GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

January 28, 2021

Docket No. USTR-2020-0041 (85 Fed. Reg. 81,263)

Jake Ewerdt
Director for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Mr. Ewerdt,

The Global Data Alliance (GDA)[1] provides this submission in response to the request by the Office of the US Trade Representative (USTR) for comments on the 2021 Special 301 review under Section 182 of the Trade Act of 1974 (Special 301).[2]

GDA members rely on intellectual property (IP) – including copyrights and related rights, patents, trademarks, and trade secrets – and on the ability to transfer data across borders in many aspects of their international operations. However, GDA members increasingly face market access barriers in the form of unnecessary and discriminatory data localization mandates and data transfer restrictions that have a direct impact on their ability to acquire, protect, enforce, and enjoy the benefits of, IP rights. Between 1995 and 2015, such data-related trade barriers have increased by over 800%, and the rate of increase has further accelerated in recent years.[3]

Section 182 of the Trade Act of 1974, as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act of 1994 (19 USC § 2242), requires USTR to identify countries based on *inter alia,* policies that deny "fair and equitable market access to United States persons that rely upon intellectual property protection." In this submission, we focus on market access barriers that impact IP-intensive industries by mandating data localization or restricting legitimate data transfers.[4]

National policies on cross-border data transfers are – alongside standards of IP protection and enforcement – important determinants of the ability of economies to create, innovate, and generate new IP. They also are important measures of the openness and fairness of those markets to non-nationals who rely on IP in their commercial operations.

Innovation and market access-limiting data localization mandates and data transfer restrictions take many forms. Sometimes the policies expressly require data to stay in-country. Sometimes, these policies impose unreasonable conditions on sending data abroad or prohibit such transfers outright. In other cases, the policies require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors. Sometimes these measures cite privacy, security, or "indigenous innovation" as their underlying purpose, but not only do such measures often fail to advance these purposes, but they also create market access barriers. For example, these measures may:

- Reflect a choice of policy tools that are significantly more trade-restrictive than necessary to achieve the stated public policy goal;
- Constitute unnecessary, unjustified and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or
- Treat cross-border data transfers less favorably than domestic data transfers.

Sustained attention to these issues is critical, because in today's digitized economy, research and development (R&D), IP generation, and other creative and scientific endeavors are increasingly cross-border in nature.

For example, artificial intelligence (AI) involves the application of analytical techniques to data generated in various countries, transferred across borders, and consolidated into larger data sets. AI helped fast-track the COVID-19 vaccine, cutting timelines from years to months, as researchers analyzed drug discovery data transferred from around the world to quickly identify potential drug candidates.[5] Trade barriers that impede data transfers make such AI-based analysis much more difficult, if not impossible, as they prevent the consolidation of representative data sets necessary to conduct AI innovation. In this way, these trade barriers directly impede new innovations and creations that could advance human health and welfare.

Failing to attend to data-related trade barriers also threatens other IP priorities – from engaging in cross-border R&D, to protecting brands, to investigating IP infringement, to conducting comprehensive prior art searches. Likewise, with so many patented or copyrighted innovations functionally dependent upon satellite or other cross-border data communications (e.g., IoT software applications in the aerospace, automotive, and agricultural machinery sectors; music and video streaming services that disseminate licensed US film or music content), cross-border data transfer restrictions make it difficult, if not impossible, for innovators and creators to sell or provide support to their IP-protected products abroad – interfering with their ability to enjoy the benefits of their IP rights abroad. In each of the foregoing examples (and many others), innovation and market access-limiting data localization mandates and data transfer restrictions impact US IPR holders in respect of the availability, acquisition, scope, maintenance, enforcement, and enjoyment of IP rights.

The Global Data Alliance urges USTR to attend to the growing threat to US trade and IP priorities presented by unfair market access barriers in form of cross-border data transfer restrictions and data localization mandates. We look forward to your questions and comments.

Submission of Global Data Alliance for
Special 301 Annual Review

This submission responds to USTR's solicitation of information relevant to the Special 301 Annual Review, and contains the following major sections:

A. Cross-Border Data Transfers and Innovation in Today's Global Environment

The global outbreak of COVID-19 presents one of the most complex challenges governments have faced in modern times. Meeting this challenge has proven to be a highly complex endeavor, requiring globally coordinated inventive and creative solutions that are protected by IP rights. In addition to innovative activities necessary to COVID-19 response and recovery, many other economic activities in a socially distanced environment depend upon cross-border access to IP-intensive technology and software tools. As governments around the world continue to navigate and respond to the public health crisis, policymakers should maintain a strong commitment to policies that foster cross-data data-enabled innovation necessary to COVID-19 response and recovery.

