



January 31, 2022

Docket No. USTR-2021-0021 (86 Fed. Reg. 70,855)

Jacob Ewerdt
Director for Innovation and Intellectual Property
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508
Attn: Special301@ustr.eop.gov

Dear Mr. Ewerdt,

BSA | The Software Alliance¹ provides the following information in response to the notice published by the Office of the US Trade Representative (USTR) seeking comments on the 2022 Special 301 review under Section 182 of the Trade Act of 1974 (Special 301).²

BSA members rely heavily on access to US trading partners' markets and the adequate and effective protection and enforcement of patents, copyrights, and trade secrets within the context of intellectual property (IP) legal frameworks abroad. BSA members also depend upon cross-border data transfers and work across transnational IT networks to invest in research and development (R&D) at home, acquire and enforce IP rights, and to realize a return on those investments in R&D and IP. Inadequate IP protection and enforcement abroad are a challenge, as are market access barriers that unreasonably restrict BSA members from engaging in R&D or protecting, enforcing, or enjoying their IP across borders. BSA members also face significant challenges due to the availability and extensive use of unlicensed software products, especially unlicensed use of software products or services by governments, state-owned enterprises (SOEs), and business entities.

Many creative, technological, and scientific endeavors in today's digitized economy are cross-border in nature. Focused attention is required not only on standards of IP protection and enforcement abroad, but also on the market access barriers that impact US persons who rely on IP. 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, and researchers analyzed drug discovery data transferred from around the world to quickly identify potential candidates.³ Market access barriers that impede data transfers make such AI-based analysis much more difficult 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.

Data-related market access barriers also threaten 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 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), the cross-border data transfer restrictions that US trading partners impose can make it difficult, if not impossible, for US innovators and creators to sell or provide support to their IP-protected products or in foreign markets — interfering with their ability to enjoy the benefits of their IP rights abroad. In each of the foregoing examples (and many others), data-related barriers to innovation and trade harm US IP rightsholders in respect of the availability, acquisition, scope, maintenance and enforcement, and enjoyment of IP rights.

Maintaining US technology leadership is a critical goal. However, it will not be possible to meet that goal without sustained attention to the growing threat that data-related barriers to innovation and trade pose to the United States and to US persons who rely on IP.

BSA supports USTR's continued efforts to attend to the growing threat to US trade and IP priorities presented by inadequate IP protection and enforcement abroad, as well as unfair market access barriers that harm US persons who rely on IP. Nevertheless, USTR has missed the opportunity in recent years to use the Special 301 process as a tool to call attention to, and address the IP and innovation-related aspects of, "data nationalism," particularly as it manifests itself in cross-border data policies aimed at benefiting local champions at the expense of US IP rights holders. We urge USTR to take the opportunity in the 2022 Special 301 review cycle to address this growing global challenge. We look forward to your questions and comments.

BSA’s 2022 Special 301 Submission contains the following major sections:

A.	Introduction.....	4
B.	Software, Innovation, and Intellectual Property — Statistical Overview	4
C.	Data-Related Market Access Barriers and the Innovation Lifecycle.....	5
1.	Barriers to Core Innovation and R&D	5
2.	Barriers to IP Acquisition, Registration, and Maintenance.....	6
3.	Barriers to IP Enforcement and Brand Protection.....	6
4.	Barriers to IP Commercialization.....	6
D.	Special 301 Report Statutory Criteria	7
E.	Digital Market Access and IP Issues in Select Economies.....	7
1.	Intellectual Property Issues	8
a.	Artificial Intelligence and Machine Learning.....	8
b.	Copyrights	8
c.	Government and SOE Legalization.....	8
d.	Software License Compliance.....	9
e.	Patents	9
f.	Trade Secrets and Other Proprietary Information.....	9
2.	Digital Market Access Issues	10
F.	Conclusion	11

A. Introduction

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world’s most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers IP compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

B. Software, Innovation, and Intellectual Property — Statistical Overview

As USTR Ambassador Katherine Tai has stated, “[the key to our global competitiveness and creating shared prosperity begins at home](#).”⁴ BSA agrees. US global competitiveness requires investments in the innovation and IP ecosystem and in high technology worker skills for a competitive US workforce.

BSA members — representing the enterprise cloud and software sector — invest heavily in innovation and IP (more than any other sector), support US technology leadership, create and provide training for the jobs of tomorrow for US workers, and build stability and resilience into the US economy at a time of unprecedented economic uncertainty. We summarize several relevant statistics below.

