reform, implementing the announcements made in the Polish Deal (a legislative initiative adopted by the lower chamber of Parliament) – this legislation sets out a tax of a supplementary nature that applies to entities subject to CIT and Tax Capital Groups, whose share of income in revenues (other than from capital gains) will be less than 1 percent, or which will incur a loss for a given tax year. The tax is aimed at large corporations not paying taxes in Poland.

- → Proposal of advertisement tax (after pre-consultation) – this measure proposes to levy on all broadcasters and publishers, including major tech companies. All entities conducting business activity in the scope of conventional advertising (press, radio, TV) and internet advertising will be subject to the obligation to pay the fee.

Portugal

Sharing Economy Barriers

Any driver seeking to provide app-based transportation services outside of the traditional taxi industry must be licensed under the for-hire category. In addition, for-hire platforms will face restrictions that will limit their capacity to compete.

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

Spain

Copyright-Related Barriers

In Spain, reforms of the *ley de propriedad intelectual* in 2014 resulted in an unworkable framework, requiring "equitable compensation" for the provision of "fragments of aggregated content" by "electronic content aggregation service providers."[150] 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.[151]

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.[152] An economic study prepared by the Spanish Association of Publishers of Periodical Publications found that the result of *ley de propriedad intelectual,* which was meant to benefit publishers, was higher barriers to entry for Spanish publishers, a decrease in online innovation and content access for users, and a loss in consumer surplus generated by the internet. The results are most concerning for smaller enterprises facing drastic market consolidation and less opportunity to compete under the law.[153]

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

---

[150] Boletín Oficial de las Cortes Generales, Congreso de los Diputados, Informe de la Ponencia: Proyecto de Ley por la que se modifica el Texto Refundido de la Ley de Propriedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, No. 81-3 (July 22, 2014).

[151] El Confidential, *Nuevo intento de imponer el canon AEDE: piden a Menéame 2,5 millones de euros al año* (Feb. 7, 2017), *available at* https://www.elconfidencial.com/tecnologia/2017-02-07/canon-aede-meneame-internet-facebook-agregadores_1327333/ (Spanish).

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

[153] *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), *available at* 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

Spain is considering a draft DST, with a similar structure to the French DST, which would apply a 3 percent tax to revenues from targeted advertising and digital interface services. This tax would apply only to companies generating at least €750 million in global revenues for all services and €3 million in in-country revenues for covered digital services.

On June 2, 2020, USTR initiated a Section 301 investigation into Spain's DST. On January 14, 2021, USTR determined that Spain's DST is unreasonable and discriminatory and burdens or restricts U.S. commerce. On June 7, 2021, USTR determined to take action in response in the form of additional duties of 25 percent on certain products of Spain, and it also determined to suspend application of the additional duties for up to 180 days. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to

establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, Spain should repeal its DST.

Royal Decree – Law 7/2021 - Sales Of Goods And Supply Of Digital Content Directives

Spain rushed through directives (Royal Decree – Law 7/2021 - Sales Of Goods And Supply Of Digital Content Directives) under an emergency procedure (RD-L) involving no consultation, impact assessment, or other stakeholder involvement. The directives were directly approved by the Council of Ministers without being previously announced, despite the relevant implementing act diverging significantly from the text of the directives. Apart from this approach being incompatible with the general principles of transparency and stakeholder involvement to which member states signed up to under the Better Regulation initiative, the divergence from the EU texts risks creating barriers to trade, fragmenting the Single Market, and undermining legal certainty. The government justified the use of such an omnibus RD-L by stating that it was late in meeting the implementation deadlines of the directives. However, the government did not just transpose the directive as they were. In most cases, the government observed the usual obligation to conduct a public consultation and publish an impact assessment. Despite their importance for many sectors, including ours, this obligation was not observed with respect to the Sales of Goods and Supply of Digital Content Directives. Implementing such divergent rules without a proper impact assessment creates major legal uncertainty, especially for smaller cross-border players, and in general creates a market barrier for traders and manufacturers, requiring them to operate differently in Spain in comparison to other markets.

With respect to repair and after sales services, while Directive (EU) 2019/771 should not impose, as an objective requirement for conformity, an obligation on sellers to ensure the availability of spare parts throughout a specific period of time, the law sets such requirement: producers must ensure the existence of (i) an adequate technical service, as well as (ii) spare parts for a minimum period of 10 years from the date on which the good ceases to be manufactured.

RTVE (National Public Service Media Organism) Levy

The Spanish government aims to use the transposition of the Audiovisual Media Services Directive (AVMSD) as an instrument to mandate Video On Demand services (such as Prime Video) and video-sharing platforms (such as Twitch) to finance the public broadcaster RTVE by paying a levy equal to 1.5 percent of their Net Annual Revenue.

The obligation to finance RTVE was first introduced when the government decided to prohibit publicity on RTVE, so it needed to obtain funds from other sources. This levy is currently paid by the following players with varying rates: (1) Local free TV: 3 percent of net revenue, (2) Pay TV: 1.5 percent of net revenue and (3) Telecoms: 0.9 percent of net revenue. After 15 years of lobby, the Telcos will be exempt from this obligation with the new law.

Sweden

Copyright-Related Barriers

A 2016 Supreme Court ruling[154] 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.

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

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

Restrictions On U.S. Cloud Service Providers

U.S. CSPs continue to face challenges in Sweden caused by the conflict of law perception between Swedish law (disclosure under the Secrecy Act) and the U.S. CLOUD Act fueled in part by protectionist sentiment. Since the first negative statement by the eSam legal expert group in late 2018, we have seen a proliferation of negative statements, guidelines, and opinion pieces emerging based on misconceptions about the U.S. CLOUD Act, questioning whether it is compatible with Swedish law for the public sector to use U.S. CSPs. A formal public investigation began in 2019, and will run until Q3 2021 to consider 1) the legal preconditions for outsourcing IT operations and 2) more durable forms of coordinated state IT operations. AWS is currently engaged with State and Commerce to put pressure on Sweden to resolve the issue. The U.S. Department of Commerce at the U.S. Embassy to Sweden has engaged on this issue, but the issue remains unresolved.

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 taximeter (or secure an exemption) and must be connected to a central accounting system, making it more difficult for drivers to report their taxes when working via apps.

Hong Kong

Copyright-Related Barriers

Previously, Hong Kong had considered measures to bring its copyright law in line with the realities of the 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 the national digital economy.

Data Flow Restrictions And Services Blockages

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

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.

National Security Law

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

The national security law allows the Hong Kong authorities to request message publishers, platform service providers, hosting service providers and/or network service providers to remove a message deemed to constitute an offense endangering national security; restrict or cease access by any person to the message; or restrict or cease access by any person to the platform or its relevant parts. The Hong Kong authorities have reportedly demanded that internet service providers block access to websites in Hong Kong. Website blocks are barriers to maintaining a free and open internet which is critical to digital trade.

Cybersecurity of Critical Information Infrastructure Bill

The Hong Kong government announced a plan to introduce a bill to strengthen the cybersecurity of critical information infrastructure in Hong Kong in 2022. While no detail has been made available as of October 2021, USTR should ensure that no restrictions on cross-border data flows and no data infrastructure localization mandates are included as part of the new law. Any new data localization requirements will put US companies at a competitive disadvantage vis-a-vis their Chinese and Hong Kong competitors.

India

Local Content Requirements

Aligned with the government of India's continued rhetoric on self-reliance, the Public Procurement (Preference to Make in India), Order of 2017 and subsequent revisions mandates that only Class-I suppliers (with local value addition >50 percent) and Class-II suppliers (local value addition – 20 percent to 50 percent) are eligible to bid for Government procurement. This is applicable to both products and services. While this order and compliance to this order is applicable to all entities, Indian or foreign, it poses a significant challenge to software and cloud service providers CSPs to demonstrate local value add. This model does not take into account the investments and other contributions made by CSPs that enable the Indian Tech ecosystem and their global competitiveness, such as skilling initiatives, Cloud innovation centers, quantum computing lab etc. need to certify their percentage of local content, for which they rely on their vendors' local value addition as well.

Local Technical Standards

The Indian government's think tank, the NITI Aayog, launched the "Data Empowerment and Protection

Architecture" (DEPA) in September 2021. The DEPA is a consent-based framework for individuals to securely access and share their information between businesses. By proposing a new technological architecture consisting of India-specific data protection, processing, and sharing standards, the DEPA could lead to trade restrictive standards and inflict unnecessary burdens on foreign companies.

Equalization Levy

In March 2020, the Indian Parliament expanded the scope of India's existing "equalization levy" in its amended national 2020 Budget.[155] This included a new two percent tax on the sale of goods and services by non-Indian companies over the Internet into India. A wide range of companies are required to pay this tax, given the broad definition of those in scope. Without any public consultation, the tax was set to apply beginning April 1, 2020.

While structurally different from DSTs from European countries, the tax is similar insofar as it discriminates against U.S. firms and exempts local businesses. Under the tax, "e-commerce operators" are defined as "non-residents who own, operate or manage a digital or electronic facility or platform for online sale of goods, online provision of services, or both." Pursuant to this definition, the scope is far broader than DSTs such as those in Europe. Further, the threshold is set at approximately $267,000 compared to the 750 million euro global threshold.

On June 2, 2020, USTR initiated a Section 301 investigation into India's DST. On January 6, 2021, USTR determined that India's DST is unreasonable and discriminatory and burdens or restricts U.S. commerce. On June 7, 2021, USTR determined to take action in response in the form of additional duties of 25% on certain products of India, and it also determined to suspend application of the additional duties for up to 180 days. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, India should repeal its DST. In the meantime, USTR should reject pressure to terminate its Section 301 investigation while the DST remains in effect.

Proposed Regulations on Cloud Services

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

E-Commerce Policy

The Department for Promotion of Industry and Internal Trade (DPIIT) launched a consultation on the Draft National e-Commerce policy that outlined a number of concerning policy proposals including further restrictions on cross-border data flows and restrictions on foreign direct investment. The development of the draft Policy had significant process and representation concerns. Initially released in January 2019, the draft Policy represents the government of India's official position on a host of digital economy issues. The 2019 draft was explicitly discriminatory and contemplated: (1) broad-based data localization requirements and restrictions on cross-border data flows; (2) expanded grounds for forced transfer of intellectual property and proprietary source code; (3) preferential treatment for domestic digital products and incentives for domestic data storage in India (e.g., provision of infrastructure; incentives to domestic data center operators). The policy also introduces the notion of

[155] *India: Digital Taxation, Enlarging the Scope of 'Equalisation Levy'*, KPMG (Mar. 24, 2020).

community data as a "national resource" where countries are "custodians" over data. The rules also impose obligations on all e-commerce entities without regard to unique e-commerce models and relationships between the entities, buyers and sellers. It is also unclear how the requirement for every e-commerce entity to register itself with the DPIIT is connected with protection against unfair trade practices by e-commerce entities, and creates an arbitrary and artificial distinction between offline sellers and e-commerce entities as registration requirements do not apply to offline sellers. Such additional non-tariff barriers have a dampening impact on the market access of foreign players into the Indian e-commerce market.

A revised draft of the draft Policy has been in the works ever since. Media reports have suggested the following: (i) certain categories of data such as defence, medical records, biological records, cartographic data, and genome mapping data should not be transferred outside India; (ii) certain categories of e-commerce data should be mirrored/stored in India (with the government/a proposed e-commerce regulator deciding the categories). Such proposals, if implemented, would significantly affect cross-border flows of data and pose barriers to free trade. However, there is no visibility into the revised draft Policy yet.

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,[156] 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

In September 2019, the Ministry of Electronics and Information Technology (MeitY) constituted a Committee of Experts on Non-Personal Data to deliberate on a governance framework for non-personal data (NPD). In August 2020, it released a report outlining a mandatory sharing and access framework for NDP for consultation. The revised report based on stakeholder comments was released in December 2020 and contained significant changes. The positive changes were exclusion of data processors from the scope of the NPD framework (the revised report expressly mentioned CSPs and SaaS providers as one such type of data processor); no mandatory requirement for business-to-business sharing of NPD; no classification of NPD into public, private, and community NPD; recommendation that the personal data protection bill not expand in scope to include NPD. However, the proposed framework for NPD continues to be problematic due to the vague and wide scope of key concepts such as "NPD" and "public interest," and the retention of the mandatory NPD sharing requirements. Data localization requirements have also been retained for "sensitive" NPD. 'Sensitive' NPD would accordingly be subject to data localization requirements as per the PDP Bill.

The reconstituted Parliamentary Committee on the Personal Data Protection Bill is considering expanding the scope of India's PDP Bill to include all data and reconfigure it as a Data Protection Bill. The PDP Bill already contains a provision (in Section 91) that creates a legal basis for the sharing of "Non-Personal Data" between corporations and their competitors or government. The proposed Framework would require mandatory sharing and access to aggregated data held by private companies, and compel industry to share this data with competitors and government agencies. This would pose conflicts with obligations under international commitments relating to IP and trade secrets protection by mandating disclosure of protected and business confidential information. Further, the Framework would impose additional localization mandates and disclosure requirements. A wide coalition of industry has raised concerns with these recommended measures that would "create powerful disincentives for India's innovation ecosystem."[157] There is a chance that the mandatory sharing of non-personal

[156] 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 . . .").

[157] Global Industry Statement on Non-Personal Data Report (Sept. 18, 2020), *available at* https://www.ccianet.org/wp-content/uploads/2020/09/Global-Industry-Statement-on-Non-Personal-Data-Report-final.pdf.

data will be included in the scope of the PDP Bill. The PDP Bill specifically excludes anonymised data from its scope. However, it creates an exception for the government to direct any data fiduciary or processor to share any anonymised data or other "non-personal data." The two use cases defined are (1) to enable better targeting of service delivery; or (2) to promote evidence-based policy making. These use cases are poorly defined. There is no clear rationale for including this provision in the PDP Bill. It is also a departure from the draft Bill and the Committee's report. Moreover, since a separate government committee is currently examining the issue of NPD comprehensively, any proposed framework for NPD should be deferred until the PDP Bill is passed and appropriate standards, rules and regulations have been issued (e.g., on anonymisation). It is also not clear with whom such data must be shared and what the modalities of such transfer will be (payment, data exchanges, etc. This provision could raise concerns around privacy and issues with the allocation of liability for companies, especially since the re-identification of de-identified data is a criminal offense.

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

Data Flow Restrictions And Service Blockages

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

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

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

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

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

data storage and information security systems. Furthermore, the notification came unannounced and companies had been given a short 6-month window for compliance. Since then, FAQs have been released and the regulator worked with various entities to approve their roadmap for compliance. Since April 2021, the localization conditions are being enforced.

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, discussed above. These would harm a wide range of U.S. exporters to India and damage India's domestic digital economy. For example, the Data Protection Bill would require companies to store a copy of all "sensitive personal data" and mandating that "critical" personal data can only be processed within India. These definitions of personal data all remain very unclear and, if not addressed, will create significant market access barriers for U.S. firms doing business in India.