An effective COVID-19 response and recovery requires innovation conducted on a transnational scale. The critical importance of cross-border data transfers for IP-intensive activity is evident in, for example, multinational teams of biopharmaceutical researchers engaged in vaccine development and multi-regional clinical trials, as well as IP-intensive manufacturing and distribution processes to produce and disseminate those treatments at scale to global populations. It is also evident in the context of software-enabled remote work, remote learning, and remote health applications that have helped provide resilience and operational continuity for the organizations upon which workforces, students, and patients depend. Another scenario involves cross-border access to copyrighted and patented software solutions that can help farmers make planting and harvesting decisions guided by insights from satellite and sensor-based weather forecasting and environmental analytics. Across every sector of the economy, and at every stage of the production value chain, cross-border data transfers and IP protections create the conditions to sustain economic activity – helping businesses and workers stay employed, reach new markets, and develop new products.[6]

Innovation necessary for COVID-19 response and recovery is underpinned by cross-border movements of know-how, information, and data in an environment supported by patent, trade secret, copyright, trademark, and regulatory data protections.[7] In this way, the dual confidence in the ability to protect IP across borders as well as the ability to transfer data across borders has come to play an increasingly important role in attenuating and overcoming the impacts of the pandemic.

B. Cross-Border Data Transfers and Innovation — Statistical Overview

Cross-border access to technology and seamless movement of information online are critical to overcoming today's economic challenges in the face of increasing restrictions on merchandise trade and the international movement of persons. Even before COVID-19, cross-border data transfers were estimated to contribute trillions of dollars to global GDP,[8] and 60 percent of global GDP was expected to be digitized by 2022, with growth in every industry driven by data flows and digital technology.[9] Furthermore, 75 percent of the value of data transfers reportedly accrued to traditional industries like agriculture, logistics, and manufacturing. [10]
Since March 2020, the importance of data transfers has only grown. For example, before COVID-19, an estimated 5%–15% of US employees worked remotely. As of mid-2020, roughly 50% of US employees, or more, are working remotely, with many relying on cross-border access to cloud-based remote work software solutions.[11] Similarly, remote health technology solutions, often accessed across national borders via the cloud, have become indispensable to protecting populations and economies in the COVID-19 era. Expected to grow by 700% by 2025, some regions are seeing even more rapid growth – up to 40-fold – for non-urgent telemedicine visits.[12]

C. Cross-Border Data Transfers and the Innovation Lifecycle

Cross border data transfers are critical at every stage of the innovation life cycle, and in all facets of IP legal frameworks. This includes: (1) early stages of innovative and creative processes, including basic R&D, initial conception, and design; (2) the acquisition and maintenance of IP rights; (3) the enforcement of IP rights and brand protection activities; and (4) the ongoing enjoyment and commercialization of those IP rights.

1. Data Transfers and Core Innovation

In every sector, cross border data transfers play an integral role in basic research and development (R&D), and other core innovative and creative functions. For example, in semiconductor design as well as biopharmaceutical research, basic R&D depends upon access to globally sourced research materials from laboratories and research institutions from across the world, as well as collaboration, joint research, and the exchange of ideas and knowledge among teams of inventors, designers, authors, and other creators and innovators in different countries.

Trade barriers that impede data transfers undermine basic research and scientific activity, as well as the development of new treatments and inventions to protect human health and welfare.

This collaborative, multinational approach to technological and creative endeavor integrates and binds together the international IP legal framework as well as scientific and artistic communities. R&D teams across universities, commercial labs, and enterprises in different countries collaborate across borders to develop new products, cures, and other advances protected by patents, trade secrets, copyrights and trademarks. Typically, such R&D also often requires the use of copyrighted software solutions and research data accessible across cloud-enabled and networked environments, as well as the application of artificial intelligence (AI)-based analytical techniques to data transferred across borders and consolidated into larger data sets.[13]

As explained by the World Intellectual Property Organization (WIPO),[14] the US Patent & Trademark Office (USPTO),[15] and other IP authorities,[16] such R&D depends upon the application of AI-related tools to globally sourced data sets. Data sets consolidated across IT networks and borders can be analyzed (e.g., through machine learning or data analytical techniques) to identify to meaningful insights, patterns, and connections that can aid R&D teams in the discovery and development of novel solutions to scientific and technical challenges.

2. IP Acquisition, Registration, and Maintenance

The ability to transfer data across borders is also critical to the acquisition of IP rights. Applicants must be able to transfer information across borders in order to apply for patent, copyright, trademark or other rights in a coordinated manner with IP office authorities in different countries. Access to data from multiple countries – such as prior art references – is also an integral part of the patent application examination process. They must also be able to transfer data across borders in order to avail themselves of WIPO-administered international registration and examination frameworks for IP rights, such as the Patent Cooperation Treaty, the Madrid Registry for trademarks, or the Hague System for the International Registration of Industrial Designs.

Data localization mandates and data transfer restrictions that prohibit the transfer of “important,” “critical,” or “sensitive” data (e.g., under Chinese measures discussed below) create uncertainty regarding the future ability to transfer information and data necessary to these procedures for the acquisition, registration, and maintenance of IP rights.

3. IP Enforcement and Brand Protection

In today's global marketplace, IP infringement is increasingly complex and globalized, requiring sophisticated investigatory tools. No IP enforcement program can be effective without the ability to trace – on a cross-border basis – counterfeiting, commercial scale piracy, and other illicit activities with insights and information derived from foreign source countries, distribution hubs and networks, and end-user markets. Data localization measures and unnecessary data transfer restrictions directly interfere with the ability to investigate and counteract transnational IP infringing activities.