- **Growing the US economy through innovation:** BSA members, comprising leading software producers and service providers, invest heavily in the US economy. As of 2021, the US software industry (including US software exports) was responsible for \$1.9 trillion of total US value added GDP.⁵
- **Investing in Innovation and IP Protection:** BSA members invest heavily in US creativity, innovation, and IP generation. Annual US software industry R&D investments exceed US\$103 billion,⁶ and BSA members are counted among: (a) leading US patent recipients (accounting for roughly 75% of all US patents issued to US companies among the top 10 patent grantees);⁷ (b) leading US AI-related patent owners (accounting for 70% of AI-related patents owned by top 10 US companies);⁸ and (c) leading US copyright and trademark holders (accounting for 40% of brand value among US companies in the top 10 ranked brands).⁹
- **Committing to IP Enforcement:** BSA invests in IP enforcement to address the global problem of unlicensed and counterfeit software. Malware from unlicensed software costs companies nearly \$359 billion per year.¹⁰ We partner with key stakeholders around the world to raise awareness of the risk of malware, ransomware, and other critical security threats and drive license compliance through sound IT procurement. BSA handles over 4,000 enforcement actions per year and has removed nearly 1 million infringing host-site links and over 200,000 marketplace listings.¹¹
- **Supporting advanced technology jobs for US workers:** As of 2021, the US software industry supported 15.8 million jobs — jobs that pay more than twice the national average for all occupations.¹² Over 12 million of these jobs are found outside of the technology sector. Software jobs are growing rapidly across all 50 states.¹³
- **Supporting and upskilling tomorrow’s IP-intensive workforce:** BSA members invest heavily in skills development to support tomorrow’s advanced manufacturing and services jobs at home. This means upfront investments in computer programming, software coding, and other digital skills — the skills that are needed to design and build the advanced, connected goods and services demanded in today’s economy, and to compete in connected agriculture and other core industries. A four-year degree is often not necessary to acquire the coding and other skills necessary for software jobs. [Transform Your Trade](#) and similar programs connect workers with software training opportunities in the manufacturing and service sectors across [all 50 US states](#), the [private sector](#), [community colleges](#), vocational schools, and apprenticeship programs.¹⁴ And there is room for further growth, as an estimated [1 to 2 million ICT- and software-related jobs](#) continue to go unfilled in America,¹⁵ especially in the manufacturing sector, where [40 percent of](#)

[manufacturers urge greater investment in skills for advanced manufacturing](#), including software engineering, computer-aided design and manufacturing (CAD/CAM), industrial machinery mechanics, and Computer Numerical Control (CNC) machinery operations.¹⁶

C. Data-Related Market Access Barriers and the Innovation Lifecycle

Data-related market access barriers impact every stage of the innovation life cycle for US persons who rely on IP. 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. These data-related market access barriers — particularly in the form of data localization mandates and cross-border data transfer restrictions — have increased by over 800%, and the rate of increase has further accelerated in recent years.

The WIPO Global Innovation Index (GII), which ranks 132 countries against 81 innovation and IP-related indicators and which aims to help policymakers “discover what works best in producing an ecosystem where people can achieve their highest potential, innovating and creating to improve lives everywhere,” highlights these risks.¹⁷ The GII does not directly account for countries’ cross-border data restrictions, despite the fact that several countries that impose such barriers have stated their belief that such barriers advance “indigenous innovation” goals and despite the close nexus between the cross-border exchange of knowledge, ideas, and information and cross-border access to technology (on the one hand) and R&D, scientific endeavor, innovation, creativity, and intellectual property generation (IP) (on the other). Many of the GII’s metrics would likely be directly impacted by new cross-border data restrictive measures in China, India, and Vietnam, etc., including strict data localization mandates and prohibitions on transfers of “important,” “sensitive,” or “critical” information (whether “personal” or “non-personal”). These measures — often implemented quickly and with minimal input from the public — directly impact GII metrics in the cross-border context, including: (1) legal and operational stability; (2) regulatory quality; (3) ICT access and use; (4) gross expenditures on R&D; (5) university-industry R&D collaboration; (6) cross-border knowledge absorption and output; (7) research talent; and (8) High-tech and ICT services imports.¹⁸

Below we describe four ways in which such data-related barriers harm US persons who rely on IP.