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

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

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

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

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

Discriminatory Or Opaque Application Of Competition Regulations

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

In addition, there may be more that the CCI can do to protect the confidential information of investigated parties and third parties. The improper disclosure of information, and information leaks more generally, can have a

detrimental impact on the investigatory process and the standing of the agency. Providing adequate protections for this information can increase the quality of investigations by encouraging cooperation and voluntary submission of confidential information.

Barriers To Mobile Payments

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

Blocking Foreign Direct Investment

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.[158]

[158] *India Shuts Down Kashmir Newspapers Amid Unrest*, Al Jazeera (July 17, 2016), *available at* 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) (reporting on the practices of the Jammu and Kashmir governments to "increasingly [use] a communication blackout to prevent unrest in the valley."), *available at* http://india.blogs.nytimes.com/2012/10/03/youtube-and-facebook-remain-blocked-in-kashmir/?_r=0

Non-IP Intermediary Liability Restrictions

USTR correctly highlighted numerous problems with India's non-IP liability framework in the 2020 National Trade Estimate:

> The absence of a safe harbor framework for Internet intermediaries related to non-IP-protected content shared by third parties 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 non-IP third-party user content: any citizen can complain that certain content is "disparaging" or "harmful," and intermediaries must respond by removing that content within 36 hours. Draft regulations announced in late 2018 (the "Information Technology (Intermediary Guidelines) Rules 2018") threaten to further worsen India's intermediary liability protections. These draft rules would require platforms to become proactive arbiters of "unlawful" content, shifting the onus of the state to private parties.
>
> If these draft rules come into force, they will incentivize overly restrictive approaches to policing non-IP user-generated content and will undermine many Internet-based platform services.

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

Unfortunately, the publication of draft rules to amend India's intermediary guidelines include additional problematic requirements on issues such as the "traceability" of originators of content, local incorporation requiring certain intermediaries to establish a physical office in India, proactive filtering, and compressed timelines for content removal.[159]

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. The 2019 draft e-commerce 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.[160] 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 cybercrimes or any activities going against national interest.

[159] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 (Dec. 24, 2018), *available at* https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

[160] Mint, *SC flags tech pitfalls, asks Centre to curb social media misuse* (Sept, 25, 2019), *available at* https://www.livemint.com/news/india/sc-flags-tech-pitfalls-asks-centre-to-curb-social-media-misuse-1569350515906.html.

Infrastructure-Based Regulation Of Online Services

In March 2015, India's telecom regulator, Telecom Regulatory Authority of India (TRAI), issued a consultation paper on "Regulatory Framework for Over-the-Top services."[161] TRAI has recently recommended that there is no need to regulate OTT communication services. However, it is up to the government to accept or reject these recommendations. In 2016, there were additional consultation papers on issues including net neutrality,[162] VoIP, [163] and cloud service.[164] Many of these consultations have sought feedback on whether there is a need for regulation of OTT providers that offer such services. However, again, regulators have provided little feedback or response to industry submissions. TRAI's recent recommendations[165] proposing light touch regulation of cloud services is a worrying example of regulatory overreach. Finally, the Ministry of Telecommunications recently released draft registration guidelines for machine-to-machine (M2M) service providers in India, with a focus on increasing regulation of M2M service providers.[166]

Restrictions On U.S. Cloud Service Providers

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

In 2020, DPII extended its demand for minimum local content to the procurement of software and services. As per the Notification, the local requirement to categorize a supplier as a 'Class I' supplier is 50percent and a Class 2 Supplier is 20percent. The formula for calculation of Local Content has not been explicitly defined and has been left to the discretion of the different procurement agencies. This policy introduces market entry barriers that will impact specifically multi-national companies that have global R&D centers and therefore cannot assign the cost of development to one country; in addition, investments made in the ecosystem (such as the build of data centers or investments in startups) have also been ignored.

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.

---

[161] TRAI, *Consultation Paper on Regulatory Framework for Over-the-Top (OTT) Services* (Mar. 27, 2015).

[162] TRAI, *Consultation Paper on Net Neutrality* (May 30, 2016).

[163] TRAI, *Consultation Paper on Internet Telephony (VoIP)* (June 22, 2016).

[164] TRAI, *Consultation Paper on Cloud Computing* (Oct. 6, 2016).

[165] Telecom Regulatory Authority of India Releases Recommendations on "Cloud Services" ('Sept. 14, 2020), *available at* https://trai.gov.in/sites/default/files/PR_No.70of2020.pdf.

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

Disaster Recovery

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

Cloud Empanelment Guidelines

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

Customs Duties On Electronic Transmissions

India has been critical of the World Trade Organization's moratorium on customs duties on electronic transmissions and believes that ending the moratorium will enable the growth of domestic businesses.[167] Any imposition of new duties on electronic transmission would be inconsistent with India's WTO commitments and would significantly impact an exporter's ability to operate in India's increasingly growing digital economy. The USTR should take a strong position to push back on India's opposition to the moratorium, given its impending expiry at the 12th WTO Ministerial Conference in December 2021.

Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules

In February 2021, the government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which amongst other things require service providers to appoint local officers, have a local address, publish transparency reports and enable users to verify themselves. Separately, for "publishers," there is a requirement to adhere to a prescribed Code of Ethics, with incidental product changes to ensure rating and classification as per prescribed guidelines and implement access and parental control mechanisms and to implement a three-tiered grievance redressal mechanism.

The rules were imposed without final stakeholder engagement or notification, leaving U.S. industry exposed to substantial compliance burdens and liability exposure — jeopardizing not just the legal stability of the safe harbor but also the safety of personnel on the ground. The rules also have a potential chilling effect on human rights and future investment, and will lead to over-removal and censorship of legitimate content, including political speech.

New Geospatial Data Guidelines

New guidelines relating to geospatial data and associated services were introduced in February 2021. While the guidelines were ostensibly aimed at opening up India's mapping policy and improving the ease of doing business through deregulation, they also contain elements that are discriminatory to foreign service providers. For instance, the guidelines provide preferential access to Indian companies to access geospatial data and develop geospatial

[167] Dep't for Promotion of Industry & Internal Trade, Draft National e-Commerce Policy, at 10 (2019) ("By making the moratorium permanent, and with more and more products now traded digitally in the era of additive manufacturing and digital printing, the GATT schedule of countries will erode and will vanish ultimately. Assuming that all nonagricultural products can be traded electronically, then everything will be traded at zero duty. So, the protection that is available to India, for the nascent industries in the digital arena will disappear at once, and that is an immensely important issue which concerns public policy makers in the developing world."), *available at* https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf [hereinafter "India National E-Commerce Strategy"].

services in India by prohibiting foreign entities from creating and owning geospatial data finer than a certain spatial accuracy threshold. While foreign entities can obtain a license for such maps or data through an Indian entity provided it is used only for the purpose of serving Indian users, subsequent reuse and resale of such maps/data is prohibited. There is also a data localization requirement for such data, which has to be stored and processed on a domestic cloud or on servers physically located in India.

Indonesia

WTO Information Technology Agreement Commitments

Indonesia continues to contravene its WTO binding tariff commitments by charging tariffs on a range of imported technology products that are covered by Indonesia's commitments under the Information Technology Agreement (ITA) and which should receive duty free treatment. Indonesia has only implemented ITA commitments that fall under 5 categories of goods/HS codes (Semiconductors, Semiconductors Equipment, Computers, Telecommunications Equipment and Software, and Electronic Consumer Goods). Further, Indonesian customs has also sought to re-classify technology goods that have similar functions into dutiable HS codes that are outside of the 5 categories as a means to raise revenue, but in most cases the reclassified HS codes are also themselves covered by Indonesia's ITA commitments. This practice widely affects the IT industry and negatively impacts U.S. investors and their workers.

Local Content Requirements: Hardware, Software, and Public Procurement

Indonesia's Ministry of Industry issued regulation No.22/2020 (IR22) on the Calculation of Local Content Requirements (LCR) for Electronics and Telematics, with a government target to achieve 35percent import substitution by 2025. IR22 provides specific and extensive requirements for manufacturing and development for both digital and non-digital physical products. The policy will have an additional administrative burden to physical ICT products that are needed for ICT companies to operate in Indonesia. There are also indications that the Indonesian government may also introduce an importation threshold for ICT equipment. The government has also signaled intention to build on this LCR requirement and add similar LCRs for software and applications, which would impact companies that provide services over the internet, including cloud services. The Government plans to introduce the importation threshold by the end of 2021. In addition to that, Indonesia intends to introduce LCR in government procurements, which will limit U.S. companies' ability to serve the Indonesian government.

Financial Services Data Localization

The Bank of Indonesia still requires core/important financial transactions to be processed domestically. That said, the Financial Services Authority (OJK) has incrementally allowed some electronic processing systems to be based offshore for banking services, insurance services, multi-financing services, and lending based technology. Despite some progress, the overall policy requires businesses to domestically process their financial transactions; this is mainly driven by the inability of regulators to trust multilateral law enforcement systems.

E-Commerce Regulation

Indonesia's Government Regulation No. 80/2019 (GR80) on E-Commerce draws a clear distinction between domestic and foreign e-commerce business actors, and prohibits personal data from being sent offshore unless otherwise approved by the Ministry of Trade through a list of countries which can store Indonesian e-commerce data.[168] This effectively requires e-commerce business actors to locally reside personal data for e-commerce customers. Trade Regulation 50/2020 (TR50) on E-Commerce, an implementing regulation of GR80, also requires e-commerce providers with more than 1,000 domestic transactions annually to appoint local representatives, promote domestic products on their platform, and share corporate statistical data with the government. Both GR80 and TR50 pose de facto data localization measures and local content requirements, which increase overhead costs for foreign entities and create undue market barriers.

[168] *Indonesia issues e-commerce trading regulation*, EY (Jan. 15, 2020), *available at* https://www.ey.com/en_gl/tax-alerts/ey-indonesia-issues-e-commerce-trading-regulation.

Customs on Electronic Transmission of Digital Goods

In 2018, Indonesia's Ministry of Finance (MOF) issued Regulation 17/2018 (Regulation 17), which amends Indonesia's Harmonized Tariff Schedule (HTS) Chapter 99 to add: "Software and other digital products transmitted electronically." This makes Indonesia the only country in the world that has added electronic transmissions to its HTS. Despite zero tariffs, companies have expressed concern over the potentially severe (and unnecessary) administrative burden of this new regulation, including potential customs documentation or reporting requirements, but MOF has indicated that any data reporting under this system will be voluntary. Imposition of any duties on digital products under this regulation would raise serious concerns regarding Indonesia's long-standing WTO commitment, renewed on a multilateral basis in December 2019, not to impose duties on electronic transmissions. In addition, using a tariff schedule for the application of such duties on non-physical products raises fundamental questions and challenges related to the harmonized tariff system, the role of customs authorities in the digital space, and the determination of country of origin for electronic transmissions. If implemented on a mandatory basis, these customs duties would be levied on the same electronically supplied services (ESS) that are subject to a VAT in Indonesia. Moreover, left unchecked, Indonesia's actions will set a dangerous precedent and may encourage other countries to violate the WTO moratorium. This is especially critical as members at the WTO continue discussions on e-commerce, and as the renewal for the moratorium comes up during the 12th WTO Ministerial Conference which will be held in December 2021. Indonesia must rescind Regulation 17 and remove Chapter 99 from its HTS.

Data Flow Restrictions And Service Blockages

While the government of Indonesia has introduced Government Regulation 71/2019 to revise the earlier GR 82/2012, forced data localization measures still remain. In the draft implementing regulations of GR 71/2019 (in the form of Communications & Informatics Ministerial Regulation on the Governance of Electronic Systems Providers for Private Scope), storing and processing of data offshore by any Electronic Systems Providers (ESPs) will require prior approval from the Minister. These measures reflect market access barriers, which require foreign services to undergo additional red tape when delivering products and services online.[169]

While Indonesia's GR71 provides greater visibility on its data localization policy[170] (i.e., only Public Scope Electronic System Providers are required to store and process data onshore), the ensuing implementing regulations (or the lack thereof) continue to be a significant barrier to digital trade, and is inhibiting foreign firms' participation in Indonesian e-commerce. Public Scope ESPs are defined to also include public administration which goes beyond national security and intelligence data. No further clarity has been made on the circumstances by which data can be stored and processed offshore in the case of Public Scope ESP including the guidelines that the Minister of Communications and Informatics will use when reviewing every individual data offshoring request by Private Scope ESPs. Indeed, U.S. firms have lost, and continue to lose, business in Indonesia from customers due to the ambiguity in the data localization requirements. GR71 was a step in the right direction towards reforming Indonesia's data localization policy and strengthening international trade, but the lower-level regulations are at risk of resurfacing significant market access barriers because of the incongruent approach with GR71 as the umbrella regulation. Further, data localization policy remains in place for banking and financial sectors despite the possibility of Private Scope ESPs to store and process data offshore based on GR71. Additionally, GR71 has mandated the advent of an interagency committee to set up and oversee the exception for Public Scope ESPs to store and process data offshore. However, the industry is concerned that there is limited progress in the finalization of the implementing regulations of GR71, creating tremendous business uncertainty and increased compliance risks. IA urges USTR to strongly encourage Indonesia to move swiftly in finalizing the implementing regulations of GR71 and for these regulations to prohibit data localization.

---

[169] Herbert Smith Freehills LLP, *Draft regulation may require all local and foreign websites and apps to register with MOCI, available at* https://www.lexology.com/library/detail.aspx?g=9ae4aa21-dcb0-4c26-8e68-840f483873f6.

[170] Baker Mckenzie, *Indonesia: New Regulation on Electronic System and Transactions* (Oct. 28, 2019), *available at* https://www.bakermckenzie.com/en/insight/publications/2019/10/new-regulation-electronic-system-and-transactions.

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

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

Discriminatory Or Opaque Application Of Competition Regulations

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

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

Indonesia's GR71/2019 and its ensuing implementing regulations by the Minister of Communications and Informatics will be the primary regulations for digital platforms. However, the government seems to have indicated further regulations on OTT as it relates to broadcasting services. The plan is gaining momentum amidst the judicial review of the Broadcasting Law and a subsequent plan to revise the Law with an outlook of subjecting OTT platforms under a new regulation. The regulation will ostensibly seek to create an equal playing field between OTT platforms and traditional platforms (e.g. broadcasting, telecommunications, media), but will likely impose additional requirements on foreign providers such as the need for foreign providers to submit to screening of content and provide law enforcement access as a condition for operating in the Indonesian market.

Excessive Government Access On Cybersecurity

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

Duties On Electronic Transmissions

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

HTS skirts Indonesia's commitment under the WTO Moratorium on Customs Duties on Electronic Transmissions, a commitment that Indonesia reaffirmed as recently as December 2019.

