October 28, 2022

Mr. William Shpiece
Chair of the Trade Policy Staff Committee
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Re: Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 87 Fed. Reg. 56741 (Sept. 15, 2022): Docket Number USTR–2022–0013

Dear Mr. Shpiece,

BSA | The Software Alliance[1] provides the following information in response to your request[2] for written submissions to the Trade Policy Staff Committee (TPSC) regarding significant trade barriers for inclusion in the National Trade Estimate on Foreign Trade Barriers (NTE Report). The efforts of the Office of the US Trade Representative (USTR) to support open markets and combat trade barriers are critical to supporting the global economic recovery amidst numerous global challenges. We look forward to any questions that you may have regarding our submission.

Sincerely yours,

Joseph Whitlock
Joseph Whitlock
Director, Policy
BSA | The Software Alliance

---

[1] BSA | The Software Alliance (www.bsa.org) 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 compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *See* USTR, Request for Comments on Significant Foreign Trade Barriers for the National Trade Estimate Report, 87 Fed. Reg. 56741 (Sept. 15, 2022), at: https://www.federalregister.gov/documents/2022/09/15/2022-19896/request-for-comments-on-significant-foreign-trade-barriers-for-the-2023-national-trade-estimate

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Submission of BSA | The Software Alliance re
National Trade Estimate on Foreign Trade Barriers

This document responds to USTR's solicitation of information relevant to the NTE Report, and contains the following major sections:

I. Executive Summary

The following executive summary introduces the importance of software and digital trade, relevant NTE criteria for digital trade, and key market access and intellectual property (IP) priorities in select economies.

A. Software and Digital Trade — Statistical Overview

Over the past decade, the US software industry and cross-border digital trade have become a primary driver of the global economy. As illustrated below, the US software industry has helped build stability and resilience into the US economy at a time of unprecedented economic uncertainty:

- Software drives growth: As of 2021, the US software industry (including US software exports) were responsible for $1.9 trillion of total US value added GDP and 15.8 million jobs — jobs that pay more than twice the national average for all occupations.[3]
- Software drives innovation: For example, BSA members are counted among the top US patent recipients (accounting in 2021 for nearly 75 percent of all US patents issued to US companies among the top 10 patent grantees)[4] and among the major US copyright and trademark holders. Annual US software research and development (R&D) investments exceed US$103 billion.[5]
- Software drives economic opportunity: Jobs in software development, computer programming and related fields are growing so rapidly that the US Bureau of Labor Statistics estimates 1 million computer programming jobs need to be filled in the United States.[6]

Internationally, these trends are also pronounced, and they have only accelerated in the wake of the COVID-19 pandemic and amidst growing economic uncertainty today:

- Digital trade drives the global economy: Pre-2020, software-enabled cross-border data transfers were estimated to contribute trillions of dollars to global GDP,[7] with 75 percent of the value of cross-border data transfers benefitting industries like agriculture, logistics, and manufacturing.[8]
- Digital trade is key to a global economic recovery: Post-2020, the shift to cloud- and software-enabled activity has accelerated. For example, the number of employees working remotely in mid-2020 is estimated to have grown (at least) four-fold over prior years,[9] while telehealth services are expected to grow seven-fold by 2025.[10] Digital trade is particularly important to small- and medium-sized enterprises that can benefit from reduced barriers to foreign market access offered by digital technologies.

Digital trade is the critical factor in global economic growth today. In every sector and at every stage of the production value chain, cloud- and software-enabled data transfers enable the digital tools and

---

[3] Software.org, Software – Supporting US Through COVID (2021), available at: https://software.org/wp-content/uploads/2021SoftwareJobs.pdf
[4] 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
[5] Software.org, Growing US Jobs and the GDP (Sept. 2019), available at: software.org/wp-content/uploads/2019SoftwareJobs.pdf.
[6] BSA | The Software Alliance, *A Policy Agenda to Build Tomorrow's Workforce* (2018), available at: https://www.bsa.org/files/policy-filings/05022018BSAWorkforceDevelopmentAgenda.pdf.
[7] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), at https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.
[8] *Ibid.*
[9] *See generally,* Global Data Alliance, *Cross-Border Data Transfers and Remote Work* (2020), https://www.globaldataalliance.org/downloads/10052020cbdtremotework.pdf. Prior to the COVID-19 crisis between five and fifteen percent of US employees worked remotely. Today, studies indicate that 50 percent or more of employees are working remotely, with even higher percentages in certain regions and certain professions.
[10] *See generally*, Global Data Alliance, *Cross-Border Data Transfers and Remote Health Services* (2020), available at: https://www.globaldataalliance.org/downloads/09152020cbdtremotehealth.pdf.

insights that are critical to enabling entrepreneurs and companies of all sizes to create jobs, boost efficiency, drive quality, and improve output.[11]