1. Barriers to Core Innovation and R&D

Data-related market access barriers undermine basic research and scientific activity conducted by US persons who rely on IP. In every sector, cross border communication and data transfers play an integral role in basic R&D, and other core innovative and creative functions. For example, in semiconductor design and 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.

This collaborative 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 AI-based analytical techniques to data transferred across borders and consolidated into larger data sets.¹⁹

As explained by the World Intellectual Property Organization (WIPO),²⁰ the US Patent & Trademark Office (USPTO),²¹ and other IP authorities,²² 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 meaningful insights, patterns, and connections that can aid R&D teams in the discovery and development of novel solutions to scientific and technical challenges.

Market access barriers that impede data transfers make such AI-based analysis much more difficult for US persons who rely on IP. Such barriers prevent the consolidation of representative data sets necessary to conduct AI innovation. In this way, these trade barriers directly impede new innovations and creations by US creators, inventors, and IP holders that otherwise could advance scientific and technological progress.

2. Barriers to IP Acquisition, Registration, and Maintenance

Data-related market access barriers threaten the ability of US persons who rely on IP to acquire, register, and maintain IP rights. Applicants must be able to transfer information across borders to apply for patents, copyrights, trademarks, 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 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.

USPTO has studied the distortive impact of non-commercial considerations on patent and trademark application rates abroad.²³ It would be also relevant to review the impact of data-related market access barriers on the ability of US persons to apply for IP rights abroad or at home — particularly where research activities occur in part outside the United States. Indeed, data localization mandates and data transfer restrictions that prohibit the transfer of large and undefined data sets deemed to be “important,” “critical,” or “sensitive” (as in China’s pre-transfer security assessment mandates in its Personal Information Protection Law²⁴) create significant uncertainty regarding the ability to transfer information and data necessary to these procedures for the acquisition, registration, and maintenance of IP rights.

3. Barriers to 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.

Data-related market access barriers can impede IP enforcement by interfering with efforts to monitor marketplaces, gather evidence of infringement in multiple locations, research details of illicit networks, and use 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 in an online environment.

4. Barriers to IP Commercialization

Data-related market access barriers directly undermine 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 cross-border data communications, 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. Special 301 Report Statutory Criteria

Trade barriers and digital protectionism are growing at the very time that data-based innovation and IP generation are helping to sustain economic activity and employment. Against this background, USTR's Special 301 review of trading partners' barriers to IP protection and enforcement and associated market access barriers has ever greater salience.

Pursuant to the Special 301 statutory mandate, 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 two separate sets of criteria:

- “Those foreign countries that **deny adequate and effective protection of intellectual property rights, or**
- **deny fair and equitable market access to United States persons that rely upon intellectual property protection**” (emphasis added).

In this submission, we address both elements of Section 182 of the Trade Act. The document highlights US trading partners with **deficiencies in protecting and enforcing intellectual property rights** and US trading partners that have erected **unfair market access barriers** that affect BSA members. For some countries, the market access barriers present the higher threat to BSA members' ability to do business in the market. In other cases, US trading partners are deficient on both counts.

This year we relate these trade-related challenges to BSA's COVID-19 Response and Recovery Agenda;²⁵ and BSA's Digital Trade Agenda.²⁶

Drawing on these BSA resources, BSA'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 do not propose specific country rankings on the Watch List, Priority Watch List, or Priority Foreign Country lists, and instead request that USTR and the Special 301 subcommittee take BSA's input into account within the broader annual Special 301 review this year. We also refer the reader to BSA's NTE submission for country-specific discussions of innovation and IP-related concerns in each of these markets.

E. Digital Market Access and IP Issues in Select Economies

Both to recover from COVID-19 and to realize the full potential of digital trade, it is important to establish legal frameworks that foster innovation and promote confidence in the digital economy. Effective IP protections and adequate enforcement are a key component of building that trust, as they allow inventors and creators to expect a commercial return on their investments in innovative software-enabled products and services. In addition to IP, data governance policies including privacy protections, cybersecurity measures, standards development process, and other matters are also instrumental for developing trust and confidence among consumers and business customers, investors and developers, and regulators of software-enabled products and services. Conversely, weak IP laws and enforcement mechanisms and data governance rules that are either absent or result in unnecessary market access impediments can undermine this confidence and not only reduce trade and commercial opportunities for BSA members and other US innovators who rely on IP but can harm the economic development and job creation opportunities in the US trading partner.