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

Unilateral Or Discriminatory Digital Tax Measures

Under Law 2/2020, Indonesia introduced a series of changes to its tax code, including an expansion of the definition of permanent establishment for purposes of Indonesia's corporate income tax and a new "electronic transaction tax" (ETT) that targets cross-border transactions where tax treaties prohibit Indonesia from taxing corporate income from the transaction. Notably, in March 2020, Indonesia introduced tax measures targeting digital services as part of an emergency economic response package. One of these taxes applies to e-commerce transactions carried out by foreign individuals or digital companies with a significant economic presence. Per reports, the significant economic presence will be determined through the companies' gross circulated product, sales and/or active users in Indonesia.[171] Companies determined to have a significant economic presence will be declared permanent establishments and as a result subject to domestic tax regulations.[172] If this determination of permanent establishment conflicts with an existing treaty, such as the U.S.-Indonesia tax treaty, then a new ETT would apply to income sourced from Indonesia.[173] The implementation details have yet to be further outlined in a government regulation, and Indonesian officials have said that they would be aligning their policies with the OECD consensus. In October 2021, the Indonesian parliament approved a major tax overhaul bill without further provisions on the ETT, a sign that the Indonesian government is moving towards committing to the global consensus. Nevertheless, given that the ETT has been passed into law and can be revived at any point with the issuance of an implementing declaration, USTR should continue to closely monitor developments on this front.

Regulations On Subsea Cable Corridors

The Minister of Fisheries and Marine Affairs issued a Decree 14/2021 mandating that all subsea cables in Indonesian waters need to follow 14 prescribed routes and to have 4 pre-determined main landing points in Manado, Kupang, Papua and Batam. This is despite the fact that more than half of existing cables are located out of these prescribed corridors, and there is limited business case to follow such routes and landing points. This restricts the ability of U.S. cloud and infrastructure services providers to determine the best business case for such landings and tilts the playing field in favor of domestic players.

Further, as part of the new GR 5/2021 on business licensing, subsea cable permits require a series of licenses from several Ministries such as Environment, ICT, Transport, and Investment. The requirement from the ICT Ministry specifically asks for (1) foreign operators to partner with a local network operator, (2) the local partner to be part of the consortium, (3) a minimum of 5percent stake by the local partner, and (4) obligation to land in Indonesia. Such local rent-seeking requirements are significant market barriers for US providers to establish their business operations in Indonesia.

---

[171] *Indonesia Taxes Tech Companies Through New Regulation*, The Jakarta Post (Apr. 1, 2020), *available at* https://www.thejakartapost.com/news/2020/04/01/indonesia-taxes-tech-companies-through-new-regulation.html.

[172] *Id.*

[173] *Indonesia Government Proposes Key Tax Changes*, EY (Mar. 19, 2020), *available at* https://taxnews.ey.com/news/2020-0604-indonesian-government-proposes-key-tax-changes.

Regulation On Private Electronic Systems Providers

In December 2020, the ICT Ministry issued Ministerial Regulation 5/2020 on private electronic systems providers (ESP), effective immediately. Foreign and local ESPs were required to register with the government and appoint a local point of contact to share access to data and systems to the government for supervisory and law enforcement purposes upon request. ESPs are required to comply with very strict 24 hours turnaround time for regular content removal requests and 4 hours for urgent removal requests. ESPs are also expected to provide the Indonesian government with access to data and systems for "supervisory and law enforcement purposes" within 5 calendar days upon request. Failure to meet these requirements could result in fines and/or product blockage. The broad and vague definitions mean that in theory many US services suppliers would be entirely in scope. The lack of clear definitions also could be potentially abused, since a court order is not required for data access requests by the government.

Restrictions On Cloud Services

According to a recent regulatory review by the Asia Cloud Computing Association (ACCA), Indonesia's regulatory framework is the least conducive for the adoption of public cloud technology in the financial services industry. The biggest gaps are in the areas of data localization, the requirement to seek prior regulatory approval, and the lack of differentiation in the materiality of workloads.

First, Indonesia's financial institutions are still blocked from using offshore data centers. Bank Indonesia – the country's central bank – still requires payment transactions to be processed domestically. The Financial Services Authority (OJK) has incrementally allowed some electronic systems to be processed offshore in the banking and insurance sector, but this has not been permitted in sectors including multi-financing and lending based technology. Industry reports these rules are motivated in part by regulators' lack of trust in multilateral law enforcement systems.

Second, the OJK requires financial institutions to seek its approval 2 to 3 months before moving workloads to the public cloud. For instance, Regulation No. 38/POJK.03/2016 requires commercial banks planning to operate an electronic system outside Indonesia to seek approval from the OJK 3 months before the arrangement starts. In addition, financial institutions that plan to outsource the operation of their data centers or disaster recovery centers must notify the OJK at least 2 months before the arrangement starts.

Third, Regulation No. 9/POJK.03/2016 only allows commercial banks to outsource "support work" (i.e., activities that are low risk, do not require high banking competency and skills qualification, and do not directly relate to operational decision-making). These workloads that can be outsourced are all subject to the same regulatory requirements, with no differentiation in terms of materiality, unlike in other jurisdictions, such as Australia and Singapore.

Jamaica

Divergence From Privacy Best Practices

IA encourages USTR to monitor developments on a data protection act modeled on the GDPR.

Japan

Deductive Value Definition For Inventory Transfer By Non-Resident Importers At Importation

In Japan, unlike EU import custom procedures, when importers declare their import customs by deduction method, on which the declaration value is calculated by deducting domestic costs from Japan's domestic price, it is unclear whether marketing expenses paid by non-resident importers are deductible. The Uniform Customs Code in the EU states that, when using the deduction method on imports into the EU, direct and indirect costs of

marketing must be deducted from the unit price when they are made in connection with sales in the EU. The unclearness causes complicated declaration procedures and unnecessary burden on importers.

Infrastructure-Based Regulation Of Online Services

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

If 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.

Furthermore, MIC is going to revise the Guidelines for Protection of Personal Information in Telecommunications Business following the amendment of TBA. During the course of the discussion, the so-called "communication related privacy" right was proposed. IA is also concerned that the definition of the proposed right is too vague to understand, and this unique concept could make it difficult, leading to conflict of compliance with the Personal Information Protection Act which protects privacy rights of the general public.

Sharing Economy Barriers

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

- → *License cap:* Japanese law has capped the number of taxi and other hire licenses. Only in some jurisdictions may taxi and for-hire vehicle companies petition for additional licenses to be issued, although in practice such petitions are rarely ever successful.

- → *Minimum trip duration.* While the number of city hire licenses is not capped, city hire cars must be booked for a minimum of two hours.

- → *Price controls*: Regulations set a minimum price floor and a maximum price ceiling for both taxis and hire cars.

- → *"Return-to-garage" rule:* Hire car drivers must return to their registered place of business after completing every trip.

- → *Barriers to independent taxi operators*: In order to receive a license to work as an independent taxi driver—as opposed to an affiliate of a larger taxi firm—a driver must first have 10 years of experience driving for the same taxi firm and be at least 35 years old.

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

Copyright-Related Barriers

Despite limited exceptions for search engines[174] and some data mining activities,[175] Japanese law today does not clearly provide for the full range of limitations and exceptions necessary for the digital environment[176] – which creates significant liability risks and market access barriers for U.S. and other foreign services engaged in caching, machine learning, and other transformative uses of content.

Divergence From Privacy Best Practices

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

Infrastructure-Based Regulation Of Online Services

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

The law is planned to be enforced by April 2021.

IA is concerned that the regulation on digital platforms may tilt the level playing field of competition as it currently designates regulated businesses only based on the size of sales in business and does not pay attention to the characteristics of platform business or the multi-sided nature of the business and dynamically evolving competitive landscape ignoring new businesses enter the market constantly.

Market-Based Platform Regulation

The Japanese Consumer Affairs Agency (CAA) established a new online consumer protection law, "Act on the Protection of the Interests of Consumers Using Transaction Digital Platforms," in May 2021. The aim of this law is to mandate platforms to perform certain obligations to facilitate resolution of disputes between merchants and consumers. As a key impact, digital platforms will be obligated to disclose information about merchants if requested by consumers. The draft of the Cabinet Office ordinance is currently being discussed.

The Headquarters for Digital Market Competition (DMCH) in Japan published its final report on "Competition in the Digital Advertising Market" in June 2021. This report concluded that the P2B Act should be applied to digital advertising and organic search (e.g., as quality, conflict of interest, complaints handling, search algorithm change). The applicability of P2B to organic search is also being considered by the Cabinet Legislation Bureau. There are concerns on whether a wholesale application of the P2B Act to organic search is feasible given the unique nature of the product and potential algorithmic change disclosures.

[174] Copyright Law of Japan, Section 5 Art. 47-6 (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"), *available at* http://www.cric.or.jp/english/clj/cl2.html.

[175] Copyright Law of Japan, Section 5 Art. 47-7 (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), *available at* http://www.cric.or.jp/english/clj/cl2.html.

[176] 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.

Revisions To The Copyright Act

In 2020, revisions to the Copyright Act were introduced to crack down on leech websites and expand the scope of illegal downloading. This is in response to the damage to the Japanese manga (comic book) and entertainment industries by pirate sites which typically operate on servers located in jurisdictions lacking sufficient copyright protection. Although the 2020 amendment makes it illegal to download anything other than music or videos, downloads that cause only minor damage to the copyright owner (e.g., screenshots), are exempted. The revisions to expand the definition of illegal downloading will take effect on January 1st, 2021.

Jordan

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

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

Kenya

Burdensome Or Discriminatory Data Protection Regimes

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

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

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

The law also provides for extra-territorial application of its provisions to data processors and controllers "not established or ordinarily resident in Kenya, but processing the personal data of subjects located in Kenya." This

provision does not include a description of what actions bring a foreign business within its scope, including, for example, targeting the data subjects in the country.

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

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

Copyright-Related Barriers

The East African Legislative Assembly passed the East African Community Electronic Transactions Act in 2015. While the Act provides for some level of protection of intermediaries from liability for third-party content, it fails to include any "counter-notice" procedures for a third party to challenge content takedown requests, and it removes legal protections if the intermediary receives a financial benefit from the infringing activity. Lack of a counter-notice provision exposes internet intermediaries to business process disruptions through frivolous takedown notices.
Even more problematic, vague language about "financial benefits" can remove an entire class of commercially-focused intermediaries from the scope of liability protections, and can result in a general obligation on these intermediaries to monitor internet traffic, disadvantaging commercial services from entering numerous East African markets, including Kenya, Uganda, Tanzania, Burundi, Rwanda, and South Sudan.

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

Infrastructure-Based Regulation Of Online Services

The ICT regulator plans to conduct a study on how to treat "over-the-top technologies and services (OTTs)."[177] IA encourages USTR to monitor the development of this plan and to promote a light-touch framework for regulating information services that is consistent with the U.S. approach.

Unilateral Or Discriminatory Digital Tax Measures

In April 2020, a rushed COVID-19 tax relief law was passed with a clause for 20 percent withholding tax charged on 'marketing, sales promotion and advertising services' provided by non-resident persons. This was followed by a 1.5 percent digital services tax law for both resident and non-resident entities in July 2020, which is scheduled to come into effect in January 2021. At the same time, the Ministry of Finance is preparing regulations on VAT (14 percent) on "digital marketplace services" for both non-resident and resident providers. Kenya's unilateral corporate tax proposals create concerns not only around targeting and discriminating against ICT services, but also around the legitimacy of an international tax system that has been built around multilateral coordination.

[177] 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.

Non-IP Intermediary Liability Restrictions

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

Local Equity Ownership In ICT Firms And Data Localization

In 2020, the Kenyan government introduced an ICT Policy which included a clause on "equity participation",[178] stipulating that by 2023, only firms with 30 percent local ownership would be licensed to provide ICT services. The Policy also stipulated data localization mandates for "Kenyan data (to) remain in Kenya". Subsequently, the 2020 Data Protection Law gave the ICT Minister the power to mandate data localization. In 2021, the new Office of the Data Commissioner issued draft regulations proposing that data processed for the purpose of "actualising a public good" shall be processed in a server and data center based in Kenya. This would include (but not be limited to) data related to civic registration and national identification systems; primary and secondary education; elections; health; electronic payments and public revenue administration. Such data localization mandates are a barrier to cross-border digital trade, and the forced local equity ownership requirement limits market access opportunities for US companies operating in Kenya.

Digital Taxation

In 2020, three tax laws were implemented. First, a 20percent withholding tax on "marketing, sales promotion and advertising services" provided by non-resident persons. Second, 1.5percent digital service tax on income from services derived from or accruing in Kenya through a digital marketplace. Third, changing the VAT liability of exported services from zero-rated to exempt, so that the services provided by the local entity to overseas entities would no longer be classified as services for export and the local entity would no longer claim VAT refunds on its costs for those services.

Korea

Burdensome Or Discriminatory Data Protection Regimes

Several South Korean regulators have threatened a number of U.S. tech firms with investigations and fines for not complying with prescriptive South Korean privacy law, even though these firms do not maintain data controllers on South Korean territory. As a result, services have been forced to modify the way they do business in South Korea. There is a broader, worrying trend of South Korean regulators requiring local presence as a condition to operate in the cross-border services space, which may be inconsistent with Korea's commitments in the Free Trade Agreement.

Copyright-Related Barriers

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

Data Flow Restrictions And Service Blockages

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

[178] *See Publication of the National Formation Communication and Technology Policy Guidelines, 2020*, Bowmans Law (Sept. 1, 2020), https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/publication-of-the-national-information-communication-and-technology-policy-guidelines-2020/.

Separately, there is pending legislation that may be interpreted to require online service providers to establish local servers in order to ensure user protection from deliberate diversion of traffic and slowed service. Penalties for not complying with this requirement would include up to a three percent fine based on revenue.

Discriminatory Or Opaque Application Of Competition Regulations

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

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

Overly Restrictive Regulation Of Online Services

Congress members have proposed an OTT bill to regulate online video platforms, targeting overseas service providers. In addition, on March 8, 2019, the Korea Communications Commission announced its key plans for 2019 which included drawing up "Network Use Guidelines" which would "require overseas operators to 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.

The Ministry of Science & ICT announced the regulations made pursuant to amendments to the Telecommunications Business Act passed in May 2020, and the regulations came into effect on December 10, 2020.[179] There are concerns that the new rules impose impractical obligations on foreign services, and certain provisions may conflict with Korea's trade commitments to the United States. The rules subject predominantly U.S. Internet services to disproportionate levels of risk and responsibility regarding network quality management outside their practical control. The rules inappropriately shift the burden for several responsibilities pertaining to network management to "value-added telecommunications service providers" (VTSPs), even though they lack the technical or information capabilities to control end-to-end delivery of the content in South Korea. Internet service providers (ISPs) who control the network infrastructure and management should remain the most adept to primarily control service reliability. These changes could also lead to unbalanced bargaining positions resulting in discriminatory or anti-competitive behavior by ISPs to the detriment of VTSPs, which could lead to demands for increased usage fees or other contractual conditions.