B. NTE Report Statutory Criteria and Policy Priorities for Software and Digital Trade

Unfortunately, trade barriers and digital protectionism are growing at the very time that digital trade and connectivity are helping to sustain economic activity and employment. Against this background, USTR's review of trade barriers under Section 181 of the Trade Act of 1974, as amended (19 USC § 2241), has ever greater salience. The statute requires USTR to "identify and analyze acts, policies, or practices of each foreign country which constitute significant barriers to, or distortions of —

- United States exports of goods or services (including … property protected by trademarks, patents, and copyrights exported or licensed by United States persons);
- foreign direct investment by United States persons, especially if such investment has implications for trade in goods or services; and
- United States electronic commerce."[12]

In this submission, we address all three statutory elements of Section 181 of the Trade Act as they relate to the trade-related challenges that BSA members increasingly face abroad, and as they relate to the trade-related aspects of BSA's COVID-19 Response and Recovery Agenda[13] and BSA's Digital Trade Agenda.[14] Drawing on these BSA resources, BSA's NTE submission address policies of note in the following markets: Australia, Brazil, China, India, Indonesia, Japan, Korea, Singapore, Thailand, Vietnam, and the European Union (EU).

C. Digital Market Access and Intellectual Property (IP) Issues in Select Economies

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. We discuss several digital market access issues and several intellectual property (IP) issues below.

1. Digital Market Access Issues

We highlight the following digital market access issues: (1) cross-border data transfers and data localization; (2) discriminatory trade barriers including discriminatory digital taxes; (3) customs requirements on electronic transmissions; (4) security; (5) standards; and (6) procurement restrictions.

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;

---

[11] *See* Global Data Alliance, *The Cross-Border Movement of Data: Creating Jobs and Trust Across Borders in Every Sector* (2020), at https://www.globaldataalliance.org/downloads/GDAeverysector.pdf ; See Global Data Alliance, *Jobs in All Sectors Depend Upon Data Flows* (2020), at https://www.globaldataalliance.org/downloads/infographicgda.pdf.
[12] 19 USC 2411 *et seq.*
[13] BSA | The Software Alliance, *Response and Recovery Agenda* (2020), at: https://www.bsa.org/files/policy-filings/05272020bsaresponserecoveryagenda.pdf.
[14] BSA | The Software Alliance, *Digital Trade Agenda* (2018), at: https://www.bsa.org/files/policy-filings/05072019bsa_advancingdigitaltradeagenda.pdf.

- Constitute unnecessary, unjustified and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or
- Treat cross-border data transfers less favorably than domestic data transfers.

Sustained attention to these threats is critical. Unfortunately, some markets, including **China, India, South Korea, Indonesia, and Vietnam**, have adopted, or have proposed, rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory.

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. 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.[15] South Korea's Cloud Security Assurance Program (CSAP) requires use of local data centers for a broad range of cloud services.[16] The proposed implementation regulation for Indonesia's Government Regulation 71/2019 and OJK Regulation 13/2020 also contain data localization requirements. Likewise, Vietnam's 2018 Cybersecurity Law[17] and draft implementing regulations, including Decree 53/2022, 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 transfers, as well as the EU's bilateral and plurilateral trade negotiations and developing policies and legal jurisprudence, which could dramatically restrict cross-border data transfers with third countries.

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."[18] Some countries, including **India** and **South Africa**, have also expressed support for the imposition of customs duties on electronic transmissions. If successful, these misguided efforts would increase costs of digital products and services and reduce productivity and competitiveness for local industries in the implementing countries.

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, Thailand, and Vietnam** — are using or proposing to use security concerns to justify *de facto* trade barriers. 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

---

[15] *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.

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

[17] *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.

[18] 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."

patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data.

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 or proposing de facto cybersecurity mandatory certification for ICT products, services and processes. 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. Countries adopting nationalized standards for IT products include **China and South Korea**.

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 **Australia, China, South Korea, and India.**

2. Intellectual Property Issues

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, India, and Indonesia.** In addition, countries including **China and South Korea** have implemented or proposed policies, such as sector-specific outsourcing or IT risk management frameworks, that require source code review of technologies or services.

Patents: BSA members depend around the world upon effective patent protection to eligible computer-implemented inventions, in line with their international obligations.

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 have yet to modernize their copyright frameworks in this regard.

Artificial Intelligence and Machine Learning: IP frameworks are critical to data-enabled innovations, including artificial intelligence (AI), machine learning, cloud-based analytics, and the Internet of Things (IoT). 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 Act and Singapore's January 2019 Copyright Review Report, which permit data analytics to be performed for both non-commercial and commercial purposes subject to requirements of lawful access — e.g. via a paid subscription.[19] The EU has also recently incorporated text and data mining exceptions to its copyright regime. Finally, in the United States, the "non-consumptive" reproductions that are necessary for the development of AI-related technologies are

[19] Singapore Ministry of Law, Singapore Copyright Review Report, pp. 32-34 (Jan. 17, 2019), available at: https://www.mlaw.gov.sg/content/dam/minlaw/corp/News/Press%20Release/Singapore%20Copyright%20Review%20Report%202019/Annex%20A%20-%20Copyright%20Review%20Report%2016%20Jan%202019.pdf.