1. Intellectual Property Issues

We outline below several IP priority issues for BSA members. Please see BSA's 2021 NTE submission for additional country-specific analysis of each of the areas noted below.²⁷

a. Artificial Intelligence and Machine Learning

The National AI Initiative Act of 2020 became law on January 1, 2021, providing for a coordinated program across the entire Federal government to “ensure continued US leadership in AI research and development, lead the world in the development and use of trustworthy AI in the public and private sectors, and prepare the present and future US workforce for the integration of AI systems across all sectors of the economy and society.”²⁸

Along with the ability to transfer data across borders, IP frameworks are critical for data-enabled innovations, including AI, machine learning, cloud-based analytics, and IoT. US leadership in these AI-related technologies has been a priority for the US government for many years,²⁹ and will continue to be.³⁰ AI, machine-learning, and data analytics systems are “trained” by ingesting large data sets to identify underlying patterns, relationships, and trends that are then transformed into mathematical models that can make predictions based on new data inputs. Countries around the world are taking a range of approaches to modernize their legal frameworks for AI systems. This includes Japan’s May 2018 Copyright Law Amendment Act³¹ and Singapore’s new Copyright Act in November 2021, which permit data analytics to be performed for both non-commercial and commercial purposes subject to requirements of lawful access.³² The **EU** has also recently incorporated text and data mining exceptions to its copyright regime. In India, the government has set up the *National Programme on Artificial Intelligence*³³ to implement a principled framework to guide the development and use of responsible AI technologies.³⁴ Finally, in the United States, the “non-consumptive” reproductions that are necessary for the development of AI-related technologies are considered fair use. BSA urges the US government to continue promoting such AI-focused legal frameworks, including in countries like **Australia**³⁵ and **Brazil**, to foster innovation and creativity.³⁶

b. Copyrights

Innovation in the digital environment requires legal frameworks that provide copyright holders with the tools necessary to effectively enforce their copyrights. An effective framework for online copyright enforcement must balance the legitimate needs and interests of all parties with a role in driving innovation, including content creators, Internet service providers, online platform providers (i.e., intermediaries), and members of the public. These interests are best accommodated through safe harbor frameworks that provide online intermediaries with limitations on monetary liability for third party content in exchange for removing content upon notification of claimed copyright infringement from a relevant rights holder. Although a statutory safe harbor framework is a well-established international best practice reflected in the US and Singaporean legal systems (among others), other countries, such as **Brazil** and, in the case of **Mexico**, the 2020 reforms to the Federal Copyright Act regarding safe harbors and notice and takedown need to be upheld by the Supreme Court, in order to maintain compliance with the U.S.–Mexico–Canada Agreement (USMCA).³⁷

c. Government and SOE Legalization

The use of unlicensed software by governments is particularly challenging to BSA members. Because BSA members rely on governments to provide protection and enforcement of their IP rights, if governments are unwilling to comply with the law, there is often little that BSA or our members can do on our own. For example, BSA and its members continue to encounter significant issues with unlicensed software use among Brazil’s over 5,000 municipal governments. We urge the US Government to use mechanisms such as Special 301 to engage with US trading partners on behalf of US companies on this important issue.

d. Software License Compliance

The use of unlicensed software by enterprises and governments is a major commercial challenge for BSA members. According to BSA's Global Software Survey — a global survey of more than 20,000 respondents that estimates the volume and value of unlicensed software installed on personal computers across more than 110 national and regional economies — the commercial value of unlicensed software globally is at least US\$46 billion.³⁸ Not only does the use of unlicensed software impact the revenue stream of BSA members — deterring investments in further innovation, but it also exposes enterprises and agencies engaged in such activity to higher risks of malware infections and other security vulnerabilities.³⁹ Malware from unlicensed software costs companies worldwide nearly US\$359 billion a year. Chief information officers (CIOs) report that avoiding data hacks and other security threats from malware is the number one reason for ensuring their networks are fully licensed.