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

[179] Kim Eun-jin, *New Law Holds Netflix, Google and Facebook Responsible for Net Quality*, BusinessKorea (December 2, 2020), http://www.businesskorea.co.kr/news/articleView.html?idxno=56099.

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.

Restrictions To Cloud Services

The Korean government continues to maintain a protectionist stance to keep global cloud service providers out of the local public sector market through the Korea Internet & Security Agency (KISA) Cloud Security Assurance Program (CSAP). Industry reports that the four main technical requirements that have prevented all global CSPs from being able to obtain the CSAP: (1) physical separation; (2) Common Criteria (CC) certification; (3) vulnerability testing; and (4) use of domestic encryption algorithms.

Through these onerous requirements that depart from international standards, the CSAP effectively casts technical blockers to trade and prohibits global CSPs from accessing public sector workloads in Korea. The government requires CSAP-like controls in other sectors, such as in healthcare, with the Ministry of Health and Welfare (MOHW)'s inclusion of the CSAP-like controls as a requirement for Electronic Medical Record (EMR) system providers who seek to use public cloud services. While MOHW claims that the controls are not mandatory, it plans to provide medical insurance reimbursement premiums only to medical institutions with certified EMR systems, thus creating an unlevel playing field for companies who are unable to obtain the CSAP.

Location-Based Data Restrictions

Korea's restrictions on the export of location-based data have led to a competitive disadvantage for international suppliers seeking to incorporate such data into services offered from outside of Korea. For example, foreign-based suppliers of interactive services incorporating location-based functions, such as traffic updates and navigation directions, cannot fully compete against their Korean rivals because locally-based competitors typically are not dependent on foreign data processing centers and do not need to export location-based data. Korea is the only significant market in the world that maintains such restrictions on the export of location-based data. While there is no general legal prohibition on exporting location-based data, exporting such data requires a license. To date, Korea has never approved a license to export cartographic or other location-based data, despite numerous applications by foreign suppliers. U.S. stakeholders have reported that Korean officials, citing security concerns, are linking such approval to a separate issue: a requirement to blur certain integrated satellite imagery of Korea, which is readily viewable on other global mapping sites based outside of Korea. Korean officials have expressed an interest in limiting the global availability of high-resolution commercial satellite imagery of Korea, but have no ready means of enforcing such a policy since most imagery is produced and distributed from outside of Korea. It is unclear how limiting such availability through specific services (e.g., online mapping) of a particular supplier addresses the general concern, since high-resolution imagery, including for Korea, is widely available as a stand-alone commercial product (and is often available free of charge), and offered by over a dozen different suppliers.

Government-Imposed Content Restrictions and Related Access Barriers

Rules announced in 2019 by the Korean Communications Commission will enable officials to filter online content and block websites based outside the country.[180] While in the pursuit of enforcing existing laws regarding illegal content, some have raised concern that it follows authoritarian models of Internet regulation.[181]

---

[180] Press Release, Korean Communications Commission, 방통위, 불법정보를 유통하는 해외 인터넷사이트 차단 강화로 피해구제 확대 ["KCC Expands Relief Measures by Strengthening Blocking of Overseas Internet Sites that Distribute Illegal Information"] (February 12, 2019), *available at* https://kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=1&boardSeq=46820.

[181] *Analysis: South Korea's New Tool for Filtering Illegal Internet Content*, New America (Mar. 15, 2019),

Amendments To The Telecommunication Business Act

In August 2021, the Korean National Assembly passed legislation that requires mobile application marketplaces to permit users to make in-application purchases through payment platforms not controlled by the marketplace itself. This legislation is a global-first move that affected only two U.S. digital companies and none of their Korean competitors. It threatens a U.S. business model that has allowed successful Korean content developers to reach global audiences, and is at tension with Korea's obligations under the Korea-U.S. FTA. In the absence of a payment service integrated into a mobile application marketplace, it is unclear how the application distributor could recover the costs it incurs in maintaining the mobile application marketplace, and monetize the broad benefits accorded to all application developers, including those from Korea.

Malaysia

Cabotage Policy On Submarine Cable Repairs

In 2019, the Ministry of Transport issued an exemption to the Merchant Shipping Ordinance 1952 that would allow non-Malaysian ships to conduct submarine cable repairs in Malaysian waters. The exemption was key in reducing the time required to conduct submarine cable repairs. Submarine cables are the global backbone of the internet, carrying around 99 percent of the world's internet, voice and data traffic, including the backhaul of mobile network traffic and data for digital trade. In November 2020, the new Minister of Transport suddenly announced the revocation of the exemption as a means to protect the domestic shipping industry from foreign competition. Industry groups have repeatedly raised concerns with the arbitrary and discriminatory nature of the revocation and call on the Malaysian government to restore its earlier exemption.

Restrictions To Cloud services

In October 2021, the Minister of Communications and Multimedia announced that the Malaysian Communications and Multimedia Commission (MCMC) would subject data centers and cloud service providers to licensing obligations under the Communications and Multimedia Act 1998 (CMA 1998) starting January 2022. If applied to cloud service providers, the new requirements could compel such entities to: incorporate locally in Malaysia; appoint local shareholders, including a fixed percentage of shareholders from the Bumiputera ethnic group; comply with the provisions of the Communications and Multimedia Act 1998, including requirements on content removal; allow interception of communications subject to the discretion of the Communications and Multimedia Minister; and make mandatory payments (potentially a portion of revenue) to the Universal Service Fund, which is typically used to improve internet connectivity in underserved areas. Such licensing requirements are tailored towards telecommunications and internet service providers, and as a matter of international best practice, they are not normally applied to other sectors of the economy.

Mexico

Transportation Consignment Note

In the approved 2021 Budget, a line was included that allowed the Secretariat of Communications & Transportation (SCT) and the Tax Administration Service (SAT) to increase reporting requirements. To implement these new reporting requirements, the SCT and SAT published regulations that require a carta porte (transportation consignment note), which is an addendum to the invoices that documents the origin, destination, and the goods transported inside of the country.

---

https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/analysis-south-koreas-sni-monitoring/; *Is South Korea Sliding Toward Digital Dictatorship?*, Forbes, (Feb. 25, 2019), *available at* https://www.forbes.com/sites/davidvolodzko/2019/02/25/is-south-korea-sliding-toward-digital-dictatorship/.

As of September 30, this carta porte will require the incorporation of new and mandatory catalogues and information related to the goods, locations of origin, intermediate points and destinations, and will also refer to the means by which they are transported (either road, rail, air, sea, river or multimodal).

These measures will increase the complexity of the business environment and the conduct of business and trade in Mexico and North America. Under the United States-Mexico-Canada Trade Agreement (USCMA), the inclusion of a supplementary Bill of Lading contradicts the spirit of the agreement and some specific provisions established in the Customs Administration, Trade Facilitation, and Cross Border Trade in Services chapters.

Local Content Requirements

In September of 2020, Senator Ricardo Monreal presented a legislative project that seeks to reform the Federal Telecommunications Act and require a 30percent local content quota for Over-the-Top (OTT) platforms operating in Mexico. A local content quota for OTT platforms would violate Mexico's commitments under USMCA (Articles 14.10 and 19.4.1), as well as limit free expression and consumer choice, distort the growing audiovisual market, and stifle investment and competitiveness. The Senator subsequently presented a revised bill in February of 2021 that seeks to establish a 15percent local content quota. If this policy was enacted and services failed to launch, Mexican audiences and creators would have fewer legitimate options for film and television content.

The bill would also expand the Federal Telecommunications Institute (IFT) licensing requirement for restricted TV and audio services to cover OTT services — even those operating from abroad. Imposing such onerous new licensing requirements on OTT services would be inconsistent with USMCA Articles 14.2, 14.4, 14.10, 15.3, 15.7 and 19.4.

In addition, the Mexican government has shared a draft proposal of their own for the audiovisual industry. The proposal puts forward a number of concerning ideas, including: requiring digital streaming platforms to use Mexican content classification (art. 26), creating a reinvestment requirement whereby operators of digital streaming platforms that provide their services in Mexico must allocate each year the amount equivalent to 5percent of the profits that they report annually to the Ministry of Finance and Public Credit as a donation to the promotion of national cinema through the Mexican Institute of Cinematography (art. 26), and requires a visible section with audiovisual content of national origin (art. 26).

A bill proposed by Senator Ricardo Monreal establishes amendments to the Cinematography Law that similarly set a 15percent-10percent national content quota requirement for OTT services.

These policies, if enacted, would plainly violate Mexico's USMCA obligations.

Tariffs On Express Shipments

The U.S.-Mexico-Canada Agreement (USMCA) entered into force on July 1, 2020, and included positive outcomes for U.S. Companies in the Customs Chapter, including streamlined, simplified, and expedited border processing to help speed border clearance times and lower costs for low-value shipments. This included commitments by Mexico to implement new *de minimis* and informal clearance thresholds.

On May 27, 2021, Mexico's Tax Administration Service (SAT) published revised General Foreign Trade Rules that raised the informal clearance threshold to $2,500. The increase to $2,500 went into effect on June 26 for shipments valued at >$117. However, the Secretary of Economy still needs to harmonize its own regulations to allow for this change to be fully implemented which has not happened to date. Specifically, the Secretary of Economy needs to update Section IX, Article 10 of the Annex 2.4.1, which still requires compliance with all applicable Official Mexican Standards (*Norma Oficial Mexicana*, or "NOM'") for those courier shipments with a value of $1,000 or more. Mexico should fully implement its commitments under USMCA's Customs Chapter, including eliminating the new import rates and implementing an informal clearance threshold for shipments up to USD $2,500."

In addition, Mexico has also published new regulations that increased import rates on shipments from the U.S. and Canada valued between US$50-117 by 1percent (from 16 percent to 17 percent). For non-USMCA shipments, the import rate was also increased by 3 percent (from 16 percent-19 percent) for shipments between US$50-1,000. These changes were made without warning or following appropriate protocols, and they became effective immediately. While this is a small increase, we view it as a violation of the USMCA and a sign that the current Mexican Administration does not intend to implement its customs commitments, and may in fact, take additional steps that will disadvantage U.S. exporters.

Restrictions On Cloud Services

Industry is tracking financial sector regulations. Mexican financial sector regulators - National Banking and Securities Commission (CNBV) and the Central Bank of Mexico (Banco de Mexico) - have issued Draft Provisions Applicable to Electronic Payment Fund Institutions (IFPEs). The particular articles of concern in the draft regulation (PROVISIONS APPLICABLE TO ELECTRONIC PAYMENTS INSTITUTIONS, REFERRED TO IN ARTICLES 48, SECOND PARAGRAPH; 54, FIRST PARAGRAPH; AND 56, FIRST AND SECOND PARAGRAPHS OF THE LAW TO REGULATE FINANCIAL TECHNOLOGY INSTITUTIONS) are Articles 50 and 49. Article 50 would impose the obligation of data residency and multi-scheme providers to E-Payment Institutions (IFPEs) that use cloud computing services.

Article 49 would establish an authorization model with a high degree of discretion and lack of transparency for the use of cloud computing services. These draft requirements to localize data run counter to the spirit, if not the letter, of USMCA's landmark digital and financial services provisions. These draft regulations undermine U.S. financial services providers, which already face lengthy and uncertain approval processes from CNBV or Banco de Mexico in order to use secure U.S.-based cloud computing services. Additionally, the regulation could negatively affect the adoption of cloud computing in the country and create an uneven playing-field, where US cloud computing companies would be at a disadvantage with respect to local data center companies.

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

Separately, on January 28, 2021, Mexico issued a final regulation on electronic payment fund institutions, which includes certain requirements relating to use of cloud service suppliers by electronic payment fund institutions. This regulation, which entered into force in April, requires electronic payment fund institutions to maintain a business continuity plan in the case of disaster recovery that relies on either 1) a multi-cloud approach with at least two cloud service providers from two different jurisdictions, or 2) an on-premise data center in country that doesn't depend on the primary (foreign) cloud provider. The approvals process run by the National Banking and Securities Commission (CNBV) that is required for financial services companies to use cloud services is resource intensive and is discriminatory towards foreign cloud providers, whereas existing local on-premise data centers merely need to complete a shorter, simpler notification process which takes months, as opposed to years. This de facto data localization requirement is in addition to an already complex and time-consuming process that electronic payment fund institutions face in order to gain regulatory approval to use offshore cloud infrastructure, whereas in-country infrastructure enjoys an expedited process.

On another note, the ICT Cloud Policy was published in September, including very concerning provisions regarding data localization that could drive federal government cloud procurement to favor cloud providers with data centers in Mexico; and the recommendation to federal institutions to celebrate procurement contracts derived from Framework Agreements already in place, which could work in discrimination of some providers without agreement. It could potentially violate USMCA Articles 13.4, Section 1 on National Treatment and Non-discrimination, and 13.11 on Technical Specifications, regarding Government Procurement; Article 22.4 Non-discriminatory treatment and Commercial Considerations, and Article 19.2 on Location of Computing Facilities (this last provision in the case of state-owned enterprises that act in a commercial capacity).

NOMs For Safety, EMC, Telecommunications And RF

NOMs for Safety, Electromagnetic Compatibility, Telecommunications, and Radio Frequency are both duplicative of, and divergent from global regulations. Relevant NOMs include NOM-001, NOM-003, NOM-016, and NOM-019. Each of these NOMs requires product testing. While some of these NOMs have equivalency agreements recognizing test reports for equivalent standards in the U.S. and Canada, some NOMs will require testing to the NOM standard itself, or lack an equivalency agreement altogether. This results in the need for redundant testing to NOM standards, increasing the cost and barriers for importing ICT goods into Mexico. For example, equipment that has yet to demonstrate compliance with NOM-001 will need to be tested to the latest version of this standard unless and until an equivalency agreement is reached and reciprocity clause is accepted between the U.S., Canadian, and Mexican governments. Where an existing CB report can be used, NOM certification will generally take 4-5 weeks after an application has been processed and samples have been received at a certification lab.

Filtering, Censorship, And Service-Blocking

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

The United States has raised concerns with the Mexican government that the requirements relating to use of cloud service suppliers by electronic payment fund institutions have a negative competitive impact on the business of U.S. service suppliers.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- → *License cap*: Certain states (e.g., Colima, Querétaro, and Guanajuato) limit the number of vehicles that can work with app-based transportation services.
- → *Cash payment prohibition:* Drivers working with app-based transportation services are prohibited from accepting cash payments in several states (Mexico City, Puebla, Querétaro, Yucatán, Sonora, San Luis Potosí, Coahuila, Colima, Aguascalientes, and Tijuana-Baja California).
- → *Vehicle requirements:* Depending on the state, vehicles providing app-based transportation services must not be more than 4-7 years old.
- → *Vehicle identification:* Some cities and states require vehicles providing app-based transportation services to have visible external identification, increasing the risk of physical violence and intimidation by the incumbent taxi industry.