Cross-border data transfers are critical to many aspects of IP enforcement - from monitoring marketplaces, to gathering evidence of infringement in multiple locations, to researching details of illicit networks, to using administrative or judicial tools in multiple jurisdictions to preserve evidence and secure recourse. The ability to track and trace infringing activities across IT networks and borders is particularly important as many infringing acts involve an online element, whether via the offer and sale of infringing articles online; the cross-border

exfiltration of source code, trade secrets or other proprietary data; the circumvention of technological protection measures; or the unauthorized and unlicensed use of copyrighted software or trademarks in an online environment.

> *Cross border access to information is frequently necessary for IP infringement investigations (e.g., obscuring patterns and trends in counterfeiting and piracy and making it more difficult for investigators to obtain forensic data to identify criminal enterprises engaged in counterfeiting, piracy, and other IP infringement)*

4. IP Commercialization

Cross-border data transfers are also critical to the ability of enterprises to commercialize and enjoy the benefits of their IP rights. When a country mandates data localization or restricts data transfers, it can easily frustrate the ability to enjoy the benefits of any IP right granted. With so many patented or copyrighted innovations functionally dependent upon satellite or other cross-border data communications (e.g., IoT software applications in the aerospace, automotive, and agricultural machinery sectors; music and video streaming services that disseminate licensed film or music content), cross-border data transfer restrictions make it difficult, if not impossible, for innovators and creators to sell or provide support to their IP-protected products or in foreign markets – interfering with their ability to secure a commercial return on, or otherwise enjoy the benefits of, their IP rights abroad.

D. Data-Related Market Access Barriers that Impact Innovation and IP

In this submission, we focus on the second element of Section 182 of the Trade Act, highlighting cases in which trading partners that have erected **unfair market access barriers** that affect GDA members who rely on IP in their commercial operations.[17] GDA's Special 301 submission notes policies of concern in the following markets: Brazil, China, India, Indonesia, South Korea, Thailand, Vietnam, and the European Union (EU). We also refer USTR for additional details to GDA's NTE submission for country-specific discussions for innovation and IP-related concerns in each of these markets. GDA does not provide specific country listing recommendations (as between Priority Watch List or Watch List) for these countries, but requests that USTR include the information submitted in its qualitative overall review of the referenced countries.

1. Brazil

The entry into force in September 2020 of the Brazilian Personal Data Protection Bill (known in Brazil as LGPD) engendered legal uncertainty for companies that need to transfer data from Brazil to other countries. The LGDP imposes obligations regarding international data transfers that are dependent on implementing regulations that are still pending. In September 2020, the Global Data Alliance sent the Brazilian government a letter requesting that, until data transfer regulations are in place, guidance be issued confirming that companies may continue to responsibly transfer data internationally based on global best practices that are consistent with the overall LGPD objectives.[18] To date, this guidance has not been issued. We encourage the US Government to continue engaging with Brazil in this important issue.

2. China

China's data localization requirements and data transfer restrictions create significant market uncertainty for foreign persons who rely on IP rights in exporting their products and services to China, and in their commercial operations in China. Since 2017, the Government of China has issued numerous policies and standards having a direct and restrictive impact on the ability to transfer data across borders, both into and out of China. Some of these measures were designed to implement the Cybersecurity Law (CSL or the Law), which became effective in that same year,[19] and some also focus heavily on concepts of indigenous innovation and preferences for domestically-generated IP and technology.

The Global Data Alliance supports continued efforts to improve bilateral and regional economic dialogue, including through APEC, aimed at developing workable and constructive solutions on these cross-border data policy matters that have direct impacts on the interests of US persons who rely on IP. Because so much inventive and creative IP-related activity implicates the ability to transfer data across borders, China's numerous data localization mandates and transfer restrictions create significant legal uncertainty for both GDA member companies and their business partners in China. Measures of concern are listed below.

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[20] The CSL contains significant restrictions on the ability to transfer data out of China.[21] The Cyberspace Administration of China (CAC) and other authorities continue to issue measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of critical information infrastructure (CII) or "important information"), or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry (e.g., requiring that all personal information and important information collected in China, and not just by CII operators, must be held in-country). Because the CSL and subsidiary measures appear to authorize Chinese authorities to prevent US innovators and IP holders from transferring their own propriety information (including trade secrets), if deemed to be "important" or "critical," these measures create significant uncertainty for innovative and creative activity in China.

Cybersecurity Classified Protection Scheme: In May 2020, China posted the final version of the Cybersecurity Classified Protection Scheme (CCPS),[22] a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL. The September 22, 2020 "*Guiding Opinions on Implementing CCPS and CII Protection Scheme*"[23] includes specific data localization mandates and data transfer restrictions, requiring that, "[p]ersonal information and important data collected and generated by the operators throughout their operation in China shall be stored in China, and where cross-border transfer is required for business reasons, such transfer shall follow relevant rules and undergo a security assessment.

