January 30, 2024

Docket No. USTR-2023-0014 (88 Fed. Reg. 84869)

Claire Avery-Page
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 Ms. Avery-Page,

BSA | The Software Alliance[1] provides the following information in response to the notice published by the Office of the US Trade Representative (USTR) seeking comments on the 2023-2024 Special 301 review under Section 182 of the Trade Act of 1974 (Special 301). USTR's leadership – together with its partners at the US Patent & Trademark Office (USPTO) and the US Copyright Office – on international IP policy is critical to the development of a global policy and legal environment in which the technologies of tomorrow can emerge and flourish.

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. Finally, as innovators and creators, BSA members also rely heavily on AI tools to create new IP and to assist others in doing the same. BSA's 2024 Special 301 submission builds on its submissions in prior years, but it adds new material regarding the importance of the United States promoting calibrated policies to ensure that AI continues to advance US global leadership in innovation and creativity.

The competitiveness of US innovators in the globalized economy is buoyed by polices that create as much certainty as possible in the protection and enforcement of their IP. USTR can play an important role in establishing such certainty by engaging with our trading partners to promote alignment with the US framework for IP protection. USTR's international engagement should promote both the core substantive protections afforded by US patent and copyright law as well as the critical flexibilities that have been integral to the development of digital technologies. We note the importance of such flexibilities to the development of AI technology in particular – an area in which US companies are global leaders.

Artificial Intelligence (AI) is at the center of many creative, technological, and scientific endeavors in today's digitized economy. AI involves the application of analytical techniques to data generated in various countries, transferred across borders, and consolidated into larger data sets. AI provides creators with new tools to enhance their craft— in visual and special effects in film, in sound mixing, in architectural planning, and in vehicular styling and design. In healthcare, AI helped fast-track the COVID-19 vaccine, cutting R&D timelines from years to months, as researchers were aided by computational analysis of drug discovery data transferred from around the world to quickly identify potential candidates.[2]

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

BSA's 2024 Special 301 Submission contains the following major sections:

A. Introduction 3
B. Special 301 Report Statutory Criteria 3
C. Software, Innovation, and Intellectual Property — Statistical Overview 3
D. Artificial Intelligence and the United States' Approach to International IP & Innovation Policies 4
1. What AI-Related IP Policies Should US Trading Partners Adopt? 4
2. What AI-Related Data & Innovation Policies Should US Trading Partners Adopt? 5
E. Data-Related Market Access Barriers and the Innovation Lifecycle 6
F. Digital Market Access and IP Issues in Select Economies 6
1. Intellectual Property Issues 6
a. Artificial Intelligence and Machine Learning 6
b. Copyrights 7
c. Software License Compliance 7
d. Patents 7
e. Trade Secrets and Other Proprietary Information 8
2. Digital Market Access Issues 8
G. Conclusion 9

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. Special 301 Report Statutory Criteria

Trade barriers and digital protectionism are growing at the very time that AI- and 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"

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.

C. 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."[3] 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 AI-based innovation and IP, thereby supporting US technology leadership, creating the jobs of tomorrow for US workers, and building 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.[4]

- **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$100 billion,[5] and BSA members are counted among: (a) leading US patent recipients (accounting for roughly 60% of all US patents issued to US companies among the top 10 patent grantees);[6] (b) leading US AI-related patent owners (accounting for 70% of AI-related patents owned by top 10 US companies);[7] and (c) leading US copyright and trademark holders (accounting for 40% of brand value among US companies in the top 10 ranked brands).[8]

- **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.[9] 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.[10]

- **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.[11] Over 12 million of these jobs are found outside of the technology sector. Software jobs are growing rapidly across all 50 states.[12]

- **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. Numerous 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.[13] 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,[14] 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.[15]

D. Artificial Intelligence and the United States' Approach to International IP & Innovation Policies

Continued US leadership in AI is both critical to, and fundamentally dependent upon, a healthy and well-calibrated innovation ecosystem spanning US and allied economies. The success of the Biden-Harris Administration Executive Order on AI is premised upon both stable and predictable international IP rules relating to AI as well as stable and predictable rules that promote cross-border access to data from around the world.