→ *Data-sharing requirements:* Companies providing transportation apps are increasingly receiving requests for data sharing and some of them, as in Mexico City, require them to share specific trip data beyond any reasonable safety or public policy purpose, compromising privacy and even the security of users. The amount of information required poses a disproportionate cost and raises competitive concerns, given that city authorities currently operate an app-based system for hailing government concession taxi services.

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

→ Increase of costs of spectrum usage: The same Fiscal Bill 2021 includes a proposal to increase the costs to invest in spectrum in Mexico, that could substantially increase the costs of internet access to end-users.

→ Net Neutrality: Telco Regulator could issue pending regulations. These regulations could shift Internet consumption, as the draft proposal does not consider clear wording on how carriers promote their commercial offer, which could consolidate discriminatory practices against similar services on zero-rating and bundled services. The draft is also considering wording to increase the Telco Regulator capabilities to order ISPs to block traffic, which violates USMCA provision to promote free data flows while hindering freedom of speech.

Digital Taxation

On September 8, 2020, the Secretary of Finance & Public Credit, Arturo Herrera, presented to the Mexican Congress the legislative project for the Government's Budget for 2021. Included in the proposal was the implementation of a "kill switch," an enforcement mechanism that the Mexican government initially proposed in their 2020 Budget against non-resident entities that do not comply with the application of the VAT, and Income Tax retentions on non-resident supplies of digital services to Mexican consumers.

Industry raised concerns with a previous attempt to implement this in 2019,[182] and the kill switch was removed in the previous Budget. However the fact that a limited number of companies registered in the government's regime (35 companies in Mexico, by mid-2020 compared to more than 100 in Chile in the same timeframe, due to Mexico's incredibly complex registration process) led them to reintroduce the measure as a way to force compliance, being approved by Congress in November 2020 and entering into force on January 1st, 2021.[183] The regulation empowers the tax authority to work with the telecom regulator to non-resident Internet platforms, removing them from accessibility to Mexican users. So far, the provision hasn't been used as the vast majority of US Internet companies have already been registered and have been complying with fiscal obligations. Nevertheless, the implementation of this blocking could fragment the Mexican Internet and lead to technical problems that will likely impact third parties. Likewise, there is a high probability that this provision could violate USMCA articles. Articles 15.3 of National Treatment for Services and Service Suppliers; Article 15.6: Local Presence; Article 18.3: Access to and Use of Public Telecommunications Networks or Services; Article 19.10(a): Principles on Access to and Use of the Internet for Digital Trade; and most importantly Articles 17.17 and 19.11 regarding Free flow of data across borders.

Copyright Liability Regimes For Online Intermediaries

Mexico made amendments to its Federal Copyright Law in 2020[184] in attempts to bring its law in compliance with commitments under USMCA. There are concerns that the text of the provisions implementing Articles 20.88 and 20.89 of the USMCA inappropriately narrow the application of this framework for Internet services. Likewise, the

[182] Industry Letter (Oct. 14, 2019), *available at* https://www.ccianet.org/wp-content/uploads/2019/10/Multi-Association-Letter-on-Mexican-Tax-Issue.pdf.

[183] Income Tax Law, *available at* http://www.diputados.gob.mx/LeyesBiblio/pdf/LISR_310721.pdf; VAT Law, *available at* http://www.diputados.gob.mx/LeyesBiblio/pdf/77_310721.pdf, Tax Code, *available at* http://www.diputados.gob.mx/LeyesBiblio/pdf/8_310721.pdf.

[184] Federal Copyright Law (Spanish), *available at* http://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf.

provision implemented through the amendment of in Article 232 Quinquies fr. II of the Copyright Law establishes administrative offenses and a fine, when ISPs: do not remove, take down, eliminate or disable access to content upon obtaining a notice from the right holder; or do not provide to a judicial or administrative authority information that identifies the alleged offender. This provisions contravenes Article 20.89.(9) of the USMCA, and other provisions of the Bill, since the impossibility of applying the measures provided in the treaty do not per se originate a responsibility for ISPs.

Currently, the Supreme Court is analyzing an unconstitutionality action presented by the National Human Rights Commission against these amendments, arguing that in some aspects it breaches USMCA and freedom of expression.

New Zealand

Copyright-Related Barriers

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

New Zealand relies on a static list of purpose-based exceptions to copyright. In practice, this means that digital technologies that use copyright in ways that do not fall within the technical confines of one of the existing exceptions (such as new data mining research technologies, machine learning, or innovative cloud-based technologies) are automatically ruled out, no matter how strong the public interest in enabling that new use may be. For example, there is a fair dealing exception for news in New Zealand, but it is more restrictive than comparable exceptions in Australia and elsewhere, and does not apply to photographs – which limits its broader applicability in the digital environment.
As a result, New Zealand's approach to devising purpose-based exceptions is no longer fit for purpose in a digital environment. This approach creates a market access barrier for foreign services insofar as it is unable to accommodate fair uses of content by internet services and technology companies that do not fall within the technical confines of existing exceptions. To eliminate this barrier and comply with the U.S. standard and prevailing international norms, New Zealand should adopt a flexible fair-use exception modeled on the multi-factor balancing tests found in countries such as Singapore and the U.S.

Intermediary Liability

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

Unilateral Or Discriminatory Digital Tax Measures

In June 2019, the New Zealand Government released a discussion document outlining two options for digital taxation measures: (1) to apply a separate DST to certain digital transactions, or (2) to change international income tax rules at the OECD.[185] The first option, the national DST, would be a 3 percent tax on gross turnover attributable to New Zealand of certain digital businesses. The businesses in scope would include intermediation platforms, social media platforms, content sharing sites, search engines and sellers of user data. The discussion document repeatedly specifies U.S. firms as being within the scope of the proposed tax.

[185] Tax Policy, Inland Revenue, *Options for Taxing the Digital Economy: A Government Discussion Document*, (2019), http://taxpolicy.ird.govt.nz/sites/default/files/2019-dd-digital-economy.pdf [New Zealand]; Benjamin Walker, *Analysing New Zealand's Digital Services Tax Proposal*, Austaxpolicy, (Apr. 23, 2020), https://www.austaxpolicy.com/analysing-new-zealands-digital-services-tax-proposal/.

Like other DSTs, the potential New Zealand DST is in tension with WTO rules. In addition, as proposed, it could be considered a 'covered tax' under various double taxation treaties, including the agreement with the United States. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, New Zealand should abandon consideration of its DST.

Online Content

New Zealand's proposed online safety legislation – the Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill - is currently before Parliament. The Bill, which is framed in response to the Christchurch attacks of 2019, proposes 2 main changes: 1) the establishment of a notice and take down scheme for 'objectionable' online content backed by civil penalties; and 2) a new criminal offence for the act of livestreaming objectionable content. A parliamentary committee has just reported on the Bill, recommending (among other things) to make the Bill's claim of extraterritorial application more explicit, such that international services accessible by New Zealand citizens will be obligated to remove content that fits in the notably broad and subjective category of 'objectionable', 'regardless of whether an online content host is resident or incorporated in New Zealand or outside New Zealand'. This approach would create a significant burden on internationally accessible services.

Data Sovereignty

The NZ Government has admirable 'Cloud First' policies[186] and has recently joined a Digital Partnership Agreement with Chile and Singapore, with supportive provisions that affirm DEPA "partners' levels of commitments relating to transmission of information and location of computer facilities" and "recognise the value of information flows and the development of new technologies and services."[187] However, in recent years indigenous Maori groups have increased concern about data on their people being stored outside New Zealand which may have implications for the free flow of data across borders.[188]

Nigeria

Copyright-Related Barriers

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

The Code prevents Pay TV and other broadcasting/streaming platforms from making their content exclusive and directs them to sub-license content at prices the Commission will regulate. This would create an unfavorable environment for such platforms as it reduces their value to their subscribers with a potential plunge in revenue. The Code takes away the liberty rights holders have to use and license their content as they deem fit. This appears to go against intellectual property rights.

[186] New Zealand Government, *Cloud Services*, *available at* https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/.

[187] New Zealand Foreign Affairs & Trade, *DEPA Modules*, *available at* https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-modules/#bookmark2

[188] New Zealand Government, *Co-designing Māori Data Governance*, *available at* https://data.govt.nz/toolkit/data-governance/maori/.

Broadcasting Code

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

Data Flow Restrictions And Service Blockages

Nigeria's 2013 Guidelines for Content Development in Information and Communication Technology establish local hosting requirements for government (sovereign), consumer and subscriber data, unless express approval has been obtained from the technology regulator (NITDA) for a cross-border transfer. This is in addition to 2011 Guidelines from the telecoms regulator requiring local hosting of subscriber data and from the Central Bank Guidelines requiring domestic routing of card transactions; the Central Bank Guidelines do not envisage the possibility of cross-border transfers.

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

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

Digital Taxation

The 2020 Finance Act introduces income tax obligations for non-resident companies providing digital goods and services in Nigeria. While the law applies to all non-resident companies earning above a certain threshold, extensive media coverage and analysis by experts has repeatedly mentioned the targeting of US multinationals. The law specifically references non-resident companies with a 'significant economic presence' in the country which is defined by a number of factors including: a minimum amount of revenue generated from users in Nigeria, transmitting data about Nigerian users, or the availability of local websites or local payment options. Exceptions have been built into the law for companies that are covered by a multilateral agreement to which the Nigerian government is a party.

Protection from Internet Falsehoods and Manipulation Bill

A Bill for Protection from Internet Falsehoods and Manipulation was introduced in the Senate in December 2019. Beyond hate speech, the proposed law broadly criminalizes statements that may prejudice the country's security, public health, public safety, or friendly relations with other countries; or that may diminish confidence in the government. Online content service providers would also be subject to orders to disable access to the offending content or to issue 'correction notices' to all end users that may have had access to the content. If passed the law would significantly limit freedom of speech and could also be used to suppress content from political opposition.

Pakistan

Restrictions On Cloud Service Providers

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

Unilateral Or Discriminatory Digital Tax Measures

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

Non-IP Intermediary Liability Restrictions

In February 2020, the Ministry of Information Technology and Telecommunication (MoITT) released the Citizens Protection (Against Online Harm) Rules. After civil society and industry groups expressed widespread concerns, the government announced in March 2020 that a committee led by the Pakistan Telecommunication Authority (PTA) would conduct an "extensive and broad-based consultation process with all relevant segments of civil society and technology companies." However, the Cabinet approved and published on Oct. 20, 2020 substantially similar rules. After another round of consultation, MoITT published a third version of the Rules on June 18, 2021.

The current version, titled "Removal and Blocking of Unlawful Content (Procedure, Oversight and Safeguards) Rules" retains the problematic provisions of the previous drafts. These include:

- → Mandatory local office presence and registration by the entity providing the service.
- → Obligation to appoint a local "compliance officer" to liaise with the PTA on content removal requests.
- → Obligation to appoint a local "grievance officer" and post their contact details online. The grievance officer would be required to redress complaints from the public within 7 days of receipt.
- → Short turnaround times for content removal (48 hours or 12 in case of an emergency).
- → A requirement to "comply with the user data privacy and data localization provisions" of a forthcoming Data Protection Law.
- → A requirement to provide user data to investigative authorities in accordance with existing federal law.

Internet Services

In November 2020, Pakistan adopted the Removal and Blocking of Unlawful Online Content (Procedure, Oversight, and Safeguards) Rules. The Government is currently re-drafting the Rules. The Rules apply to the removal and/or blocking of online content that is deemed unlawful on any information system. Local and international industry players have expressed concerns regarding provisions that would pose significant barriers to operating in Pakistan, including burdensome registration and licensing requirements, content restrictions, requirements that companies maintain a physical presence in Pakistan, and data localization. Pakistan periodically blocks access to Internet services for hosting content deemed to be "blasphemous" or "immoral" or on grounds that such services can be

used to "undermine national security." PTA has also sent notices to U.S. based social media platforms, threatening adverse action if those platforms did not remove objectionable content.

Data Localization

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

After multiple rounds of public consultation, MOoITT released a new version of the bill in August 2021. While some of the provisions around criminal liability and data localization are slightly improved, significant concerns remain regarding impediments to the cross-border flow of "sensitive" and "critical" data. Furthermore, these terms – "sensitive" and "critical" – are ill-defined, with "unregulated e-commerce transactions" falling within the definition of critical data

Pakistan is also in the process of finalizing a Cloud First Policy. This policy also imposes data localization requirements on wide and open-ended classes of "sensitive" and "secret" data. In the financial sector, the State Bank of Pakistan (SBP) prohibits financial sector institutions from storing and processing core workloads on offshore cloud.

These data localization requirements are ineffective at enhancing the protection of personal data, and would significantly increase costs for U.S. firms, potentially deterring market entry.

Panama

Data Residency

The Government Innovation Authority (AIG) of Panama published (09/10) resolution No. 52 ordering all cloud services, mission-critical, or state-security databases, or sensitive institutional data of all Government Entities must be held in Panamanian territory by December 31, 2022.

Burdensome Or Discriminatory Data Protection Regimes

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

In addition, Article 2 of the Protection of Personal Data bill mentions that databases containing "critical State data shall be kept in Panama." The definition of critical State data set forth in Article 3, however, is very broad. This could create a *de facto* data localization mandate for all data, even if this is not the objective of the law. The U.S. government should work with Panama to ensure that this language does not result in a data localization requirement.

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect the

taxi industry by limiting the number of vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

- *Fleet restrictions:* No individual may own more than two vehicles that are used to provide app-based transportation services. Companies are not allowed to own fleets, a restriction that does not apply to the taxi industry or to other modes of transportation.

- *Vehicle requirements:* Vehicles providing app-based transportation must be less than seven years old. This requirement does not apply to any other type of transportation.

Peru

Copyright-Related Barriers

Peru does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Peruvian law currently includes a long but inflexible list of rules that does not clearly provide for open limitations and exceptions that are necessary for the digital environment[189] – 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.[190]

Peru remains out of compliance with key provisions under the U.S.-Peru Trade Promotion Agreement (PTPA). Article 16.11, para. 29 of the PTPA requires certain protections for online intermediaries against copyright infringement claims arising out of user activities. USTR cited this discrepancy in its inclusion of Peru in the 2018 Special 301 Report, and Industry supports its inclusion in the 2022 NTE Report. Industry urges USTR to engage with Peru and push for full implementation of the trade agreement and establish intermediary protections within the parameters of the PTPA.

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

- The creation of a whitelist, which will include the permitted countries for cross-border transfer of data, even though the Peruvian Data Protection Law does not include such restrictions. The proposal creates barriers for service´s trade and obstacles to product development and innovation by giving clearly preferential treatment to domestic data storage.

- The issuance of digital security quality badges for private companies, which will be the governmental cybersecurity certification ignoring the existence of global security standards.

- The creation of a national data center intended to host the information provided by the public sector entities.