Organizations now face a one-in-three chance of encountering malware when they obtain or install an unlicensed software package or buy a computer with unlicensed software on it — threatening severe costs due to the loss or exposure of proprietary and sensitive data, including customer derived personal data and trade secrets, and from system outages due to a malware infection. A single malware attack can cost a company US\$2.4 million on average and can take up to 50 days to resolve. To the extent that the infection leads to company downtime, or lost business data, it can also seriously damage a company's brand and reputation. Additionally, the average cost to rectify a ransomware attack in 2021 has been estimated at US\$1.85M, more than double compared to 2020.⁴⁰ Furthermore, collateral damage from ransomware attacks is even more severe — one survey reported that organizations that acceded to ransomware demands never recovered up to a third of encrypted files. Nearly a third of organizations lost more than half their files, and only 8% reported recovery of all their data.⁴¹

BSA has engaged with US trading partners to reduce the incidence of unlicensed software use by enterprises and government entities, with varying degrees of success. These efforts include promoting voluntary compliance measures, such as effective, transparent, and verifiable software asset management (SAM) procedures, where enterprises and government agencies implement the necessary processes to efficiently manage, control, and protect their software assets and, as a result, ensure that all software is properly licensed. Governments can lead by example and adopt such measures for their own procurement and IT maintenance systems, which can send a powerful signal to enterprises in their countries.

e. Patents

BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for businesses, governments, and consumers. It is critical that countries provide effective patent protection for eligible computer-implemented inventions, in line with their international obligations.

f. Trade Secrets and Other Proprietary Information

BSA members rely on the ability to protect valuable trade secrets and other proprietary information to maintain their competitive position in the global marketplace. Countries with weak trade secret protection rules, or that have (or are proposing) policies requiring disclosure of sensitive information, include **China**,⁴² and **South Korea**.⁴³ Additionally, **India's** proposed Non-Personal Data Governance Framework, if implemented, could require the transfer of sensitive proprietary data sets to government entities and to competitors, undermining rights holders' capabilities to protect their trade secrets.⁴⁴ Even India's upcoming data protection law contains provisions that will mandate the transfer of proprietary data to government entities.⁴⁵ Further, the parliamentary committee assessing the Bill reaffirmed the powers of the government to demand proprietary data — and recommended removing trade secret exemptions against data portability requests and requiring companies to disclose 'fairness in algorithms' and 'methods of processing' used, as part of their transparency obligations.⁴⁶

2. Digital Market Access Issues

We highlight the following digital market access issues: (a) cross-border data transfers and data localization; (b) discriminatory trade barriers that impact US persons who rely on IP; (c) customs requirements on electronic transmissions; (d) security; (e) standards; and (f) procurement restrictions.

a. Cross-Border Data Transfers and Data Localization

The ability of US companies to continue leading global advances in innovative technology is under a rising threat from foreign government policies that restrict digital trade and market access. Data-related market access barriers take many forms. Sometimes the policies expressly require data to stay in-country or impose unreasonable conditions on sending data abroad. 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 are based on privacy or security concerns, but too often the real motivation appears to be protectionist, as reflected in their design and operation. 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.

China has published numerous measures that require data localization or restrict data transfers including the Data Security Law, the Personal Information Protection Law, and the Cybersecurity Law, as well as numerous subsidiary measures.⁴⁷ **India** too has imposed data localization requirements, including through India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018, which imposes data and infrastructure localization requirements.⁴⁸ India has also proposed to impose data localization requirements and transfer restrictions under its Personal Data Protection Bill.⁴⁹ The parliamentary committee reviewing the bill has recommended additional restrictions on cross border transfers, and reaffirmed support for data localization as a measure that can enhance India's national security, digital economy, and the privacy of its citizens.⁵⁰ Other regulators and government bodies continue to voice affirmation for data localization across different policy documents.⁵¹

The proposed implementation regulations for **Indonesia's** Government Regulation 71/2019 and OJK Regulation 13/2020 also contain data localization requirements. Likewise, **Vietnam's** 2018 Cybersecurity Law,⁵² Decree 72 on Management, Provision and Use of Internet services and Online Information, and the draft Personal Data Protection Decree impose improper data localization requirements. These guidelines raise significant market access concerns for companies offering software, IT, and data services overseas.