***Data Security Law*:** In July 2020, China released the draft *Data Security Law of the People's Republic of China*.[24] The draft law is extremely broad and undefined. It also remains unclear how the law would interact with existing legal frameworks. The law would apply to "any entity that carries out data activities" and contains ambiguous language regarding the ability to transfer data across borders.[25]

Personal Information Protection Law: On October 21, 2020, the National People's Congress released the first draft of the Personal Information Protection Law (**Law**). The Law appears to include stricter localization requirements and data transfer restrictions than the Cybersecurity Law of China, including through: (1) local data storage requirements; (2) residency requirements; and (3) mandatory security assessments, required for personal operators of Critical Information Infrastructure (CII) and those whose information processing exceeds CAC-specified volumes.

3. European Union

Over the past five years, the European Union has modernized its digital economy regulatory and policy framework, with the Commission rolling out an assertive digital policy agenda guided by a focus on "digital sovereignty." This concept is defined in various ways and with varying degrees of restrictiveness across the Commission and Member States. The European Strategy for Data adopted in February 2020 clearly endorses that the EU will maintain an open, but assertive approach to international data flows and pledges that the EU will continue to address unjustified obstacles and restrictions to data flows in bilateral discussions and international fora. There are some calls for data localization in Europe especially in the wake of the CJEU *Schrems II* decision, such as Council declarations on the need to create an EU Cloud Federation, contributing to the emergence of projects such as GAIA-X.

Global Data Alliance members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, and in harnessing the value of data to the benefit of European citizens and the European economy. However, some of the measures under consideration may constitute *de facto* market

access barriers, including in the areas of data privacy, cybersecurity, data governance, artificial intelligence, and cloud resilience in the financial sector (the so-called the 'Digital Operational Resilience Act' (DORA)), and as such make it more difficult to innovate and create in Europe with full confidence that it will be possible to commercialize and integrate the resulting inventions, products, or services within a company's larger global product or service ecosystem.

As the incoming European Commission develops and implements new policy proposals, the Global Data Alliance asks that trade authorities from the United States and the EU work intensively to ensure the continuity of transatlantic data transfer mechanisms, and refrain from adopting policies that impede cross-border data transfers.

Cross-Border Data Flows: Measures that impede the flow of data across borders impose substantial burdens on companies with international operations. In the transatlantic context, some commentators have observed an unleveled playing field where data transfers to certain countries, in many cases close economic and political allies of the EU, are scrutinized or restricted, yet no similar scrutiny or restrictions are imposed on countries where data privacy, cybersecurity, and other data collection practices are much more opaque.

On July 16, the European Court of Justice ruled in the Schrems II case on the validity of Standard Contractual Clauses (SCCs). SCCs are one of the main mechanisms under EU law to legally transfer personal data from the EU to third countries, especially in the absence of an adequacy decision.

The Court decision found that:

- The use of SCCs for the transfer of personal data to recipients established in third countries is valid;
- However, controllers and processors are required to verify, on a case-by-case basis, whether the law of the third country where the recipient is based ensures an "essentially equivalent" level of protection of the personal data transferred. This assessment must take into consideration both (1) the contractual clauses / additional safeguards agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned, and (2) any laws of that country that make the recipient unable to ensure an essentially equivalent level of protection, including as regards any access by the public authorities of that third country to the personal data transferred;
- The EU-US Privacy Shield is annulled and can no longer be used for transfers to the US.

The Court decided that unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to SCCs, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country, including due to possible public authorities' access to that data.

This case and subsequent guidance from the European Data Protection Board has significant bearing on companies that operate in Europe and / or act as service providers for customers in Europe. This situation also adds uncertainty with regards to the robustness and durability of the SCCs, a mechanism used by 90 percent of companies that transfer data internationally to some 180 countries. Broadly speaking, this situation also creates major challenges for EU- and foreign-based entities that have integrated transnational innovation, engineering, publishing and other creative operations. There remains significant uncertainty for both EU- and foreign-based entities that have integrated transnational operations focused on cross-border R&D, creative content (music, film, written materials, software, etc.), and other IP-protected data. studios.

Data Flows in Trade Agreements with Third Countries: In February 2018, the European Commission released data transfers provisions for trade agreements, seeking to address concerns from Member States, trading partners, and industry that EU Free Trade Agreements ("FTAs") lacked trade negotiating proposals on cross-border data transfers. This position was a positive step towards the EU endorsing binding trade commitments specifically focused on cross-border data transfers. However, it raised concerns due to its self-declaratory nature and potentially unlimited scope of exceptions with regards to privacy safeguards. To date, the European Commission has reportedly tabled this negotiating proposal in ongoing FTA negotiations with the UK, Australia, and New Zealand. The EU also tabled this negotiating proposal at the WTO Joint Statement Initiative talks on e-commerce.

In January 2020, a quorum of 17 Member States called for the Commission to adopt a high-level of ambition on data flows in the WTO e-commerce negotiations, even if it means diverging from the EU position as formally set by the negotiating directives. By adopting forward-looking data flows provisions, the EU would be able to retain its influence on the multilateral stage and to continue to effectively push back against localization efforts in third countries. It would also bring it closer to its main trading partners—first and foremost the United States—and address some of the friction between trade and privacy following the CJEU Schrems II case.