The proposal also includes broad definitions of digital service providers that do not consider key differences among digital service providers, such as Cloud Services Providers, that do not have access to nor intervention in their client's information, and organizations that use digital channels to provide their services. The Data Protection Authority would determine model contract clauses, which appear to exceed what is currently required under the Data Protection Law. The national data center would incentivize domestic data storage by providing infrastructure

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

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

to domestic data center operations, where the state would have total control over data. The ability to move data and access information across borders is essential for businesses regardless of size or sector. Data localization measures serve as barriers to trade and offer governments a false choice between achieving regulatory objectives, such as data privacy and security, and data movement. Instead of going down this path of data localization, Peru should rely on the already approved Guidelines for the Use of Cloud Services for entities of the Public Administration, and endorse the use of international standards and best practices, which are accepted and adopted, such as ISO 9001, ISO 27001, ISO 27002, ISO 27017, ISO 27018 y SOC 1, 2 y3.

Local Content Requirements

On July 11, 2021, the Secretary of the Peruvian Congress published the report of a bill that proposes to modify the Audiovisual and Cinematographic Activity Promotion Law. The document unifies two bills, the first (6257) creates screen quotas, while the second (7465) proposes the creation of a Film Commission and the promotion of audiovisual productions. The published text is now prepared to be discussed by the plenary of Congress, which is expected to happen in the coming weeks.

The bill seeks to do a number of things, including establishing local content requirements and the creation of a new incentive regime. Specifically, Article 20 states that the Ministry of Culture may set "annual rules on minimum percentages of exhibition and commercialization of Peruvian cinematographic works in any medium or system. This percentage must not exceed twenty (20percent) percent of the total commercial and cultural works exhibited in the country during the same period of time."

If these policies were enacted and services failed to launch, Peruvian audiences and creators would have fewer legitimate options for film and television content. In addition, these policies, if enacted, would plainly violate Peru's free trade agreement obligations.

Digital Trust Framework Draft Regulations

In 2020, the Digital Government Secretariat of Peru released Emergency Decree 007 - Digital Trust Framework draft regulations for consultation.[191] The proposal appears to give preferential treatment to domestic data storage and domestic service providers. Industry reports that the draft proposal includes: (1) the creation of a whitelist of permitted countries for cross-border transfer of data, even though the Peruvian Data Protection Law does not include such restrictions; (2) the issuance of digital security quality badges for private companies which will be the governmental cybersecurity certification (ignoring the existence of global security standards); and (3) the creation of a national data center intended to host the information provided by the public sector entities. The proposal also includes broad definitions of digital services providers, failing to consider key differences among digital services and the differences in these services' ability to access client's information, or organizations that use digital channels to provide their services. The Data Protection Authority would determine model contract clauses, which appear to exceed what is currently required under the Data Protection Law. The National Data Center would incentivize domestic data storage by providing infrastructure to domestic data center operations, granting the government control over the data.

As noted elsewhere in these comments, the ability to move data and access information across borders is essential for businesses regardless of size or sector. Peru should instead rely on the already approved Guidelines for the Use of Cloud Services for entities of the Public Administration, and endorse the use of international standards and best practices, which are accepted and adopted, such as ISO 9001, ISO 27001, ISO 27002, ISO 27017, ISO 27018 and SOC 1, 2 and 3.

[191] José Antonio Olaechea, *Doing business in Peru: overview*, Thomson Reuters Practical Law, *available at* https://uk.practicallaw.thomsonreuters.com/0-500-7812?transitionType=Default&contextData=(sc.Default)&firstPage=true (last accessed Oct. 29, 2020).

Russia

Data Flow Restrictions And Service Blockages

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

- Article 18 of Federal Law 242-FZ: requirement to store and process personal data concerning Russian citizens in Russian data centers. According to the current regulatory interpretation of this rule, the initial collection, processing, and storage of data must occur exclusively in Russia. Once this "primary processing" on local servers has occurred, data can be exported outside Russia subject to consent. Given the requirement to localize processing, a global web service would typically be compelled to re-architect its global systems and networks in order to comply with such a provision.

- Articles 10.1 and 10.2 of Federal Law No. 149-FZ: requirement to retain metadata for provision to Russian security agencies, and content-posting restrictions for websites.

- "Yarovaya Amendments" amending Federal Laws 126-FZ and 149-FZ: requires "organizers of information distribution on the internet" to store the content of communications locally for six months, with longer metadata storage requirements for different types of providers. In addition, this package of laws requires internet services to provide government officials with sensitive user information and to assist national security agencies in decrypting any encrypted user messages.

- "News Aggregators Law": According to the recently adopted amendments to the Federal Law 149-FZ, news search and aggregation services that exceed 1 million daily visitors and are offered in the Russian language with the possibility of showing ads must be offered through a local subsidiary in Russia. Foreign providers are not permitted to offer such services directly across the border, even though they are allowed to own the local company that offers them. The law additionally provides for significant content restrictions.

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

Filtering, Censorship, And Service-Blocking

Since 2012, Russia has been implementing a Blacklist law initially aimed at protecting children from harmful information online. The Blacklist law keeps getting expanded onto new types and categories of content including extremist, suicide-inciting, drugs-promoting, etc. By this law, intermediaries are envisioned to block certain sites or certain types of content.[192] For example, Russia has ordered all of Wikipedia to be blocked due to problematic content on a single page.

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

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

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

"Landing" Law

In July 2021, President Putin signed into force a "Landing Law", mandating large foreign IT companies to set up direct local presence in Russia. The law applies to foreign companies which own websites/apps accessed daily by more than 500,000 users from Russia and meet at least one of the following conditions: (i) it is in Russian or a Russian local language; (ii) it has ads targeted at Russian users; (iii) the website/app owner processes Russian user data; (iv) websites/apps receive money from Russian individuals and legal entities. Amongst other requirements, foreign companies will also be required to install Russian Government-provided software which will be counting the users of the website or app. Failure to comply may result in very harsh penalties, ranging from a ban for Russian companies / users to advertise with such foreign platforms or to transfer money and make payments to full or partial blocking or throttling of incompliant websites/apps. Such local presence requirements, coupled with onerous compliance requirements and harsh penalties, severely constrain the ability of US companies to operate in Russia.

Anti-Censorship Act

In January 2021, the newly imposed Anti-Censorship Act came into force in Russia, giving authorities power to block or throttle platforms censoring "socially significant information." A platform will be liable for censorship by the Russian government if it restricts access to such information, such as termination of Russian accounts as well as other content restrictions including for trade compliance purposes. The definition of censorship is extremely broad, potentially covering every single restriction applied to content such as termination of Russian accounts as well as other content restrictions including for trade compliance purposes. The law, which was introduced as a response to removals of Russian media content by international platforms channels and other content restrictions [193], targets foreign companies, in particular US digital services providers, and severely constrains their ability to operate and offer their services in the Russian market.

Restrictions From Failure To Block And/Or Remove Content

In January 2021, a law introducing significant fines for a failure by companies to block prohibited content was adopted. As per previously adopted legislation, digital platforms targeted by the law are all US digital services companies, which are required to forward the government's content removal requests to their users. If the reported content is not promptly taken down by the user, the onus is on the platform to block access to such content. Non-compliance could mean the blocking of the platform altogether by the Internet Service Provider (ISP). The new law introduced fines for violations that are astronomically high - reaching 10 to 20% of revenue by the infringer for repeat violations.

Separately, the Russian government has also exerted immense pressure on US digital platforms to remove political content deemed by the government as illegal. These have included threats to prosecute their local employees, which make it extremely challenging for U.S. digital companies to operate and compete on a reasonable basis in Russia.

[193] Human Rights Watch, *New Law Would Expand Internet Censorship in Russia*, (Nov. 23, 2020), https://www.hrw.org/news/2020/11/23/new-law-would-expand-internet-censorship-russia.

Pre-Installation Of Russian Software

In December 2019, Russia adopted a law that requires the pre-installation of Russian software on certain consumer electronic products sold in Russia and sets a dangerous precedent.[194] The law took effect in January 2021. The scope of devices includes smartphones, computers, tablets, and smart TVs, and the scope of applications includes the default pre-installation of the local search engine, navigation tools, anti-virus software, software that provides access to e-government infrastructure, instant messaging and social network software, and national payment software. This has impacted U.S. companies' ability to compete on a level playing field in the Russian market, with broader implications for continued market access, consumer choice as well as industry development.

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.

Data Flow Restrictions And Service Blockages

The Communications and Information Technology Council of Saudi Arabia (CITC) issued the Cloud Computing Regulatory Framework in 2018, with revisions made in 2019.[195] The rules contain a provision on data localization that may restrict access to the Saudi market for foreign Internet services.[196] The regulation will also increase ISP liability, create burdensome new data protection and classification obligations, and require compliance with cybersecurity and law enforcement access provisions that depart from global norms and security standards. CITC would be granted broad powers to require cloud and ICT service providers to install and maintain governmental filtering software on their networks.

The National Cybersecurity Authority (NCA) 2018 Essential Cybersecurity Controls (ECC) framework states that data hosting and storage when using cloud computing services must be located within the country.[197] The draft NCA 2020 Cloud Cybersecurity Controls (CCC) framework requires operators to provide cloud computing services

[194] *Russia passes law forcing manufacturers to install Russian-made software*, The Verge (Dec. 3, 2019), https://www.theverge.com/2019/12/3/20977459/russian-law-pre-installed-domestic-software-tvs-smartphones-laptops.

[195] *Saudi Arabia's cloud computing regulatory framework 2.0*, Lexology (Mar. 1, 2020), https://www.lexology.com/library/detail.aspx?g=f32fe934-c8f6-4a99-acc8-f5dd50342c53.

[196] *Id.* ("With regard to cloud computing, the ECC:2018 requires entities subject to its requirements to ensure that the hosting and storage of their data occurs in Saudi Arabia. This seems to be a very broad restriction on the use of cloud services based outside the Kingdom, and it is likely to have a significant impact on the cloud market in Saudi Arabia. Cloud service providers with infrastructure in the Kingdom are likely to do well; cloud service providers based outside the Kingdom are going to need clarity as to the impact on their business; and cloud customers in the Kingdom that are subject to the ECC:2018 are likely to need their cloud service providers to confirm compliance.").

[197] National Cybersecurity Authority, *Essential Cybersecurity Controls*, *available at* https://itig-iraq.iq/wp-content/uploads/2019/08/Essential-Cybersecurity-Controls-2018.pdf.

from within the country, including all systems including storage, processing, monitoring, support, and disaster recovery centers. The requirement applies to all levels of data.[198] Neither the ECC, nor the draft CCC, distinguish between data localization requirements for different levels of data classification, which conflicts with the 2018 Cloud Computing Regulatory Framework (CCRF).[199]

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

Restrictions On Cloud Service Providers

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

This regulation also creates new data protection and data classification obligations that apply to cloud services. Sensitive data classified at levels 3 or 4 require local storage. What specific types of data fall into these categories is not explicitly defined in the framework, leaving it within the discretion of the regulator for the financial vertical (the Saudi Arabian Monetary Authority) to classify financial data as sensitive, requiring localization. It is important to note that the regulator has not yet issued any rules on data classification but could easily do so.

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

Singapore

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

---

[198] *See Saudi Arabia's draft Cloud Cybersecurity Controls*, Lexology (Apr. 29, 2020), https://www.lexology.com/library/detail.aspx?g=7e35491b-6ab0-40c6-8d10-26351fb2bc37.

[199] The CCRF allowed for lower sensitivity levels of data to be hosted outside the country, including: non-sensitive public authority data, sensitive private sector data where no sector-specific regulations apply, or "Content qualifying for Level 1 or Level 3 treatment, for which the Cloud Customer elects Level 2 treatment." *See* Communications & Information Technology Commission, Cloud Computing Regulatory Framework, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx.

Foreign Interference (Countermeasures) Act

The Foreign Interference (Countermeasures) Act (FICA) was passed on 4 Oct 2021. It has not been decided when this will come into force, though 1Q 2022 are the current indications. Similar to the earlier content legislation, the Protection from Online Falsehoods and Manipulation Bill (POFMA), FICA requires online services to remove content or carry 'corrections' on their platforms in response to claims from the government or from individuals that content is being covertly influenced by a foreign actor. It is important that FICA, with its broad powers and the anticipatory nature of some of its proposed directions, will be used judiciously to weed out coordinated influence campaigns and not as a modality of targeting critical political speech. How the law is used matters, and other countries in the region will be paying attention to the news of FICA passing into law, and the scenarios in which those powers are eventually deployed. The use of broad-ranging powers to moderate content on internet platforms, and its impact on free speech, matters. Such powers have the potential for regional/global contagion. Depending on how the powers are wielded, it may impact companies' ability to operate responsibly within the market.

South Africa

Data Flow Restrictions

In April 2021, the South African Department of Communication and Digital Technologies released a Draft Data and Cloud Policy with the aim of promoting South Africa's data sovereignty and security. The policy includes provisions that would require data to be processed and stored in-country. While the policy does not have the force of law, it is expected to influence future lawmaking and enforcement of existing laws.

Duties On Electronic Transmissions

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

Sharing Economy Barriers

Drivers seeking to provide transportation services outside of the traditional taxi industry and via apps face market access and operational restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of vehicles, lowering the quality of the services they can provide, and raising the price consumers must pay for those services.

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

Taiwan

Non-IP Intermediary Liability Restrictions And Undue Burdens For U.S. Companies

Taiwan's National Communications Commission is consulting on a draft bill that would impose administrative liability on intermediaries in the context of unlawful content, including online safety, harmful content and misinformation. The direction of the draft Digital Communication Act may impose broad requirements, including disproportionate and ambiguous provisions targeting the removal of online content, sensitive commercial data disclosure, data localization and algorithmic transparency. The liability structure is designed to impose cumulative obligations on intermediaries according to the sizes, thereby increasing significant compliance risks only for U.S. based user-generated content and live streaming services.

Data Localization

While Taiwan's sectoral regulations, such as financial services, health records and public sector, allow institutions to outsource workloads to overseas cloud, there are wordings explicitly expressing regulator's preference of data localization, such as "in principle, where customer data is outsourced to a cloud service provider, the location for processing and storage shall be within the territories of the R.O.C.," and, in the case of overseas outsourcing, "except with the approval of the competent authority, backups of customer important data shall be retained in the R.O.C." These expressions, when judged in conjunction with additional burdensome and ambiguous approval requirements, may have in effect created a de facto data localization requirement. Specifically, when an institution contemplates the outsource location, it is clear that the regulator prefers domestic destination; if the institution decides to get approved for overseas outsourcing, it has to bear the over-burdensome documentary requirements which may cause unnecessary compliance cost; even though FI is willing to bear the burden, the review process is very likely to be lengthy and unpredictable; and, the institution still need to maintain a local copy of "important" data.