Finally, BSA continues to monitor the application of measures in the **EU** that govern cross-border data flows, as well as the EU's bilateral and plurilateral trade negotiations and developing policies and legal jurisprudence, which could dramatically restrict cross-border data flows with third countries.

c. Customs Requirements on Electronic Transmissions

Across a broad cross-section of economic sectors, there are growing concerns about proposed domestic policies to improperly impose customs duties and other requirements on software and other electronic transmissions. Since 1998, World Trade Organization (WTO) Members have maintained a moratorium on customs duties on electronic transmissions. However, in 2018 **Indonesia** issued Regulation No.17/PMK.010/2018 (Regulation 17), which amends Indonesia's Harmonized Tariff

Schedule to add Chapter 99: “[s]oftware and other digital products transmitted electronically.”⁵³ A few countries, including **India**, have also expressed support for the imposition of customs duties on electronic transmissions.

d. Procurement Restrictions

Governments are among the biggest consumers of software products and services, yet many impose significant restrictions on foreign suppliers’ ability to serve public-sector customers. Not only do such policies eliminate potential sales for BSA members, but they also deny government purchasers the freedom to choose the best available products and services to meet their needs. US trading partners with existing or proposed restrictions on public procurement of foreign software products and services include **China, South Korea, and India**.⁵⁴ For example, **South Korea**’s Cloud Security Assurance Program (CSAP) not only requires use of local data centers for a broad range of cloud services, but also imposes other requirements, including the use of domestic encryption algorithms, that have the effect of prohibiting the certification of foreign cloud services.⁵⁵

e. Security

Governments have a legitimate interest in ensuring software-enabled products, services, and equipment deployed in their countries are reliable, safe, and secure. However, some markets — including **Brazil, China, India, South Korea, and Vietnam** — are using or proposing to use security concerns to justify *de facto* trade barriers.⁵⁶ Requiring cloud service providers to confine data in-country does not improve security but instead ultimately hinders it. First, storing data at geographically diverse locations can enable companies to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location and obscure the location of data to reduce the risk of physical attacks. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Separately, **Thailand**’s Cybersecurity Act raises concerns with respect to the broad authorities granted to seize or freeze computing equipment and to access privately held data without sufficient protections, such as opportunities to appeal or limit such access in view of *inter alia* IP-related considerations.

f. Standards

Technology standards play a vital role in facilitating global trade in software-enabled services and IT. When standards are developed through voluntary, industry-led processes and widely used across markets, they generate efficiencies of scale and speed the development and distribution of innovative products and services. Unfortunately, some countries have developed or are developing country-specific standards. The adoption of country-specific standards creates *de facto* trade barriers for BSA members and raises the costs of cutting-edge technologies for consumers and enterprises. As elaborated in BSA’s October 2021 NTE submission,⁵⁷ countries adopting nationalized standards for IT products include **China, India, South Korea, and Vietnam**.

F. Conclusion

BSA welcomes the opportunity to provide the foregoing brief comments to inform the development of the 2022 Special 301 Report and the US Government’s engagement with key trading partners. We look forward to working with USTR and the US agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee to achieve meaningful progress on the issues described in this submission.

¹ BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

² <https://www.federalregister.gov/documents/2021/12/13/2021-26899/request-for-comments-and-notice-of-a-public-hearing-regarding-the-2022-special-301-review>

³ 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>

⁴ <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/remarks-prepared-delivery-ambassador-katherine-tai-outlining-biden-harris-administrations-new>

⁵ Software.org, *Software – Supporting US Through COVID* (2021), available at: <https://software.org/wp-content/uploads/2021SoftwareJobs.pdf>

⁶ *Id.*

⁷ IFI Claims Patent Services, *2020 Top 50 US Patent Assignees* (accessed Oct. 11, 2021) (“2020 Top 50 US Patent Assignees”), available at: <https://www.ificlaims.com/rankings-top-50-2020.htm>

⁸ USPTO, *Inventing AI - Tracing the Diffusion of Artificial Intelligence with US Patents*, p. 8 (“Figure 6: Top 30 U.S. AI patent owners-at-grant, 1976–2018”) (Oct. 2020), <https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf>

⁹ See Interbrand, *Best Global Brands Report* (2020), [learn.interbrand.com/hubfs/INTERBRAND/Interbrand_Best_Global_Brands%202020_Desktop-Print.pdf](https://www.interbrand.com/hubfs/INTERBRAND/Interbrand_Best_Global_Brands%202020_Desktop-Print.pdf)

¹⁰ BSA Compliance Solutions Website, bsacompliancesolutions.org.

¹¹ *Id.*

¹² Software.org, *Software – Supporting US Through COVID* (2021), available at: <https://software.org/wp-content/uploads/2021SoftwareJobs.pdf>

¹³ *Id.*

¹⁴ <https://transformyourtrade.org/>; <https://blogs.microsoft.com/blog/2021/10/28/america-faces-a-cybersecurity-skills-crisis-microsoft-launches-national-campaign-to-help-community-colleges-expand-the-cybersecurity-workforce/>

¹⁵ BSA | The Software Alliance, *A Policy Agenda to Build Tomorrow's Workforce* (2018), <https://www.bsa.org/files/policy-filings/05022018BSAWorkforceDevelopmentAgenda.pdf>.