considered fair use. BSA urges the US government to continue promoting such AI-focused legal frameworks, including in countries like **Australia**[20] and **Brazil,** to foster innovation and creativity.[21]

Software License Compliance: The use of unlicensed software by enterprises and governments is a major commercial challenge for BSA members, having a commercial value of at least US$46 billion.[22] Unlicensed software also presents a serious security risk: Malware from unlicensed software costs companies worldwide nearly US$359 billion a year, and a single malware attack can cost a company US$2.4 million on average and can take up to 50 days to resolve. One means of mitigating these risks is through 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 their software assets, including for licensing purposes. Governments should lead by example and adopt such measures for their own procurement and IT maintenance systems.

D. Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the NTE Report and the United States' engagement with important trading partners in 2023. We look forward to working with USTR and the US agencies represented on the TPSC to achieve meaningful progress in addressing the barriers to trade, investment, and e-commerce identified in this submission.

[20] The copyright regime in Australia does not have an exception allowing the use of text and data mining for the purposes of develop AI algorithms. The current round of copyright reforms in Australia failed to address the private sectors' concerns and focused on non-commercial and government use exceptions. They are detailed at: https://www.communications.gov.au/departmental-news/copyright-access-reforms.

[21] 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.

[22] 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.

II. Country-by-Country Analysis

A. Australia

Overview/Business Environment

The Australian Government traditionally has been a strong proponent of facilitating cross-border data transfers and avoiding data localization requirements, recognizing that such restrictions on data will raise costs for businesses and act as a market barrier and in most cases not materially reducing cyber risk. However, disparate departments within the Government also have been prolific in policy making designed to address perceived challenges in the Australian technology ecosystem, but that non-unified approach represents complexity and overhead challenges to organizations to comply, and operational difficulties to technology companies best suited to help drive digital transformation and security in Australia.

Hosting Certification Framework (HCF): Service Providers that deliver or manage hosting services to Australian Government customers, including the facilities that host government data, their systems and supply chains, are required to be HCF-certified. The HCF was originally conceived to address supply chain and foreign ownership risks presented by data hosting providers.[23] However, the agency in charge of the HCF — the Digital Transformation Agency (**DTA**) — has indicated that the HCF may be expanded to cover Software-as-a-Service (**SaaS**) providers.

The expansion of HCF to SaaS providers adds an unnecessary layer of certification on top of existing security guidelines and mechanisms, which are already fit for purpose. Some examples include the following:

- The Attorney General Department's Protective Security Policy Framework (**PSPF**) already provides guidance to Non-Corporate Commonwealth Entities (**NCCEs**) to support the effective implementation of policy across the areas of security governance, personnel security, physical security, and information security. [24]
- The Information Security Registered Assessors Program (**IRAP**) enables Australian Government customers to ensure appropriate controls are in place and determine the appropriate responsibility model for addressing the requirements of the Australian Government Information Security Manual (**ISM**) produced by the Australian Cyber Security Centre (**ACSC**). Assessors certified under the IRAP can provide security assessments of cloud services. To assist with the assessment of cloud services, the Cloud Security Controls Matrix (**CSCM**) can be used by IRAP assessors to capture the implementation of security controls. The CSCM also provides indicative guidance on the scoping of cloud security assessments, and inheritance for systems under a shared responsibility model.[25]

Furthermore, following the recent amendments to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**),[26] owners and operators of critical infrastructure assets, including data storage/processing assets, are required to provide owner and operator information to the Register of Critical Infrastructure Assets and to notify the Australian Government whenever cyber security incidents occur. They are also required to adopt and maintain a risk management program (**RMP**) to identify hazards that present a material risk to the availability of their critical infrastructure assets, and to proactively minimise or eliminate the risk of such hazards occurring.[27]

---

[23] Release of the Hosting Certification Framework, March 2021, https://www.dta.gov.au/news/release-hosting-certification-framework
[24] Protective Security Policy Framework, Policies, https://www.protectivesecurity.gov.au/policies
[25] Australia Cyber Security Centre, Infosec Registered Assessors Program, https://www.cyber.gov.au/acsc/view-all-content/programs/irap
[26] Security of Critical Infrastructure Act 2018, https://www.legislation.gov.au/Details/C2022C00160
[27] Australia Cyber and Infrastructure Security Centre, Critical Infrastructure, https://www.cisc.gov.au/legislative-information-and-reforms/critical-infrastructure

With these regulations, guidelines, and mechanisms already in place, the application of HCF to SaaS providers is unnecessary and will further complicate the regulatory and compliance landscape, making it more costly and burdensome for businesses to navigate. The DTA has recently hosted information sessions for the development of HCF 2.0. BSA recommends the ongoing consultations not solely focus on an implementation agenda for HCF for SaaS but rather on any threats and risks not already addressed by the afore-mentioned PSPF, IRAP CSCM, and SOCI RMP. Where a gap is identified, enhancing or extending those programs first rather than introducing the burden of an additional certification scheme should be pursued.