Cloud Outsourcing For Financial Services

In Q4 2019, FSC issued an amendment to the Regulation Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation, and the Directions for Operation Outsourcing by Insurance Enterprises, the first management guidance on the use of cloud computing services by financial and insurance institutions. The amendments include several requirements that would make it difficult for financial institutions to use cloud computing services such as over-burdensome documentary requirements, ambiguous approval criteria, unclear approval timelines, and excessive duplicated audit requirements which increase compliance costs for financial institutions and Cloud Service Providers. In addition, there's currently no similar regulations addressing cloud outsourcing needs, and institutions are requested to discuss with FSC on a case-by-case basis for the Securities and Futures sector, e-Payment service providers, and fintech start-ups, elevating a Cloud adoption entry barrier constrained by the lack of guidelines.

Discriminatory Of Non-Objective Application Of Competition Regulations

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

Sharing Economy Barriers

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

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

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

Unilateral Or Discriminatory Digital Tax Measures

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

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

Digital Communications Act

The industry reports that Taiwan's National Communications Commission (NCC) is contemplating a content regulation bill ("the Digital Communications Act, DCA"), which is likely to closely model after the EU's DSA, with measures to control misinformation and impose mandatory third-party consultations on content removal and community guidelines. While the NCC has not shared the draft, the industry worries that over-extensive content regulations may reinforce censorship and add friction to cross-border digital trade.

News Media Bargaining Code

The industry reports that the Taiwan government is under pressure from news media publishers to impose a mandatory news media bargaining code to regulate commercial relations between news publishers and digital platforms. While the Taiwan government has not released any draft, the industry worries that the Code may be in tension with longstanding international trade principles of national treatment and most favored nation (MFN), by unfairly discriminating against foreign digital service suppliers and providing preferential treatment to local advertising and other digital service suppliers.

Thailand

Restrictions On Online Speech And Press Freedom

Industry had previously raised concerns with the Computer Crime Act, amended in 2016. In November 2019, the Ministry of Digital Economy and Society established an Anti-Fake News Center to combat what is considered "false and misleading" in violation of the Computer Crimes Act.[200] The government has also issued emergency decrees in relation to the global pandemic that further restrict online and press freedom.[201]

[200] *Freedom on the Net 2020: Thailand* (2020), https://freedomhouse.org/country/thailand/freedom-net/2020

[201] *Id.*

Private Data Monitoring And Seizure

In 2019, Thailand passed a controversial Cybersecurity Law following amendments in 2018. Industry has criticized the law due to provisions that enable government surveillance.[202] Under the new law, officials are granted authority to "search and seize data and equipment in cases that are deemed issues of national emergency."[203] This could "enable internet traffic monitoring and access to private data, including communications, without a court order."[204]

Data Flow Restrictions And Service Blockages

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

Non-IP Intermediary Liability Restrictions

Internet service providers who "assist or facilitate" the commission of defamation by another person can be liable as supporters of the defamatory offenses, even if the actor does not realize they are assisting or facilitating the offense.[205] 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. [206] Such rules have resulted in the blockage of U.S. online services in Thailand.

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 Cross-Border Data Flows And Data And Infrastructure Localization Mandates

On July 6, 2019, the Presidential Circular on Information and Communication Security Measures No. 2019/12 was published and creates important security measures and obligations.[207] Article 3 prohibits public institutions and organizations' data from being stored in cloud storage services that are not under the control of public institutions. The Circular also requires that critical information and sensitive data be stored domestically. Draft regulation is expected that will also mandate localization of data produced by banks and financial services.

---

[202] *See* Asia Internet Coalition Statement, (Feb. 28, 2019) ("Protecting online security is a top priority, however the Law's ambiguously defined scope, vague language and lack of safeguards raises serious privacy concerns for both individuals and businesses, especially provisions that allow overreaching authority to search and seize data and electronic equipment without proper legal oversight. This would give the regime sweeping powers to monitor online traffic in the name of an emergency or as a preventive measure, potentially compromising private and corporate data."), *available at* https://aicasia.org/wp-content/uploads/2019/03/AICStatement_Thailand-Cybersecurity-Law_28-Feb-2019.pdf.

[203] *Thailand Passes Controversial Cybersecurity Law*, TechCrunch (Feb. 28, 2019), *available at* https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/.

[204] *Id.*

[205] Dr. Kanaphon Chanhom, Defamation and Internet Service Providers In Thailand, *available at* https://www.law.uw.edu/media/1423/thailand-intermediary-liability-of-isps-defamation.pdf.

[206] Eva Galperin, *Suspended Sentence Good News for Thai Webmaster Jiew, But the Threat to Freedom of Expression Remains, Electronic Frontier Foundation*, (May 30 3012), *available at* https://www.eff.org/deeplinks/2012/05/suspended-sentence-good-news-thai-webmaster-jiew-threat-freedom-expression-remains.

[207] *New Presidential Decree on Information and Communication Security Measures*, Lexology, (July 25, 2019), availabe at https://www.lexology.com/library/detail.aspx?g=8e18f85a-286f-4d29-b017-b17541c3c66b.

The Regulation on Information Systems of Banks, published on March 15, 2020, still requires banks and financial services to keep their primary (live/production data) and secondary (back-ups) information systems within the country.[208] The Regulation establishes a framework for use of cloud services as an outsourced service, but only applies for services located in Turkey.[209]

The Law on the Protection of Personal Data (numbered 6698) governs international transfer of data, which is permitted under the following conditions: (1) when transferring personal data to a country with adequate level of protection, (2) obtaining explicit consent of data subjects, or (3) ad-hoc approval of the Data Protection Board to the undertaking agreement to be executed among data transferring parties.[210] However, industry reports that conditions make it hard to transfer data under these frameworks. Turkey has not yet announced a list of countries that meet the standard of adequate level of protection. Further, the Data Protection Board has yet to grant approval to companies that have sought the ad-hoc approval. While Turkey and the U.S. are aiming to increase trade relations, restrictions created by Turkish data protection legislation confine companies' ability to actively participate in the Turkish economy. Per an economic reform packet introduced in 2020, Turkey aims to align Article 9 of its Data Protection Law governing cross-border data flows with GDPR by March 2022.

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

Unilateral Or Discriminatory Digital Tax Measures

Turkey enacted a 7.5 percent digital tax which became effective March 1, 2020. The legislation also permits the President of Turkey to either reduce the rate to 1 percent, or double the tax to 15 percent.[211] The global threshold is 750 million euros, with a local threshold of 20m TYR. The tax applies to revenue generated from the following services: (1) "all types of advertisement services provided through digital platforms" ; (2) "the sale of all types of auditory, visual or digital contents on digital platforms . . . and services provided on digital platforms for listening, watching, playing of these content or downloading of the content to the electronic devices or using of the content in these electronic devices"; and (3) "[s]ervices related to the provision and operation services of digital platforms where users can interact with each other." Digital service providers that provide the covered services, but whose revenue does not make them subject to the tax, still must certify that they are exempt.[212]

On June 2, 2020, USTR initiated a Section 301 investigation into Turkey's DST. On January 6, 2021, USTR determined that Turkey's DST is unreasonable and discriminatory and burdens or restricts U.S. commerce. On June 7, 2021, USTR determined to take action in response in the form of additional duties of 25% on certain products of Turkey, and it also determined to suspend application of the additional duties for up to 180 days. In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to

[208] *New Regulation on Bank IT Systems and Electronic Banking Services*, Lexology, (Mar. 18, 2020), https://www.lexology.com/library/detail.aspx?g=820f9766-219b-4196-9554-bfc715fd1676.

[209] *Id*.

[210] Law on the Protection of Personal Data, *available at* https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf.

[211] Law numbered 7194 published in the Official Gazette dated (July 19, 2019) and numbered 30971, *available at* https://www.mevzuat.gov.tr/MevzuatMetin/1.5.7194.pdf.

[212] *Turkey: Digital Services Tax, A Primer*, KPMG, (Apr. 21, 2020), https://home.kpmg/us/en/home/insights/2020/04/tnf-turkey-digital-services-tax-a-primer.html.

establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, Turkey should repeal its DST. In the meantime, USTR should reject pressure to terminate its Section 301 investigation while the DST remains in effect.

Law On Geographical Information Systems

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

Import Restrictions

The Turkish government is taking increasing actions in relation to imports. In April and May, the government temporarily increased the customs duty for imported game consoles by 50 percent and introduced a 30 percent "additional customs duty" for a variety of intermediary and consumer goods imported through commercial channels until December 31, 2020. This applies to nearly 3,000 types of products, including technological devices, home appliances, industrial products, cosmetic and beauty products, musical instruments, building materials and textile products. These duties are imposed in the form of "additional customs duties" due to TR's obligation arising from its Customs Union with the EU to not amend "customs duty" rates. TR has argued the duties are justified based on provisions of WTO Agreements allowing members to take measures to protect domestic industries.

Regulation Of Social Network Providers

Turkish lawmakers passed legislation ("Law on Amendment of the Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications") in July 2020 that grants the government sweeping new powers to regulate content on social media.[213] The law went into effect October 1, 2020. The law requires social network providers with more than a million users to: (i) establish a representative office in Turkey, (ii) respond to individual complaints in 48 hours or comply with official take-down requests of the courts in 24 hours, (iii) report on statistics and categorical information regarding the Requests every 6 months, (iv) take necessary measures to ensure the data of Turkish resident users are kept in Turkey. In case of noncompliance, social network providers face serious monetary fines and 50-90 percent possible bandwidth reduction to their platform. While these amendments aim to regulate social network providers and enhance the obligations of hosting and content providers in order to protect the individuals in the internet environment, the vague obligation of data localization may require significant and costly operational changes for businesses and facilitating the execution of content removal/access blocking decisions raises significant concerns that it may lead to censorship of unwanted contents and may hinder free speech of individuals.

Further to the 2020 Amendment to the Internet Law 5651, the Turkish government is expected to introduce a social media disinformation bill in Q4 of 2021. While a draft law has not yet surfaced, the new bill will likely require a Turkish citizen to be appointed as a representative (rather than a legal entity per the 2020 amendment) and introduce fines and penalties for organized spread of disinformation.

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

[213] *See, e.g., Facebook to defy new Turkish social media law*, The Financial Times, (Oct. 5, 2020), https://www.ft.com/content/91c0a408-6c15-45c3-80e3-d6b2cf913070.

Ukraine's copyright law.[214] These problems have not been effectively addressed in the past year.[215] 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.[216] These and other provisions are in direct conflict with Section 512 of the Digital Millennium Copyright Act, and are harming the ability of U.S. companies to access the Ukraine market.

Restrictions On Cloud Service Providers

Article 11(4) of the Draft Cloud Law No. 2655 that was passed in the first reading prohibits processing of personal data and legally protected information of the public users – state and municipal authorities, state enterprises and organizations – by any cloud means, if the cloud services and/or processing centers are located outside of Ukraine. This requires any cloud infrastructure used by the public users to be physically located in Ukraine. The Data Localization Requirement is discriminatory and contrary to the international commitments of Ukraine, and the national legislation, including Ukraine's WTO GATS commitments, the Ukraine-EU Association Agreement and Article 14 of the Law of Ukraine on Protection of Economic Competition.

Legal Liability For Online Intermediaries

Ukraine adopted a law, "On State Support of Cinematography" in March 2017 which established a notice-and-takedown system for copyright enforcement. However, the final law goes beyond what the notice-and-takedown system under Section 512 of the DMCA requires in the United States and in the many U.S. trading partners who have adopted similar systems for FTA compliance. The legislation revised Article 52 of Ukrainian copyright law to impose 24- and 48-hour "shot clocks" for online intermediaries to act on demands to remove content in order for them to avoid liability. This deadline may be feasible at times for some larger platforms who can devote entire departments to takedown compliance, but will effectively deny market access to smaller firms and startups, and is inconsistent with the "expeditious" standard under U.S. copyright law. The law also effectively imposed an affirmative obligation to monitor content and engage in site-blocking, by revoking protections for intermediaries if the same content reappears on a site twice within three months, even despite full compliance with the notice-and-takedown system. The newly presented bill on Copyright and Related Rights №5552-4 (registered June 9, 2021) in its Article 58 keeps the norm on 24- and 48-hour "shot clocks" for online intermediaries to act on demands to remove content in order for them to avoid liability.

United Arab Emirates

Infrastructure-Based Regulation Of Online Services

In the United Arab Emirates (UAE), nationally controlled telecom services have consistently throttled foreign VoIP and communications services, including WhatsApp VOIP, Apple Facetime, Google Hangouts and Duo, LINE, and Viber.[217] This throttling has created significant market access barriers in a key Middle East market for U.S.-based

[214] USTR, 2016 Special 301 Report, (April 2016), *availabe at* https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.

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

[216] Law of Ukraine "On State Support of Cinematography in Ukraine"

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

internet services and apps. However, despite acknowledging the negative implications for foreign services, UAE regulators have declined to intervene, and instead have continued to insist that only national providers can provide these forms of communications services.[218] These restrictions impede market access for U.S. services and appear to conflict with UAE's GATS commitments.

U.S internet services face similar barriers in Morocco, Saudi Arabia, and Oman, where nationally owned telecom services have engaged in similar forms of throttling, however, the throttling is most severe in the UAE.[219]

Non-IP Intermediary Liability Restrictions

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

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

- A penalty of imprisonment and a fine not exceeding AED 1,000,000 may be imposed on any person who creates or runs an electronic site or any IT means, to deride or to damage the reputation or the stature of the UAE or any of its institutions, the President of the UAE, the Vice President, any of the Rulers of the Emirates, the Crown Princes, the Deputy Rulers, the national flag, the national anthem, the emblem of the state, or any of its symbols.

- Producing, transmitting, publishing, and exploiting through an electronic site, gambling and/or pornographic material or any other material that may prejudice public morals;

- Insulting others or attributing to another an incident that may make him/her subject to penalty or contempt by others by using an electronic site;

- Using electronic sites to display contempt for any holy symbols, characters, figures, and rituals of Islam, including the Divinity and the Prophets, and for any other faiths or religions and any of their symbols, characters, figures and rituals.

Sharing Economy Barriers

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

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

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

restrictions that serve no legitimate public interest and are instead meant to protect the taxi industry by limiting the number of for-hire vehicles and raising the price consumers must pay for those services.

→ *Minimum price requirement:* For-hire transportation providers must charge 30 percent more than taxis.

→ *Data-sharing requirement:* Companies providing transportation apps are routinely pressured to share data in real time, via integration into government computer systems.

The National Media Council Content Creators law applies to UAE residents and influencers operating in the UAE, including all social influencers who use their social media channels to promote and/or sell products. The law imposes licensing requirements and covers a broad scope, including "any paid or unpaid form of presentation and/or promotion of ideas, goods or services by electronic means, or network applications". Such onerous licensing requirements covering a broad scope of social influencing activities add unnecessary friction to digital trade and inhibit new social influencers, particularly those based outside of the UAE from promoting their services to the UAE market. Though law has not been widely enforced, it could be enforced on a highly selective basis to target certain influencers at will.