4. India

From an IP and innovation policy perspective, the operating environment remains challenging in India,[26] in part due to an increase in restrictive cross-border data policies. Several government authorities, including the Ministry of Electronics and Information Technology (MeitY), the Reserve Bank of India (RBI), the Department for Promotion of Industry and Internal Trade (DPIIT), and the Department of Telecommunications (DOT), have advanced policies and proposals impacting cross-border data policy matters. These requirements are included in various policies ranging from legacy regulations on government-owned weather data,[27] to proposed regulations on personal data protection, regulations on machine-to-machine (M2M) systems,[28] and payment processing regulations.[29] These policies undermine the ability of India and Indian companies to integrate innovative and creative activity with firms in other countries, weakening India's engagement with the world. We discuss several relevant measures below.

Personal Data Protection Bill: The Personal Data Protection Bill, 2019[30] (PDP 2019) was introduced to the Indian Parliament in December 2019 and, although changes have been made to the previous version of the bill, a number of serious concerns remain. These concerns include requirements to localize critical data in India; requirements to maintain copies of sensitive data in India; and a lack of clarity regarding the definition and scope of critical or sensitive data, among other issues.

National E-Commerce Policy: In February 2019, DPIIT released a Draft National E-Commerce Policy, which contains several proposals that restrict Indian customers' access to the most seamless and secure digital services. The draft policy included data localization requirements and restrictions on data flows. While it was later withdrawn given significant concerns from the industry, a revised policy may be released in 2021.

Non-Personal Data Governance Framework*:* On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data (NPD Framework), resulting in the issuance of a report in August 2020. The Global Data Alliance highlighted in its written comments concerns regarding the Framework's restrictions on cross-border data flows and local storage requirements. The framework would impose other compliance obligations for businesses by creating a new regulator in addition to the proposed Data Protection Authority (DPA) under PDP 2019 and the proposed e-commerce regulator. A revised report was issued in January 2021, but the concerning provisions impacting data flows have not been modified.

Directive on Storage of Payment System Data: In April 2018, the RBI issued the Directive on Storage of Payment System Data (Directive)[31], requiring payments firms to store data solely in India and ensure that any data processed abroad be deleted within 24 hours. (Directive), imposing data and infrastructure localization requirements that required payment system operators to "ensure that the entire data relating to payment systems operated by them (system providers) are stored in a system only in India."[32] "Data" is defined broadly, and the Directive is likely to affect both payment processors and their service providers.[33] The RBI directive imposed short deadlines and has required significant capital investments for companies to comply. In a recent development, the RBI, in a submission to the Personal Data Protection (PDP) Parliamentary committee, requested that financial data not be classified as Sensitive Personal Data and that RBI be exempted from the PDP bill – a move that could result in more sector-specific data regulation by RBI.

Cloud Computing: In 2019, MeitY established the Working Group on Cloud Computing (Working Group). The Working Group is tasked with formulating a framework for promoting and enabling cloud services in India. It is also tasked with examining the cybersecurity and privacy aspects related to cloud computing.[34] Unfortunately, reports indicate that the Working Group may propose broad data localization requirements for CSPs providing

services both to the public and private sectors in its recommendations to MeitY.[35] The recommendations have still not been published by MeitY.

5. Indonesia

The IP and innovation policy environment in Indonesia is challenging for Global Data Alliance member companies,[36] as Indonesia has developed or is developing policies that make it increasingly difficult to access the Indonesian market with digitally-enabled products and services.

E-Commerce Regulation: In November 2019, the Government of Indonesia issued GR80, a new e-commerce regulation. This regulation reportedly contains various concerning provisions relating to physical presence and registration. Of particular concern are provisions in GR 80 that reportedly stipulate that personal data cannot be transferred offshore, unless the receiving nation is deemed by the Ministry of Trade as having the same level of personal data standards and protection as Indonesia. This requirement is overly restrictive, as it does not appear to account for other internationally recognized transfer mechanisms, including transfer pursuant to APEC CBPR, or according to standard contractual clauses, binding corporate rules, certifications, marks, or other approaches. The measure should be amended to eliminate such provisions, or at least align with those of the draft PDP Bill.

6. Republic of Korea

From the perspective of data transfer and localization rules, the IP and innovation policy environment in the Republic of Korea (Korea) is concerning.[37] Korea has a strong IT market and a mature legal system. Although the Cloud Computing Promotion Act[38] came into force on September 28, 2015, data residency, physical network separation, and other restrictive data-related requirements for industry sectors, such as government/public services, finance, healthcare, and education, hamper cross-border data transfers in these sectors.

Cloud Security Assurance Program: The Korea Internet Security Agency (KISA) imposes onerous certification requirements under the Cloud Security Assurance Program (CSAP) on CSPs that provide cloud services to public sector agencies. On July 23, 2019 the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) announced revisions to the CSAP.[39] The program requires that "the physical location of the cloud system and data shall be restricted to in country and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions." The expansion of this program to cover a widening range of, even private sector, institutions is of significant concern.