Personal Data Protection

Privacy Act Reform

Australia is considering a major overhaul and revision of their privacy and personal data protection legislation, *the Privacy Act 1988*.[28] In October 2020, the Attorney General's Office published an Issues Paper,[29] to which BSA filed comments.[30] The following year, in October 2021, the Government published a Discussion Paper,[31] building upon the comments received. BSA also provided comments on the Discussion Paper.[32] We expect an exposure draft of legislative reform by the end of the year or early next.

This is an important opportunity for Australia to modernize its privacy law. We know that with the major breach of personal information reported in Australia in September 2022,[33] there is enhanced urgency to upgrade legislation to enhance information sharing and increase penalties for failure to comply with Australia's laws.

BSA's key recommendations include:

- Implementing a clear distinction between the roles and obligations of entities that decide how and why to collect personal information (**controllers**) and those that simply process collected personal information on behalf of another entities (**processors**).
- Adjust the definition of personal information such that: (1) information which presents only a remote or hypothetical risk of identifying a specific consumer would not be covered by the Act; and (2) location data, should it be listed as an example of personal information, be limited to precise geolocation information relating to an identifiable individual.
- Continue to recognize that adequately de-identified information is not subject to the Act, expressly state whether pseudonymized information falls within the definition of personal information, and, to the extent that the Act covers pseudonymized information, subject that information to less stringent requirements than those applied to personal information. The Act should also actively encourage companies to use pseudonymization.
- Recognize legitimate interests as a lawful basis for processing personal information and implement guidelines, factors, and checklists to help companies understand how to use this basis.
- Recognize existing mechanisms governing international data transfers, such as the APEC Cross-Border Privacy Rules (**CBPR**) and Privacy Rules for Processors (**PRP**) and, to the extent that new mechanisms governing international data transfers are created, these new mechanisms

[28] Australia Privacy Act 1988, https://www.legislation.gov.au/Details/C2020C00237
[29] Privacy Act Review: Issues Paper; October 2020, https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf
[30] BSA Comments on the Review of the Australian Privacy Act 1988, November 2020, https://www.bsa.org/files/policy-filings/11272020ausprivacyactrev.pdf
[31] Privacy Act Review: Discussion Paper, October 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf
[32] BSA Comments on the Review of the Australian Privacy Act 1998, January 2022, https://www.bsa.org/files/policy-filings/01212022aupriv1988.pdf
[33] Optus notifies customers of cyberattack compromising customer information, September 22, 2022, https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack

should remain voluntary and be interoperable with other global schemes. The Act also should retain the informed consent exception in APP 8.2(b).

This is an important opportunity for Australia to modernize its privacy law. Given the major breach of personal information reported in Australia in September 2022,[34] there is urgency to upgrade legislation to enhance information sharing and increase penalties for failure to comply with Australia's laws. Recent events underscore the need to increase investments in cybersecurity, while avoiding the types of counterproductive localization requirements that do not prevent such breaches.

Online Privacy Bill

In 2021, Australia introduced the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*.[35] The Bill was intended to implement the recommendations of the Australian Competition and Consumer Commission (ACCC) as described in the July 2019 report of the Digital Platforms Inquiry.[36] Among other things, the Online Safety Bill was intended to establish the development of a privacy code for digital platforms and to increase the penalties for breach of the Privacy Act.[37]

In our comments to the proposed legislation,[38] we urged the Attorney-General's Department to:

- Expressly exclude from the scope of the Online Privacy code companies which provide services designed for enterprise customers as opposed to individual consumers.
- Adjust the overly broad definition of "organisations providing social media services" such that its application is limited to online services and platforms which interact directly with individual endusers and enable or encourage such end users to post content for consumption by the public. Specifically, this definition should be narrowed to exclude services used for online business interactions and other business purposes, in line with the existing definition of social media service under the Online Safety Act (see below).
- Adjust the overly broad definition of "organisations providing data brokerage services" such that it focuses on organisations that collect and sell personal information of end-users with whom they do not have a direct relationship.
- Exempt data processors from requirements to 1) provide notice to individuals about collecting personal information; 2) seek consent for collecting, using, and disclosing personal information; and 3) act on requests to cease using or disclosing personal information, as data processors do not have a direct relationship with individual end-users — the relationship remains with the data controllers.

We understand the Bill is no longer under active consideration and we encourage the Australian Government to pursue any necessary legal reforms through the Privacy Act Review process (see above).