United Kingdom

Copyright-Related Barriers

While the UK government has stated it has no plans to implement the recently passed EU Copyright Directive, the UK is considering its post-Brexit domestic policy priorities.[220] If the UK were to implement measures similar to those just passed in the EU, online service providers in the U.S. and elsewhere would be subject to a moving target in the UK for years to come. Smaller startups and entrepreneurs would be deterred from entering the UK market given the difficulty of raising funds from venture capitalists that have consistently characterized such rules as strong impediments to investment.

Non-IP Intermediary Liability Restrictions

In April 2019, the UK government presented the Online Harms White Paper ("the White Paper") to Parliament that outlines an unprecedented approach to regulating content online.[221] The UK Government has published the Online Safety Bill, the legislation that will introduce the new regulatory regime for online harms and formally establish Ofcom as the regulator for online platforms. The Bill has been published in draft form, and will now be scrutinised by a Committee of MPs and Lords before beginning the formal legislative process in the second half of this year. We expect implementation in 2023.

The White Paper is incredibly wide-ranging, and includes a number of untested ideas. The "online harms" these new policies would target include both lawful and unlawful content, including everything from "serious violent" content to "interference with legal proceedings" and "inappropriate" content accessed by children. The proposal not only has trade implications, but also free expression concerns, to the extent these rules would conflict with U.S. law. The proposal also anticipates placing burdens on small businesses. While it is suggested that the new regulatory regime would assist startups and SMEs in fulfilling their obligations under the new rules, and emphasizes the need for proportionality, the measures contemplated in the White Paper are significant and it is unclear whether the substantial burden will be offset by this assistance. The White Paper also presents vague and untested ideas regarding "duty of care." For example, it is suggested that platforms would have to determine 'foreseeable' harm and act accordingly. The penalties contemplated are concerning and include "disruption of business activities" that would allow the regulator to force other online services to block the targeted companies'

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

[221] Sec'y of State for Digital, Culture, Media & Sport, and the Sec'y of State for the Home Dep't, *Online Harms White Paper* (Apr. 2019).

availability or presence online, ISP blocking, and senior management liability extending to criminal liability. The UK Office of Communications also released a report on regulating online platforms to address online harms.[222]

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

Following a public consultation, the UK announced in 2019 it would impose a digital services tax. The 2020 Finance Budget, presented on March 11, 2020, included legislation to introduce a digital services tax of 2 percent. The tax is to be paid on an annual basis, with accruals beginning April 1, 2020. The UK has moved forward with steps to implement the legislation with the major parties in Parliament approving the measure's passage. The tax applies to revenues of "digital services activity" which are (1) "social media platforms," (2) "internet search engines," or (3) "online marketplaces." The legislation seeks to address double taxation in instances where a firm owes multiple digital services taxes, but it is not clear whether sufficient certainty is provided to reduce double taxation under existing corporate tax structures. The UK expects to raise 2 billion pounds over a five-year period with the DST. The practical effect of the tax will be that a handful of U.S. companies will contribute the majority of the tax revenue. UK domestic constituencies have also made requests to triple the DST to 6 percent.

On June 2, 2020, USTR initiated a Section 301 investigation into the UK DST. On January 14, 2021, USTR determined that the UK DST is unreasonable and discriminatory and burdens U.S. commerce. On June 7, 2021, USTR determined to take action in response in the form of additional duties of 25 percent on certain products of the UK, and it also determined to suspend application of the additional duties for up to 180 days.

In light of the recent agreement by the OECD and nearly 140 participating member governments and jurisdictions to establish a modern, multilateral framework for taxation, including Pillar One on the reallocation of taxation rights, the UK should repeal its DST.

Backdoor Access To Secure Technologies

The UK has pursued policies that undermine secured communications by mandating law enforcement access to encrypted communications. Passed in 2016, the Investigatory Powers Act allows for authorities to require removal of "electronic protections" applied to communications data.[223] The UK also recently joined the United States and Australia in a concerning request to Facebook regarding undermining the security of user communications.[224]

Restrictions On Cross-Border Data Flows

The EU's General Data Protection Regulation (GDPR) went into effect last year, and was implemented into UK law under the Data Protection Act 2018. Since that time, some U.S. services have stopped operating in the EU over

[222] Office of Communications, *Online Market Failures and Harms – An Economic Perspective on the Challenges and Opportunities in Regulating Online Services* (Oct. 28, 2019), https://www.ofcom.org.uk/__data/assets/pdf_file/0025/174634/online-market-failures-and-harms.pdf.

[223] *See* Investigatory Powers Act (2016), *available at* https://www.legislation.gov.uk/ukpga/2016/25.

[224] Press Release, *CCIA Dismayed by AG Opposition to Stronger Consumer Encryption Options*, (Oct. 3, 2019), http://www.ccianet.org/2019/10/ccia-dismayed-by-ag-opposition-to-stronger-consumer-encryption-options/.

uncertainties regarding compliance.[225] If the UK intends to maintain GDPR compliance following Brexit, as expected pursuant to the EU Withdrawal Act (2018),[226] it is critical that there remain clear rules for U.S. exporters offering services in the UK. It is also critical that there remains a valid mechanism for companies to legally transfer the data of UK citizens following the UK's exit from the EU.

Market Access Barriers For Communication Providers

Telecommunications services of all sizes rely on fair and transparent public procurement regimes. They also rely on consistent, pro-competitive regulation of business-grade whole access and nondiscrimination by major suppliers. For example, even in the United States there is no adequate regulation on bottlenecks in access layers, particularly in the business data service market. The UK market has seen greater competition, with regulation and legal separation requiring the main national operator to provide wholesale/leased access and treat all of its customers equally. Furthermore, the regulator is legally required to carry out detailed market reviews regularly and to impose regulatory remedies where the biggest national operator is found to have significant market power.

Vietnam

Copyright-Related Barriers

Vietnam does not have a comprehensive framework of copyright exceptions and limitations for the digital economy. Vietnamese law provides a short list of exceptions that do not clearly cover core digital economy activities such as text and data mining, machine learning, and indexing of content. IA urges USTR to work with Vietnam to implement a flexible fair use exception modeled on the multi-factor balancing tests found in countries such as Singapore and the U.S. [227]

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

Vietnam's use of localization measures is a continuing problem for U.S. companies operating in the country. On January 1, 2019, Vietnam's Law on Cybersecurity took effect. The law includes both data localization mandates and content regulations that raise concerns regarding Vietnam's compliance with its trade obligations. The law requires covered service suppliers to store various categories of data within the country for a certain period of time. However, the law states that the data localization requirements will only be enforced after detailed guidance is issued in an implementing decree. The latest draft of this Decree reportedly was discussed in August 2020. Judging from the current draft, it appears that Vietnam is creating barriers for foreign service suppliers in order to favor competing Vietnamese telecommunications and cloud service suppliers.[228]

---

[225] Tech Republic, *To Save Thousands on GDPR Compliance Some Companies Are Blocking All EU Users*, (May 7, 2018), *available at* https://www.techrepublic.com/article/to-save-thousands-on-gdpr-compliance-some-companies-are-blocking-all-eu-users/; Financial Times, *US Small Businesses Drop EU Customers Over New Data Rule*, (May 24, 2018), *available at* https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

[226] Dept't for Digital, Culture, Media & Sport, Guidance, *Using Personal Data in Your Business After the Transition Period*, (Oct. 16, 2020), *available at* https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period.

[227] Law on Intellectual Property (as amended, 2009), Arts. 25, 26.

[228] Industry reports that the draft currently under discussion includes a provision that would require all domestic companies to store their data in Vietnam, while foreign companies would only have to do so if they fail to cooperate adequately with law enforcement. If all domestic entities are required to localize data under this implementing decree, no hyper-scale cloud service providers will be able to sell to Vietnamese customers, as none of them currently have a local region. Conversely, if localization mandates are issued to foreign entities with no local presence, these foreign entities will incur significant additional overhead costs vis-à-vis their local entities.

In addition to localization requirements, there also are local representation requirements for services that meet designated criteria. Draft versions of the Implementing Decree issued by the Ministry of Public Security provide detailed requirements for covered services, including requirements to comply with data requests, content takedown, and domain name seizures.[229] If a company fails to comply with these requirements, Vietnamese authorities could serve it with a "data localization" notice. It may not be practical for firms to fulfill the data access and content takedown requirements if they lack visibility into the data stored on their platforms. As a general matter of policy, governments should not use localization mandates as a penalty for noncompliance.

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, but it would also 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

In July 2021, the Vietnamese government proposed amendments to the Ministry of Information and Communication Decree 72/2013. The proposal included numerous new restrictions, including requiring all foreign enterprises providing cross-border services with over 100,000 Vietnamese unique visitor access per month to store data locally, set up branches or representative offices in Vietnam, and enter into content cooperation agreements with Vietnamese press agencies when providing information cited from the Vietnamese press. The proposal also includes onerous and sweeping requirements for content removal, especially given the proposal's broad definitions of what constitutes "prohibited acts." For example, any act that the Vietnamese government considers to be "adversely affecting social ethics, social order and safety and the health of the community" would be in scope. In addition, the proposal would require digital platforms, including cross-border suppliers, to take down violating content within 24-hours.

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.[230]

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

[229] *Vietnam: Draft Decree on Personal Data Protection*, Baker McKenzie (Apr. 1, 2020), *available at* https://www.bakermckenzie.com/en/insight/publications/2020/04/draft-decree-on-personal-data-protection.

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

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.[231]

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.[232]

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

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

Cross-Border Provision Of Advertising Services

On August 19, 2020, the Ministry of Information and Communications (MIC) released a draft Decree to amend the Decree 181/2013 (on Elaboration of some Articles on the Law on Advertising).[233] The draft would regulate advertising content, and expand the scope of application to include Apps and social media. As drafted, the draft lacks clarity on definitions, procedures and restrictions, imposes onerous reporting requirements; and obliges suppliers to actively manage ad content and placement. Revisions are needed to remove clauses to avoid confusion and prevent overlapping liability and duplication.[234]

---

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

[232] *Circular Regulates OTT Services*, Vietnam News (Nov. 15, 2014), https://vietnamnews.vn/economy/262825/circular-regulates-ott-services.html#qvpySzIcYMz25vCl.http://vietnamnews.vn/economy/262825/circular-regulates-ott-services.html#qvpySzIcYMz25vCl.97%2097.

[233] *Draft Amendment to Decree No. 181/2013ND-CP: The Impact on Cross-Border Advertising Activities*, Lexology (Oct. 2, 2020), available at https://www.lexology.com/library/detail.aspx?g=31329819-83f3-4b8e-8554-87daf272bb1b.

[234] For example, take-down requests and tax obligations should only be regulated pursuant to Decree 72 and relevant tax laws.

Restrictions On Cloud Services

On June 3, 2020, Vietnam's Prime Minister signed Decision 749/QD-TTg, which announces the country's National Digital Transformation Strategy by 2025, and specifically calls for the introduction of technical and non-technical measures to control cross-border digital platforms.

The Ministry of Information and Communications (MIC) has subsequently issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, which set forward cloud technical standards and considerations for state agencies and smart cities projects in favor of local private cloud use. These decisions clearly intend to create a preferential framework for domestic CSPs, creating de facto market access barriers. Furthermore, the MIC Minister has made public statements noting that "as Vietnamese firms are getting stronger hold of physical networks, [Vietnam] must do the same for cloud computing and digitalization infrastructures." While these standards are technically "voluntary," in practice, this will be adopted by the Vietnamese public sector as if it is mandatory.

Unilateral Or Discriminatory Digital Tax Measures

As part of the government of Vietnam's plan to protect local businesses, the Tax Administration Law, effective 1 July 2020, taxes cross-border e-commerce and other digital services.[235] The Ministry of Finance issued Circular 80 [236] providing guidance on the law and its Decree 126 in September 2021. The Circular added a requirement for foreign digital service suppliers without a permanent establishment in Vietnam to register and pay tax in Vietnam. If the foreign suppliers elect not to register, their Vietnamese customers (or commercial banks in the case of business-to-consumer transactions) will be responsible for declaring and withholding the taxes from their payments to the foreign suppliers. While Circular 80 provides for the possibility for suppliers to apply for tax treaty exemptions or reductions (where applicable), it is unclear how they would claim treaty relief for such transactions. These onerous procedures coupled with the deemed tax rates (Corporate Income Tax and VAT) will further complicate tax obligations for cross-border service suppliers and conflict with international taxation rules.

Personal Data Protection Decree

The Vietnamese government is working on a Personal Data Protection Decree (PDP) that has raised concerns about data localization requirements. The current draft sets out conditions that a processor of personal data must fully satisfy with regard to the treatment of personal data of Vietnamese citizens, including "registration" of transfer of such overseas, that will impact cross-border data flows. A related draft Decree on Administrative Penalties for cybersecurity contains high penalties for violations of the PDP - up to 5 percent of the violator's revenue in Vietnam. The draft Decree also includes so-called "additional penalties" in the form of withdrawing licenses, information or video takedown, confiscation of evidence, equipment, public apologies and correction.

Decree 85 On E-commerce

On September 25, 2021, the government issued Decree 85 on E-commerce, broadening its scope to include cross-border platforms without a local presence in Vietnam (including websites in Vietnamese language or exceeding 100,000 transactions per year). The Decree requires local and cross-border e-commerce platforms to provide vendors' information to authorities upon request and take-down information on goods that violate Vietnamese laws within 24 hours. The Decree will come into effect from 1 January 2022.

---

[235] *Vietnam's Tax Administration Law Takes Effect*, R Global (Aug. 7, 2020), *available at* https://www.irglobal.com/article/vietnams-tax-administration-law-takes-effect-in-july-2020-0f67/.

[236] Circular 80/2021/TT-BTC guiding the Law on Tax Administration, Decree 126/2020 (Vietnamese), *available at* https://thuvienphapluat.vn/tintuc/vn/thoi-su-phap-luat/chinh-sach-moi/37945/thong-tu-80-2021-tt-btc-huong-dan-luat-quan-ly-thue-nd-126-2020.

Other Geographic Regions

East African Region

Copyright-Related Barriers

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

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

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

Latin America Regional

Burdensome Or Discriminatory Data Protection Regimes

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

Unilateral Or Discriminatory Digital Tax Measures

Numerous countries in the region have already implemented or are in the process of putting indirect taxes (VAT/GST) on cross-border supplies of electronically supplied services (ESS). However, in stark contrast to the dozens of other jurisdictions in the world, countries in Latin America are not leveraging global best practices or incorporating the key OECD principles of neutrality, efficiency, certainty, simplicity, effectiveness and fairness, and flexibility. Through a newly invented process, they are creating an unlevel playing field. Specifically, governments should utilize the "Non-resident Registration" Tax Collection Model, instead of attempting to implement the "Financial Intermediary" Tax Collection Model that was recently created by the Argentine government and is potentially being replicated in Colombia, Chile, Costa Rica, and other countries.

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