Regulation on Supervision of Electronic Financial Transactions: The Regulation on Supervision of Electronic Financial Transactions (RSEFT)[40] was amended on October 5, 2016 to permit the use of cloud services by financial services institutions (FSIs). The amendment allows certain data to be stored on public cloud services. The Financial Services Commission (FSC) recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, FSC specifically requires that such data be maintained on servers located in Korea.[41]

Personal Information Protection Regime: Korea's personal information protection (PIP) regime is one of the most restrictive in the region. In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[42] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[43] and the Credit Information and Protection Act.[44] The primary result of the legislative package is to consolidate the legal protection and enforcement provisions for personal information primarily in the PIPA, and to elevate the Personal Information Protection Commission (PIPC) to a central government-level agency under the Prime Minister. These developments may aid Korea's efforts to negotiate an "adequacy" recognition from the European Commission, but questions remain regarding the impact on cross-border data transfers.

7. Vietnam

Over the past several years, Vietnam has enacted, implemented, and proposed various measures that raise concerns from a cross-border data policy perspective. The enactment of the Cybersecurity Law in June 2018, and current efforts to develop implementing rules, exacerbate existing challenges and threaten to undermine the ability of foreign companies to operate in, or do business, with Vietnam.[45]

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law, which went into effect on January 1, 2019, raises several concerns from a cross-border data policy perspective. The Government of Vietnam had indicated its intention to issue regulations implementing the Law by the end of 2019, but the implementing regulations are still pending. The latest draft of the implementing regulations was not released for public consultation and reportedly continue to contain problematic data localization requirements. Although the draft Decree allegedly did not require foreign entities to store data in Vietnam, the draft gave the government the power to impose data localization and local presence requirements on foreign entities should a company fail to comply with a request under the Law from the Ministry of Public Security (MPS). It remains particularly concerning as these requirements can be applied irrespective of whether illegality is established or a company has control over the data being used in violation, therefore posing a risk for Article 26 being triggered arbitrarily.

The draft also allegedly included a requirement for all local entities to store data locally. This is a concerning requirement that effectively enforces localization on foreign entities as a condition of doing business with local entities. These localization requirements remain a concern to industry at large.

8. Other Countries

GDA members face (proposed or implemented) data localization requirements and data transfer restrictions, or similar measures, that impact IP and innovation in other markets, including the Kingdom of Saudi Arabia,[46] Pakistan,[47] United Arab Emirates,[48] and Mexico.[49]

E. Conclusion

The Global Data Alliance welcomes the opportunity to provide this submission and looks forward to working with USTR to achieve meaningful progress in addressing the cross-border data policy concerns identified in this submission.

---

[1] The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members include BSA members and American Express, Amgen, AT&T, Citi, ITB360, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, RELX, Roche, UDS, United Airlines, Verizon, Visa, and WD-40 Company. These companies are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance. *See* Global Data Alliance, *About the Global Data Alliance* (2020), at: https://www.globaldataalliance.org/downloads/aboutgda.pdf

[2] www.govinfo.gov/content/pkg/FR-2020-12-15/pdf/2020-27515.pdf

[3] https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf

[4] We do not address the first statutory element under section 182 of the Trade Act of 1974 relating to the adequacy and effectiveness of IP protections because the GDA is organizationally focused on issues relating directly to cross-border data policies. However, GDA members own extensive portfolios of trademarks, copyrights, patents, trade secrets, and other IP rights, and rely on other trade associations to represent their specific perspectives on substantive matters of IP protection and enforcement.

[5] *See e.g.,* Ganes Kesari, *Why Covid Will Make AI Go Mainstream In 2021*, Forbes (Dec. 2020), https://www.forbes.com/sites/ganeskesari/2020/12/21/why-covid-will-make-ai-go-mainstream-in-2021-top-3-trends-for-enterprises/?sh=1d83a3f6797a; Arshadi et al., *Artificial Intelligence for COVID-19 Drug Discovery and Vaccine Development*, Front. Artif. Intell. (Aug. 2020), https://www.frontiersin.org/articles/10.3389/frai.2020.00065/full ; Ungaro, et al., *Accelerating vaccine research for COVID-*

19 with high-performance computing and artificial intelligence, HP Enterprise (2020), https://www.hpe.com/us/en/newsroom/blog-post/2020/04/accelerating-vaccine-research-for-covid-19-with-high-performance-computing-and-artificial-intelligence.html; IEEE, *Can AI and Automation Deliver a COVID-19 Antiviral While It Still Matters?* IEEE Spectrum (2020), https://spectrum.ieee.org/artificial-intelligence/medical-ai/can-ai-and-automation-deliver-a-covid19-antiviral-while-it-still-matters

[6] *See* Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), at https://www.globaldataalliance.org/downloads/GDAeverysector.pdf ; See Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), at https://www.globaldataalliance.org/downloads/infographicgda.pdf

[7] It is critical to have not only an ability to protect such proprietary knowledge through IP, but also the ability to transfer across borders that knowledge and associated digital products and services. These two elements are mutually reinforcing: On the one hand, IP protections alone are of little value without the ability to transfer data across borders for purposes of R&D and commercialization. On the other, the ability to transfer data (e.g., for cross-border R&D purposes) is insufficient without the concomitant security afforded by IP protections.