Online Safety

In June 2021, Australia enacted the Online Safety Act.[39] The purpose of the Act is to "create a new framework for online safety for Australians" and to "create a modern, fit for purpose regulatory framework

[34] Optus notifies customers of cyberattack compromising customer information, September 22, 2022, https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack
[35] https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-exposure-draft.pdf
[36] https://www.accc.gov.au/focus-areas/inquiries-finalised/digital-platforms-inquiry-0
[37] See Explanatory paper: Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, October 2021, https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf
[38] BSA Comments on the Australian Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, https://www.bsa.org/files/policy-filings/12062021auonlinepriv.pdf
[39] Online Safety Act 2021, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6680

that builds on the strengths of the existing legislative scheme for online safety."[40] BSA filed comments on the legislation when it was still before Parliament primarily urging that the legislation focus on high-risk consumer content delivery platforms and to exclude from the scope of coverage enterprise software solutions, including cloud computing services.[41]

The final legislation did not exclude low risk enterprise solutions and BSA has since participated in an intense collaboration with several other industry associations and dozens of companies to develop the Industry Codes (Codes) called for under Division 7 of the Act.

- Social Media Services
- Relevant Electronic Services (communications services, such as texts, emails, etc.)
- Designated internet services (websites and apps)
- Internet search engine services
- App distribution services
- Hosting Services
- Internet carriage services
- Manufacturers, suppliers, and those who maintain or install equipment[42]

The Codes are designed to guide companies involved in the following online industry sections to develop, implement, and enforce policies and procedures to deal with harmful content online ranging from illegal content such as child sexual abuse material and pro-terror content to legal content such as depictions of drug use and violence. A second set of Codes are to be developed to address how the industry sections handle legal content that is not appropriate for children or adults who do not wish to be exposed, such as online pornography or other "adult" content.

In a Position Paper published in September 2021, the eSafety Commissioner set out guidance and expectations for the industry as they development the codes.[43] The industry associations leading the Codes development process, including BSA, published a set of Draft Industry Codes for public comment on September 1, 2022.[44] The public consultation ended on October 2, 2022, and submissions are available on the Associations' website.[45] BSA and our partner associations are now compiling input received from the public consultations and implementing final adjustments to the Codes before submitting them to the eSafety Commissioner for registration. If the eSafety Commissioner is not satisfied with the Codes, she may initiate procedures to develop and impose industry standards.[46]

The objectives of the eSafety Commissioner and the Online Safety Act, to create incentives and mechanisms to reduce harmful online material, are unassailable. However, the Online Safety Act, especially the sections relating to the Codes, is overly broad, including industry sections as disparate as consumer facing social media services and mere conduit internet carriage services. The current draft Codes are the result of months of discussions with a very wide range of industry interests and attempt to recognize distinctions within the industry that are not well defined in the Online Safety Act. BSA has worked to ensure that the Codes reflect a dual reality that enterprise software services, such as hosting service providers and services designed for business-to-business purposes present both a relatively low risk of disseminating harmful content to the public and have significant technical, legal, and contractual limitations on whether and how such service providers are able to address instances of harmful content on their services. In many cases, the responsible parties must be the service providers' enterprise

[40] Online Safety Bill 2021, Explanatory Memorandum, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6680_ems_3499aa77-c5e0-451e-9b1f-01339b8ad871/upload_pdf/JC001336%20Clean4.pdf;fileType=application%2Fpdf
[41] BSA Comments to the Online Safety Bill 2021 Committee Inquiry, March 2, 2021, https://www.bsa.org/files/policy-filings/03022021ausonlinesafetycmte.pdf
[42] Online Safety Act Section 135.
[43] Development of industry codes under the Online Safety Act: Position Paper – September 2021, https://www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf
See also eSafety Commission Industry codes site, https://www.esafety.gov.au/industry/codes#esafety-position-paper
[44] Online Safety Codes site, https://onlinesafety.org.au/
[45] https://onlinesafety.org.au/submissions/
[46] Online Safety Act, Division 7, Subdivision D-Industry Standards

customers that have the direct relationship with individuals such as employees, customers, or the general public, rather than the enterprise service provider itself.

While the process continues underway, it will be important to carefully monitor the implementation of the Online Safety Act and the development of the industry codes or standards to ensure that the effects do not unnecessarily restrict the ability of BSA members to provide cutting edge enterprise software solutions to Australian businesses and organizations.

B. Brazil

Overview/Business Environment

Although Brazil has taken positive steps to improve market access for cloud service providers, the overall market environment in Brazil remains challenging.

Market Access

Concerns about privacy and security have been used to justify some market access barriers for foreign software companies. This situation may, paradoxically, increase risks of security vulnerabilities and decrease Brazilian consumers' confidence that their personal data will be appropriately protected. In this regard, we continue monitoring the ongoing discussions about the about a National Cybersecurity Strategy, which have been led by GSI (the Cabinet for Institutional Security of the Presidency of the Republic), to ensure future cybersecurity regulations don't inadvertently create market access barriers.