1. What AI-Related IP Policies Should US Trading Partners Adopt?

The United States must take care not to undermine its own leadership in AI by undermining legal frameworks that both promote AI innovation and deter infringement through AI-based systems. From an IP perspective, this means promoting a conducive environment for AI-based R&D, while penalizing the creation of outputs that infringe IP rights. We address three aspects of AI-related copyright policies below.

- Responsible AI Training and Protecting Artists and Copyright Holders: Training AI systems involves the computational analysis of large volumes of data. An AI system turns bits of data into tokens and maps how a token correlates with others. Computational analysis allows the AI system to predict what will come next. Copyright protection applies broadly to almost any creative expression. Some of the data used to train an AI system may be part of a copyrighted work. But the training data is normally not used for its expressive content. Rather, the data is disassembled into smaller machine-readable units — or "tokens" — and then put through a computational analysis that involves mathematical calculations of probabilities, correlations, trends, and other patterns across millions or billions of tokens in a training data set. An AI developer training a large language model, for instance, may use publicly available textual material (common examples may include public but

copyright-protected essays or anonymous commentary on a website) to create a training data set. In many LLMs, this data is used primarily to extract unprotected information about linguistic patterns (e.g., the correlations, patterns, and relationships among "tokens" spanning the 26 letters of the English alphabet and 1 million English language words, as they appear in thousands of stock phrases, figures of speech, similes, metaphors, and common expressions).

Such AI training should not be deemed to infringe copyright, meaning that it should be protected — depending upon the jurisdiction — as "fair use" or "fair dealing," or under a statutory exception. Nonetheless, we also encourage economies to consider additional steps to protect the creativity of artists. One step is to encourage voluntary conversations around automated tools to indicate that the rights-owner does not want a website used for training purposes, similar to the current "do not crawl" tools that apply to search engines. We support further discussions to arrive at effective consensus-based technical mechanisms.

- **Remedies if AI-Generated Works Infringe:** Copyright holders should have full and effective remedies when their rights are infringed. This principle applies equally to outputs generated using AI systems. Copyright remedies have been effective to deter infringement and should remain so.

- **Copyright Protection for Creators Using AI:** Generative AI can bolster creativity, just as other software applications have long been an important tool of artists and storytellers (e.g., photo enhancements for visual artists, special effects in audio-visual works, and arranging music for sound recordings). When generative AI is used to enhance human creativity, the resulting work should be protected by copyright. If copyright protection is not available simply because AI was used in the creative process, it will limit the responsible use of AI and the purpose of our copyright laws.

2. What AI-Related Data & Innovation Policies Should US Trading Partners Adopt?

The United States must also take care not to undermine its own leadership in AI by failing to negotiate rules to protect itself against arbitrary, discriminatory, disguised, or unnecessary foreign government impediments to US access to data needed to conduct cutting-edge AI research and innovation in the United States. Data lies at the core of the AI Executive Order. This includes health data, climate and emissions data, agricultural and meteorological data, and other data needed – in the words of US Secretaries Antony Blinken and Gina Raimondo – to address "some of the world's biggest challenges, from curing cancer to mitigating the effects of climate change to solving global food insecurity." Cross-border access to larger data sets also aids the exchange of incident data for high-risk AI systems, improves AI functionality, and supports testing for bias, safety, and resiliency. Impediments to US and allied cross-border access to data would frustrate the Administration's aims to "catalyze AI research" in relation to agriculture, climate, health, or the economy. Such impediments will also undermine the ability to evaluate whether AI systems would undermine its ability ensure that AI is "safe and secure." When such impediments result in AI data sets that are too small, it also impedes efforts to "test, understand, and mitigate risks" and to develop effective safeguards against "societal harms such as fraud, discrimination, bias, and disinformation," as well those relating to the workplace, competition, and security.

We urge the United States to abide by longstanding principles of democratic, transparent, and accountable governance in the digital environment by reaffirming: (1) the freedom to pursue necessary regulatory objectives; (2) the renunciation of discrimination against non-national persons, products, services, or technologies; (3) the commitment to minimize the trade-restrictive effects; and (4) due consideration for trading partner laws. These tenets – which trace back to the 1947 General Agreement on Tariffs and Trade – now apply to all multilateral trade rules, including those relating to goods, services, investment, technical regulations, and customs procedures. In the same spirit, we urge the United States to support these norms in relation to trade rules relating to the cross-border movement of data. The United States' failure to support these longstanding international rule of law norms – even vis-à-vis our closest allies – would create the unfortunate and avoidable appearance of alignment with policies favored by digital authoritarians.