¹⁶ https://software.org/wp-content/uploads/Every_Sector_Software_Manufacturing.pdf

¹⁷ World Intellectual Property Organization, *WIPO Global Innovation Index* (Sept. 2021), at: https://www.wipo.int/global_innovation_index/en/2021/index.html

¹⁸ Global Data Alliance, *Cross-Border Data Transfers & Innovation* (2021), at: <https://globaldataalliance.org/wp-content/uploads/2021/07/04012021cbdtinnovation.pdf>; Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical R&D* (2021), at: <https://globaldataalliance.org/wp-content/uploads/2021/09/09092021cbdtbiopharma.pdf>; Global Data Alliance, *Cross-Border Data Transfers & Economic Development* (2021), at: <https://globaldataalliance.org/wp-content/uploads/2021/07/05062021econdevelopments1.pdf>

¹⁹ 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/>

-
- ²⁰ 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
- ²¹ 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>.
- ²² 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](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.
- ²³ See USPTO, *Trademarks and Patents in China: The impact of non-market factors on filing trends and IP systems* (Jan. 2021), <https://www.uspto.gov/sites/default/files/documents/USPTO-TrademarkPatentsInChina.pdf>
- ²⁴ Personal Information Protection Law of the People’s Republic of China, at <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>. See Articles 38 and 40, English translation available at: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.
- ²⁵ BSA | The Software Alliance, *Response and Recovery Agenda* (2020), at: <https://www.bsa.org/files/policy-filings/05272020bsaresponserecoveryagenda.pdf>.
- ²⁶ BSA | The Software Alliance, *Digital Trade Agenda* (2018), at: https://www.bsa.org/files/policy-filings/05072019bsa_advancingdigitaltradeagenda.pdf.
- ²⁷ BSA | The Software Alliance, *National Trade Estimate Submission* (2021), at <https://www.bsa.org/files/policy-filings/10262021ntesub.pdf>
- ²⁸ See National Artificial Intelligence Initiative Office, *Overseeing and Implementing the US National AI Strategy* (2021), at: <https://www.ai.gov/>
- ²⁹ See e.g., Executive Office of the President, *Preparing for the Future of Artificial Intelligence* (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf; Executive Office of the President, *Executive Order on Maintaining American Leadership in Artificial Intelligence* (2019), <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/>
- ³⁰ See *infra* note 4.
- ³¹ Japan Copyright Act at <http://www.japaneselawtranslation.go.jp/law/detail/?id=2506&vm=04&re=01> see Article 47-7.
- ³² Singapore Ministry of Law, *Copyright Act 2021* at <https://sso.agc.gov.sg/Acts-Supp/22-2021/Published/20211007?DocDate=20211007> see Division 8 – Computational Data Analysis, Sections 243 and 244.
- ³³ See 75@75 - India’s AI Journey, Foreword (2021), <https://www.meity.gov.in/writereaddata/files/75-75-India-AI-Journey.pdf>
- ³⁴ See NITI Aayog, *Responsible AI #AIforAll, Approach Document for India, Part 1 – Principles for Responsible AI* (Feb 2021), <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>; NITI Aayog, *Responsible AI #AIforAll, Approach Document for India, Part 2 – Operationalizing Principles for Responsible AI* (Aug 2021), <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf>
- ³⁵ https://www.bsa.org/files/policy-filings/06082018BSA_Response_Australia_DCA_Copyright_Modernisation_Consultation.pdf.

³⁶ See BSA | The Software Alliance, *Comments on the Draft 2018-2022 Strategic Plan of the United States Patent and Trademark Office* (September 18, 2018), pp. 4-5, available at: www.bsa.org/~media/Files/Policy/IntellectualProperty/09202018USPTOCommentsonDraft20182022StrategicPlan.pdf.

³⁷ Since 2020, Mexico implemented the obligations arising from the USMCA by making significant improvements in its current IPR legal framework, revising its Federal Copyright Act, the Federal Criminal Code, and the Federal Law for the Protection of Industrial Property. In addition to safe harbor and notice and takedown provisions, the 2020 reforms incorporated provisions guarding against the circumvention of technological protection measures (TPMs) and protecting rights management information (RMI), which are critical for enabling online business models and products.