***Personal Data Protection Legislation**:* The Brazilian Congress approved the Brazilian Personal Data Protection Bill (known in Brazil as LGPD) in August 2018, and the law effectively came into force in September 2020. Legislation authorizing the creation of the Data Protection Agency (DPA) was approved in July 2019 and its structure was detailed through a Decree published in August of 2020. One of the provisions of the LGPD that requires implementation by the DPA is the one addressing international data transfers. In particular, the DPA must implement several of the most important grounds for transferring data outside Brazil, including issuing adequacy determinations, approving standard contractual clauses, and approving global corporate rules (akin to Binding Corporate Rules). To ensure legal certainty, BSA has requested that the Brazilian issue interim guidance confirming that companies may continue to responsibly transfer data internationally based on global best practices that are consistent with the overall LGPD objectives.[47] To date, this guidance has not issued.

Data and Server Localization Requirements: The first Guidelines on Government Procurement of Cloud Services were issued in late 2018 and a newer version was issued in late August 2021 still including server and data localization requirements that will negatively impact the procurement of cloud computing services by all federal agencies.[48] The latest version of the Guidelines adequate the language to the LGPD and add new concepts such as "cloud broker". BSA submitted comments on first draft guidelines urging Brazil to remove the localization requirements. However, Brazil did not adopt these recommendations, and the final Guidelines include the localization requirements.[49]

Copyright and Enforcement

The Brazilian Ministry of Citizenship is considering amendments to the current Brazilian Copyright Law. In July 2019, stakeholders were invited to comment on whether amending the law is necessary, and, if so, which provisions should be modified or added to the current law. BSA submitted comments suggesting the law be amended to add sections codifying notice and takedown, as well as provisions clarifying the permissibility of reproduction of content used for information analysis or research. The Ministry of Citizenship had announced it plans to issue a draft of the revised copyright law for public comment in early 2020, however, there have been no developments and the draft of the revised law is unlikely to be issued in 2021. According to the most recent data, the rate of unlicensed software use in Brazil is 46 percent. This represents a commercial value of approximately US$1.7 billion in unlicensed software.[50] This is a far greater value of unlicensed commercial software than what has been measured

[47] https://www.bsa.org/files/policy-filings/09092020bsagdalgpdimplement.pdf.
[48] https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-5-de-30-de-agosto-de-2021-341649684
[49] Comments available at: https://www.bsa.org/~/media/Files/Policy/Filings/CommentsBSA_CloudProcurement.pdf
[50] Data on the rates of unlicensed software use and commercial values are taken from the 2018 BSA Global Software Survey at http://www.bsa.org/globalstudy. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2017 in more than 100 markets. The study includes a detailed discussion of the methodology used.

throughout the rest of the region. Although recently improvements have occurred, BSA's enforcement programs in Brazil still suffer from a very slow court system that prevents cases from being settled quickly and efficiently.

Notice and Takedown: Notice and Takedown is a process not currently codified by the Brazilian Copyright Law. Although the Brazilian Superior Court of Justice has once ruled that notice and takedown principles apply to assess internet provider liability, the ruling does not address the issue completely, and due to the nature of the Brazilian legal system, it is unclear how, if at all, the ruling would apply to other cases. It is, therefore, important that the issue by codified and the relevant provisions added to the revised Brazilian copyright law. We also noted in our comments that it is very important to ensure that the appropriate safe harbors are in place to protect ISPs from liability for copyright infringing content posted by third parties, and that such safe harbors should not be conditioned on any obligation by the ISP to monitor or filter infringing activity.

Information Analysis*:* In legal systems that do not have a flexible fair use provision, which is the case of Brazil, there can be some uncertainty about the permissibility of reproductions used for information analysis or research. It is therefore extremely important to create a specific data analysis provision to avoid any questions about the non-infringing nature of data analysis uses. This will help foster innovation through the continued use of data analysis for innovation purposes, without potential barriers that the threat of potential legal sanctions for copyright infringement could pose.

Compliance and Enforcement: BSA's enforcement program is based on civil cases brought against enterprises that use unlicensed or under-licensed software. In addition, BSA promotes voluntary compliance measures, such as effective, transparent, and verifiable SAM procedures, where enterprises conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed. BSA's efforts in Brazil also include a comprehensive educational communication campaign. This campaign is conducted exclusively online and is a collaboration with the local software association, ABES (Associação Brasileira das Empresas de Software). The campaign is meant to drive awareness of the risks of using unlicensed software.

BSA's relationship with the enforcement authorities in the past years improved due to increasing public awareness of IP-related issues. While civil cases continue to encounter court backlogs, judges in several major jurisdictions are responding well to requests for trials. Additionally, *ex parte* measures are available when necessary, and the courts order companies to cease using unlicensed software.

The Superior Court of Justice has reaffirmed earlier rulings that it is insufficient to simply order companies to pay the license fee they would have had to pay in the first place for the software they have been using without authorization. Instead, fines of multiple times the market value of the unlicensed software are being imposed. This provides greater deterrence in those cases that proceed to final judgment, but also sends a message to companies that they should not wait to be sued before legalizing their software use.