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

Impediments to US leadership in AI-based innovation and creativity 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 affecting climate and health technologies that are the focus of the White House Executive Order on AI;

(2) the acquisition and maintenance of IP rights that increasingly involve AI-driven processes to optimize patent prior art searches and other IP office procedures; and

(3) the enforcement of IP rights and brand protection activities, which can be facilitated by AI tools that can identify instances of trademark, copyright and patent infringement, as well as foreign sources of IP infringing goods.

F. Digital Market Access and IP Issues in Select Economies

Below we introduce relevant IP and digital market access issues affecting US IPR holders in select trading partner economies. 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.[16]

1. Intellectual Property Issues

We outline below several IP priority issues for BSA members.

a. Artificial Intelligence and Machine Learning

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,[17] and will continue to be.[18] 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 amendment of the Copyright Act[19] and **Singapore's** Copyright Act in November 2021, both of which permit data analytics to be performed for both non-commercial and commercial purposes subject to requirements of lawful access.[20] The **EU** has also incorporated in 2019 a text and data mining exception to its copyright regime. In India, the Government has set up the *National Programme on Artificial Intelligence*[21] to implement a principled framework to guide the development and use of responsible AI technologies.[22] In Australia, the Government established a Copyright and AI Reference Group[23] to consider copyright issues emerging from AI, including how copyright protected material may be used to train AI models, measures to enhance the transparency of inputs and outputs, the implications of using AI to create imitative works, and whether/when AI-generated works should receive copyright protection. 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,**[24] **Canada, Brazil, Hong Kong, South Korea,**[25] and **the United Kingdom** to foster innovation and creativity.[26]

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), not all countries have adopted such frameworks. 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 to ensure compliance with the US–Mexico–Canada Agreement (USMCA).[27]

c. Software License Compliance

The use of unlicensed software deters investments in innovation and exposes enterprises and agencies engaged in such activity to higher risks of malware infections and other security vulnerabilities.[28] 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.[29] 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.[30]

BSA engages 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. Enforcement measures to deter such unauthorized software use may also help promote a more secure digital environment. Countries that do not undertake meaningful enforcement options – such as **Vietnam and Indonesia** – create significant cybersecurity risks for themselves and their trading partners by indirectly facilitating the dissemination of malware and increased cyberrisk. **Vietnam**, in particular, continues to remain an outlier. The Ministry of Culture, Sports & Tourism has not conducted any enforcement of the use of unlicensed software by corporate end users for three years. This inactivity has resulted in an increase in the use of unlicensed software in Vietnam, causing significant harm to BSA's members.

d. 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.

At the same time, BSA members are increasingly facing an emerging trend involving certain foreign courts issuing overbroad injunctions relating to the practice of standard essential patents (SEPs) – i.e., patents

that are necessary to practice industry standards where the patent owner has committed to license on fair, reasonable and non-discriminatory (FRAND) terms. Recently, courts in the United Kingdom and Germany have shown willingness to impose injunctions for SEP infringement in the absence of bad faith behavior. Perhaps the most problematic aspect of this judicial practice has been courts' practice of determining FRAND royalty rates based on a global license, not one restricted to patents and infringing activities within the proper jurisdiction of the national court. This practice essentially allows SEP holders to ask British or German courts to make extraterritorial (global) determinations of infringement and impose a corresponding remedy, even with respect to US patents and the price of practicing those patents in the United States. We urge USTR to further examine these cases of jurisdictional overreach.[31]

e. 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**,[32] and **South Korea**.[33] **India's** upcoming digital personal data protection law also contains provisions that will mandate the transfer of proprietary data to government entities.[34]

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.[35] **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.[36]India's new Digital Personal Data Protection (DPDP) Act 2023 currently permits companies to transfer personal data internationally. But the Government retains broad and vague powers to restrict transfer or processing of personal data to or in a territory outside India without a framework of how such a decision would be made. [37] Other regulators and government bodies continue to voice affirmation for data localization across different policy documents.[38]