[8] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.

[9] *Ibid.*

[10] *Ibid.*

[11] *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (Oct. 2020), https://globaldataalliance.org/downloads/10052020cbdtremotework.pdf

[12] *See* Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (Sept. 2020) https://globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf

[13] *See* Joshua Meltzer, *The impact of artificial intelligence on international trade*, Brookings Institution (2018), at: https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/

[14] *See e.g.,* WIPO, *WIPO Technology Trends 2019, Artificial Intelligence* (2019), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf; WIPO, *Frequently Asked Questions: AI and IP Policy (2021)*, https://www.wipo.int/about-ip/en/artificial_intelligence/faq.html; WIPO, *Artificial Intelligence and Intellectual Property Policy* (2020), https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html

[15] USPTO, *Artificial Intelligence Webpage* (2021), https://www.uspto.gov/initiatives/artificial-intelligence; USPTO, *Public Views on Artificial Intelligence and Intellectual Property Policy* (2020), https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf; USPTO, *Inventing AI - Tracing the Diffusion of Artificial Intelligence with US Patents* (Oct. 2020), https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf.

[16] *See e.g.,* Canadian Intellectual Property Office, *Processing Artificial Intelligence: Highlighting the Canadian Patent Landscape* (2020), https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/vwapj/AI_Report_ENG.pdf/$FILE/AI_Report_ENG.pdf; Japan Patent Office, *Recent Trends in AI-Related Inventions* (2019), https://www.jpo.go.jp/e/system/patent/gaiyo/ai/document/ai_shutsugan_chosa/report-2019.pdf; IP Australia, *Machine Learning Innovation – A Patent Analytics Report* (2019), https://www.ipaustralia.gov.au/sites/default/files/reports_publications/patent_analytics_report_on_machine_learning_innovation.pdf; UKIPO, Artificial Intelligence - A worldwide overview of AI patents and patenting by the UK AI sector (2019), at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf ; European Patent Office, *Patents and the Fourth Industrial Revolution* (2017), documents.epo.org/projects/babylon/eponet.nsf/0/17FDB5538E87B4B9C12581EF0045762F/%24File/fourth_industrial_revolution_2017__en.pdf.

[17] We do not address the first element relating to the adequacy and effectiveness of IP protections because the GDA is organizationally focused on issues relating directly to cross-border data policies. GDA members own extensive portfolios of trademarks, copyrights, patents, trade secrets, and other IP rights, and rely on other trade associations to represent their specific perspectives on substantive matters of IP protection and enforcement.

[18] Global Data Alliance, *Letter to Government of Brazil re LGPD Implementation and International Data Transfers* (Sept. 9, 2020), at https://www.bsa.org/files/policy-filings/09092020bsagdalgpdimplement.pdf

[19] *Cybersecurity Law of the People's Republic of China*, November 11, 2016 (CSL) (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[20] CSL, *op.cit.*

[21] Article 37 of the 2017 Cybersecurity Law (CSL) provides that "[c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland

China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment…". https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[22] *Cybersecurity Classified Protection Regulations (Draft for Comment)*, June 27, 2018 (CCPS) (Chinese), at: http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html?from=timeline&isappinstalled=0

[23] *Guiding Opinions on Implementing CCPS and CII Protection Scheme,* September 2020 (English) at: https://www.mps.gov.cn/n6557558/c7369310/content.html. The Guiding Opinions state in Section IV entitled "Strengthen the protection of important data and personal information", that "[o]perators shall establish and implement a security protection system for important data and personal information, make a backup of important networks and databases in critical information infrastructure for disaster recovery, adopt critical technical measures including identity authentication, access control, crypto protection, security audit, security isolation and trusted verification, to effectively protect the security of important data throughout its life cycle. Personal information and important data collected and generated by the operators throughout their operation in China shall be stored in China, and where cross-border transfer is required for business reasons, such transfer shall follow relevant rules and undergo a security assessment."

[24] *Data Security Law of the People's Republic of China (Draft for Comment),* July 2020, Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/

[25] The penalties outlined in the Law are of concern in part because of the ambiguity of the Law's provisions relating to cross-border data transfers. For example, Article 10 of the Law provides that the government shall "advance the safe and free cross-border flow of data," while Article 5 provides that the government shall "ensure the law-based, orderly, and free flow of data." The Law provides does not define what "law-based," "safe," and "orderly" mean; what specific legal requirements or restrictions apply to data transfers; what legal penalties apply to any breaches of those requirements; or what transparency and procedural fairness safeguards exist for regulated persons. Additionally, Article 33 of the Law imposes certain obligations in cases in a foreign law enforcement authority seeks access to data stored in China, and Article 31 requires entities engaged in "online data processing [to]… obtain a business operation permit or go through filing procedures," but provides few, if any, details on the substantive or procedural elements of these requirements. Article 33 of the Data Security Law provides that, "Where an overseas law enforcement agency asks for the data stored within the territory of the People's Republic of China, the relevant organization or individual shall report to the relevant competent department and obtain approval before providing it. Where the request for domestic data by a foreign law enforcement agency is prescribed in an international treaty or agreement concluded or joined by the People's Republic of China, such provisions shall apply."