While these are positive trends, there is room for improvement. The Brazilian court system is generally slow. For example, in many instances, it may take anywhere from six to twelve months for an expert report to be ratified by the Court, allowing lawsuits to continue. In addition, Brazilian courts in certain cases continue to require high fees for forensic experts who conduct searches and seizures. Finally, court cases filed in the northern, northeastern, and midwestern regions of the country present additional challenges due to local judges' lack of IP expertise and the low number of qualified experts to perform inspections in those locations. The Ministry of Justice's National Council to Combat Piracy and Intellectual Property Crimes (CNCP) is the main governmental entity responsible for the central coordination and implementation of Brazil's national anti-counterfeiting and piracy campaign. It is critical that the CNCP be properly funded.

C. China

Overview/Business Environment

BSA members and other international technology providers face a particularly challenging commercial environment in China.[51] BSA members recognize the importance of resolving longstanding bilateral challenges with China and have seen first-hand the challenges and evolution of China's policies in the technology sector. BSA supports continued efforts by the US and Chinese governments to achieve mutually beneficial solutions to these challenges.

China continues to present major market access challenges to BSA members. In 2017, the Government of China enacted the Cybersecurity Law,[52] which impose onerous cross-border data transfer restrictions and data localization requirements. Since that time, Chinese efforts to regulate cross-border data transfers have accelerated. This is reflected in initiatives such as the MIIT 14th Five-Year Big Data Industry Development Plan,[53] the Digital Service Trade Five Year Plan,[54] and its Digital Economy Five Year Plan.[55] These plans focus on issues such as "monitoring of sensitive data leakage, illegal cross-border data flow" and promoting China-style data transfer restrictions via pilot programs in other countries. China will also continue work on its draft Network Data Security Administrative Regulation[56] and the Security Assessment Measures for Cross-border Data Transfers[57] *(Translation here.*[58]*). China will also continue to work on* implementation and enforcement of the Data Security Law (DSL),[59] the Personal Information Protection Law (PIPL),[60] the Data Management Rules for Automotive Applications,[61] and the Internet Medical and Health Information Security Management Specifications[62]- all of which came into effect in the last 12-18 months. In this same timeframe, China issued the Platform Economy Opinions[63]; the June 24, 2022 *Cybersecurity Standard Practice Guideline — Specification for Security Certification of Personal Information Cross-Border Processing Activities by the National Information Security Standardization Technical Committee*; and the June 30, 2022 draft *Provisions on the Standard Contract for Personal Information Cross-Border Transfer*.

BSA urges the US Government to continue to engage closely with the Government of China to make meaningful progress on the range of issues mentioned in this submission to ensure fair and equitable market access for BSA members and other US and foreign companies.

Market Access

Cloud computing, despite being identified as an area of strategic development in China, remains largely off limits to foreign Cloud Service Providers (CSPs) due to several policy challenges, including equity caps, investment restrictions, and connectivity requirements. These challenges are exacerbated by

---

[51] AmCham China: China Business Climate Survey Report, at: http://www.amchamchina.org/policy-advocacy/business-climate-survey/; *See generally,* BSA Cloud Scorecard – 2018 China Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_China.pdf.
[52] *Cybersecurity Law of the People's Republic of China*, November 11, 2016 (CSL) (Chinese) at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Unofficial English translation at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
[53] https://wap.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2021/art_c4a16fae377f47519036b26b474123cb.html
[54] https://www.scmp.com/tech/policy/article/3153196/china-pursue-digital-trade-expansion-under-new-five-year-plan-cross
[55] https://english.www.gov.cn/policies/latestreleases/202201/12/content_WS61de9a35c6d09c94e48a385f.html
[56] http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm
[57] http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm
[58] https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/
[59] https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/
[60] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/
[61] http://www.gov.cn/xinwen/2021-05/12/content_5606075.htm
[62] https://mp.weixin.qq.com/s/dc7gd8EIPJzT9OD4Wp91pw
[63] https://www.chinamoneynetwork.com/2022/01/21/china-issues-new-rules-regulating-internet-giants-and-platform-economy

market entry barriers, such as restrictions on the ability to engage in cross-border data transfers and requirements to localize computing infrastructure.

BSA welcomed the commitments negotiated by the United States and China in relation to cloud service purchases in the so-called “Phase One” trade agreement. The Phase One purchasing commitments included payments for the use of IP, which encompasses royalties for the computer software. More critically, the Phase One agreement contains purchasing commitments that cover “cloud and related services”, a critical area of economic activity for US services exporters that have faced a challenging investment and export environment for these services for many years. Covered services include: (1) data hosting, processing, and related services; (2) telecommunication services; (3) computer services; and (4) information services. At a time when both the US and Chinese economies are relying increasingly on cloud-enabled business environments (including via remote work, health, and learning) to respond to the COVID-19 crisis, China and the United States have a shared interest in the fulfillment of commitments relating to computer software, as well as cloud and related services. BSA urges both countries to continue working towards fulfillment of those important commitments.