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,[39] 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.

b. 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, on January 14, 2023, Indonesia's Ministry of Finance issued a new regulation (Regulation No. 190/PMK.04/2022) requiring importers to file a customs declaration to be made for any import of intangibles through electronic transmission. A few countries, including **India**, have also expressed support for the imposition of customs duties on electronic transmissions.

c. 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. US trading partners with existing or proposed restrictions on public procurement of foreign software products and services include **China, South Korea, and India.**[40]

d. 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.[41]

e. 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 NTE submission,[42] countries adopting nationalized standards for IT products include **China, India, South Korea,** and **Vietnam**.

G. Conclusion

BSA welcomes the opportunity to provide the foregoing brief comments to inform the development of the 2023-2024 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, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *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

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

[4] Software.org, Software – Supporting US Through COVID (2021), available at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf

[5] *Id*.

[6] IFI Claims Patent Services, 2022 Top 50 US Patent Assignees (accessed Jan. 10, 2022) ("2022 Top 50 US Patent Assignees"), available at: https://www.ificlaims.com/rankings-top-50-2022.htm

[7] 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

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

[9] BSA Compliance Solutions Website, bsacompliancesolutions.org.

[10] *Id*.

[11] Software.org, Software – Supporting US Through COVID (2021), available at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf

[12] *Id*.

[13] 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/

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

[15] https://software.org/wp-content/uploads/Every_Sector_Software_Manufacturing.pdf

[16] BSA | The Software Alliance, National Trade Estimate Submission (2022), at https://www.bsa.org/files/policy-filings/10282022nteustr.pdf

[17] *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/

[18] *See infra* note 4.

[19] Japan Copyright Act at https://www.japaneselawtranslation.go.jp/en/laws/view/4207

see Article 30-4 and 47-5.

[20] 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.

[21] *See* 75@75 - India's AI Journey, Foreword (2021), https://www.meity.gov.in/writereaddata/files/75-75-India-AI-Journey.pdf

[22] *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

[23] *See* Copyright and AI reference group to be established (December 5, 2023), available at: https://ministers.ag.gov.au/media-centre/copyright-and-ai-reference-group-be-established-05-12-2023

[24] https://www.bsa.org/files/policy-filings/06082018BSA_Response_Australia_DCA_Copyright_Modernisation_Consultation.pdf.

[25] The Korea Copyright Commission recently released its Generative AI Copyright Guidelines which recommended, among other things, that AI service providers "proactively secure legal usage rights" from copyright holders. While non-binding, this could signal an intent by policy makers to require consent for the use of data that is accessible legally. If implemented, this would chill AI development and create uneven playing fields. *See* Generative AI Copyright Guidelines (January 16, 2024), available (only in Korean) at: https://www.copyright.or.kr/information-materials/publication/research-report/view.do?brdctsno=52591.

[26] *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.

[27] 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.

[28] *See id.*

[29] 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. 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

[30] Id. Nearly a third of organizations lost more than half their files, and only 8% reported recovery of all their data.

[31] Some members have highlighted requirements in India to request *ex ante* permission before filing for patent protection outside of the country in which the invention was made or the inventor resides. These requirements can be abused as a means for local offices to extract excessive fees or a way to force IP owners to file applications in countries in which they otherwise would not.

[32] 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.

[33] The Cloud Security Assurance Program (CSAP). See https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.

[34] See BSA Comments on Digital Personal Data Protection Bill, 2022, available at: https://www.bsa.org/files/policy-filings/12172022cmtsdpdp.pdf

[35] See China Report in https://www.bsa.org/files/policy-filings/10282022nteustr.pdf.

[36] 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

[37] Digital Personal Data Protection Act 2023 at: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[38] 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.

[39] *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-qh14-164904-d1.html#noidung.

[40] See BSA's recent 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/07052023indiameity.pdf .

[41] See relevant sections in BSA's 2022 Submission to USTR's National Trade Estimate at: https://www.bsa.org/files/policy-filings/10282022nteustr.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.

[42] *Id.*