[26] *See generally*, BSA Cloud Scorecard – 2018 India Country Report, at: https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

[27] *See Guidelines for Government Departments On Contractual Terms Related to Cloud Services,* (Section 2.1.d) at: http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms_0.pdf

[28] *National Telecom M2M Roadmap (2015),* at: http://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[29] *Reserve Bank of India Storage of Payment System Data Directive (2018),* at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0

[30] India *Personal Data Protection Bill (2019) at:* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[31] Storage of Payment System Data Directive, *op. cit.*

[32] Storage of Payment System Data Directive, *op. cit.*

[33] Storage of Payment System Data Directive, *op. cit.*

[34] Data Security Council of India Annual Report 2017-2018 at https://www.dsci.in/sites/default/files/documents/resource_centre/Annual-Report-2017-18.pdf

[35] Kris Gopalakrishnan-headed panel seeks localization of cloud storage data in possible blow to Amazon, Microsoft at: https://tech.economictimes.indiatimes.com/news/corporate/kris-gopalakrishnan-headed-panel-seeks-localisation-of-cloud-storage-data-in-possible-blow-to-amazon-microsoft/65278052

[36] *See generally*, BSA Cloud Scorecard – 2018 Indonesia Country Report, at: https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Indonesia.pdf

[37] *See generally*, BSA Cloud Scorecard – 2018 Korea Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Korea.pdf

[38] *Act on the Development of Cloud Computing and Protection of its Users (Cloud Computing Promotion Act)* (2015). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#liBgcolor1

[39] As announced at: https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939

[40] *Regulation on Supervision of Electronic Financial Activities (RSEFT).* http://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B0%90%EB%8F%85%EA%B7%9C%EC%A0%95

[41] E.g., under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.

[42] *Personal Information Protection Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

[43] *Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act)* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

[44] *Credit Information and Protection Act* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

[45] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) at: https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/

[46] The Kingdom of Saudi Arabia has steadily introduced a number of regulatory frameworks which contain strict data localization requirements.

- **Cloud Computing Regulatory Framework**. In March 2018, the Communications and Information Technology Commission (CITC) published the Cloud Computing Regulatory Framework. While the original Framework did not contain a localization requirement, the Framework was updated in March 2019 and now requires cloud customers to ensure that no customer data that is generated or collected by private sector regulated industries is transferred outside the Kingdom. The prohibition extends to any permanent or temporary transfer or storage (e.g. for caching, or redundancy/backup) unless it is expressly allowed under law. *See* https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf
- **IoT Regulatory Framework.** In September 2019, and following on from the Cloud Computing Regulatory Framework, the Communications and Information Technology Commission (CITC) published the IoT Regulatory Framework which regulates the use of IoT services in the Kingdom. This Framework requires all IoT service providers to host all servers used in providing IoT services, and all data inside the Kingdom. *See* https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf
- **National Data Governance Interim Regulations.** On October 20, 2020, the Saudi Data and Artificial Intelligence Authority published the National Data Governance Interim Regulations. The Regulations require the storage and processing of personal data "in order to ensure preservation of the digital national sovereignty over such data". Personal data can only be transferred or processed outside of the Kingdom if organizations obtain the approval of the relevant regulatory authority and the National Data Management Office. These Regulations are concerning given its broad application to all companies which handle personal data and represents a step towards horizontal imposition of data localization requirements in the Kingdom.

[47] In February 2020, Pakistan published a draft Data Protection Bill which included data localization requirements. Specifically, critical personal data (to be defined by the Personal Data Protection Authority) can only be processed in Pakistan and cannot be transferred out of Pakistan. Further, the Authority has the power to impose data mirroring requirements which would require a copy of the data to be stored in Pakistan. https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pdf

[48] In October 2020, the Central Bank of the United Arab Emirates published its Draft Retail Payment Services Regulations which requires all personal and payment data to be stored and maintained within the UAE.

[49] One measure of concern is a proposal that of the National Commission of Regulatory Improvement (CONAMER), the Ministry of Economy, the Central Bank of Mexico, and the National Banking and Securities Commission (CNBV) to require Electronic Payment Funds (IFPE) to: (1) demonstrate capacity to perform cloud computing services "in the national territory" of Mexico; (2) use cloud service providers headquartered in multiple different jurisdictions; or (3) receive official approval for another means of bolstering operational network continuity. *See Global Data Alliance* comments on this proposal at: https://www.globaldataalliance.org/downloads/es11232020mxpresentationgda.pdf Separately, other GDA members have raised particular concerns about September 2019 proposed amendments to the Federal Telecommunications Law that aim to impose a 30 percent national content quota for OTT services.