Nonetheless, while remaining in force, the provisions on the protection of TPMs and those related to safe harbors and notice and takedown are currently the subject of constitutional challenges initiated by the National Human Rights Commission and a minority of the Mexican Senate, which if successful would seriously undermine Mexico's USMCA obligations and IPR protection. Accordingly, Mexico should actively defend the legal reforms of 2020 so that Mexico can finally and properly implement its international obligations.

³⁸ See BSA Global Software Survey – In Brief (June 2018), available at: https://gss.bsa.org/wp-content/uploads/2018/06/2018_BSA_GSS_InBrief_US.pdf

³⁹ See *id.*

⁴⁰ Sophos, *The State of Ransomware 2021* (2021), available at: <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>

⁴¹ *Id.*

⁴² The Cryptography Law of the People's Republic of China, December 2020 (Chinese), at: <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml>; China's New Cryptography Law – Still No Place to Hide, December 2020, at: <https://harrisbricken.com/chinalawblog/chinas-new-cryptography-law-still-no-place-to-hide/#:%7E:text=The%20PRC%20National%20People%27s%20Congress,effect%20on%20January%201%2C%202020.&text=The%20Law%20provides%20that%20it%20welcomes%20foreign%20providers%20of%20commercial%20encryption.>

⁴³ The Cloud Security Assurance Program (CSAP). See <https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf>.

⁴⁴ Revised Report by the Committee of Experts on Non-Personal Data Governance Framework, accessible at: https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf. See <https://www.bsa.org/files/policy-filings/01292021bsanpd.pdf>.

⁴⁵ See Personal Data Protection Bill, 2019, Section 91, available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

⁴⁶ See Report of the Joint Committee on the Personal Data Protection Bill, 2019, (December 2021), Para 2.85, 2.99, available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

⁴⁷ See China Report in <https://www.bsa.org/files/policy-filings/10262021ntesub.pdf>.

⁴⁸ Reserve Bank of India *Storage of Payment System Data Directive (2018)* at: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0> and Ministry of Electronics and Information Technology *Guidelines for Government Departments on Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

⁴⁹ See Personal Data Protection Bill, 2019, Chapter VII - "Restriction on Transfer of Personal Data Outside India," available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

⁵⁰ See Report of the Joint Committee on the Personal Data Protection Bill, 2019, (December 2021), Para 2.149, 2.150, 2.151, 2.152, available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.

⁵¹ See TRAI Consultation Paper on Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India (December 2021), Para 2.9, 2.28, available at: https://www.trai.gov.in/sites/default/files/CP_16122021.pdf; Report of the Committee of Experts on Non-Personal Data Governance

Framework (Dec 2020), available at: https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf ; Draft National E-Commerce Policy, 2019, available at: https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

⁵² *Vietnam’s 2018 Cybersecurity Law* at: <https://luatvietnam.vn/an-ninh-quoc-gia/luat-an-ninh-mang-2018-luat-an-ninh-mang-so-24-2018-gh14-164904-d1.html#noidung>.

⁵³ Regulation 17 purports to cover a wide array of categories, classified in Indonesia’s tariff schedule between subheadings 9901.10.00 to subheading 9901.90.00, including “multimedia (audio, video or audiovisual)”; operating system software; application software; “support or driver data, including design for machinery system”; and a broad catch-all category covering “other software and digital products.”

⁵⁴ See BSA’s June 4, 2021 submission to the Ministry of Electronics and Information Technology regarding the Department of Promotion of Industry and Internal Trade’s clarifying memorandum on India’s *Public Procurement Preference to Make in India Order* at <https://www.bsa.org/files/policy-filings/06042021softprocurement.pdf>.

⁵⁵ Korea Internet & Security Agency, *Cloud Security Certification* at <https://isms.kisa.or.kr/main/csap/intro/index.jsp> (in Korean). See also <https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf>.

⁵⁶ See relevant sections in BSA’s 2021 Submission to USTR’s National Trade Estimate at: <https://www.bsa.org/files/policy-filings/10262021ntesub.pdf>. In addition to data localization requirements, many of cybersecurity related barriers include requirements to certify to domestic standards that diverge from internationally recognized security standards, use local certification bodies, even if already certified by accredited international bodies, use certain encryption algorithms, and in some cases, disclose source code.

⁵⁷ *Id.*