Restrictions on Cross-Border Data Transfers

The Government of China has put in place several laws and regulations restricting the transfers of data across borders and forcing data to be stored locally including the CSL. For BSA members that provide cloud computing services or that rely heavily upon cloud computing for their business operations, these restrictions create an uneven playing field — advantaging domestic businesses that already have local infrastructure and preventing foreign businesses from operating efficiently or at all.

***Data Security Law*:** The Data Security Law (DSL), enacted on June 1, went into effect on September 1, 2021. The DSL (a) requires the State Internet Information Department to draft rules for all “other data handlers” (i.e., not just CII operators) to restrict those other handlers’ exportation of “important data”; (b) applies to “[any person] handling important data”; (c) requires the State to create a “categorical and hierarchical system for data protection” as well as “catalog of” for “important data”, and to assess the “importance” of data based on broad criteria relating to: economic development, social development, national security, the public interest, and the lawful rights and interests of citizens or organizations; (d) authorizes each region and department to set a “catalog of important data” within that region and in corresponding industries and sectors; and (e) requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of “important data”

Following the swift enactment of the DSL, the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology have developed guidelines to establish the requisite frameworks for data categorization and classification under the DSL. As China works on classifying the scope of “important data” and other data classifications under the auspices of the DSL, it will be important to ensure that those categories of classification are not overbroad and do not automatically and improperly sweep in data categories, such as intra-company data transfers (e.g., of internal business and operational data) that are otherwise protected.

***Cybersecurity Review Measures*:** In February 2022, Cybersecurity Review Measures came into effect. The Measures, which are primarily targeted at Chinese technology companies seeking an overseas IPO listing, require both Critical Information Infrastructure operators as well as data processors to go through a cybersecurity review. Among the new risk assessment criteria proposed in the draft Measures, they include:

- data security risks involving core data, important data, or a large amount of personal information being stolen, disclosed, destroyed, or illegally used or transferred across borders;
- critical information infrastructure, core data, important data, or a large amount of personal information will be affected, controlled, or maliciously used by foreign governments after listing abroad

***Personal Information Protection Law*:** The Personal Information Protection Law (PIPL)[64] took effect on November 1, 2021. Of particular concern are requirements for *ex ante* security assessments that impact data transfers that global companies have long engaged in for their daily business operations. The PIPL also raises the following concerns:

(1) data localization requirements for "personal information" (PIPL Art. 40) and highly restrictive data transfer provisions for "personal information" (PIPL Arts. 38-40);

(2) lack of definition or overbroad scope for key concepts that implicate data localization requirements and data transfer restrictions, including what constitutes a "justified need," or a "large volume [of data]" (PIPL Art 40);

(3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localization and data transfer provisions noted above (PIPL Art. 38(1), 40);

(4) proposed data transfer "standard contracts" that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3));

(5) the absence from the PIPL of other internationally recognized data transfer mechanisms, such as intra-corporate binding rules, trustmarks, and regional certifications (PIPL, Art. 38);

(6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39); and

(7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43).

BSA and 31 other global associations raised these concerns in a letter submitted to China during the drafting process, but the concerns were not addressed.[65]

***Measures for Security Assessment of Cross-Border Data Transfers*:** On September 1, 2022, the Measures for Security Assessment of Cross-Border Data Transfers of the Cyberspace Administration of China (CAC) took effect. These security assessment measures are required only for a limited subset of companies engaging cross-border data transfers – specifically:

- A critical information infrastructure operator or a personal information processor based in China (akin to a "data controller" under the GDPR) that processes personal information for 1 million or more persons;
- A transferor of "important data";
- A processor of the personal data of more than 1 million individuals; a transferor of personal information of more than 100,000 individuals; or a transferor of sensitive personal information of more than 10,000 individuals. The latter criteria apply to the period beginning on January 1 of the preceding calendar year.

CAC also issued the Guidelines on Application of Security Assessment of Cross-border Data Transfers (First Version) on August 31, 2022.[66]

---

[64] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
[65] Multi-association Letter on Draft Personal Information Protection Law and Draft Data Security Law, June 2, 2021, at: https://www.globaldataalliance.org/downloads/en06022021gdachinadslpip.pdf
[66] The Guidelines on Application of Security Assessment of Cross-border Data Transfers require a person making a security assessment application to prepare:

- a certified copy of its unified social credit code certificate;
- a certified copy of its legal representative's ID card;

***CAC Draft Standard Contracts for Outbound Data Transfers*:** On July 28, 2022, BSA joined a multi-industry letter[67] in response to the Cyberspace Administration of China's draft Measures on Standard Contracts for the Export of Personal Information.[68] GDA recommended that the Measures should: (1) not impose greater restrictions on data transfers than necessary; (2) afford equal treatment to Chinese and foreign enterprises, services, and technologies; and (3) be administered in a uniform, impartial, and reasonable manner with a view to ensuring non-discriminatory and streamlined approvals. The GDA also recommended that the CAC seek to:

(a) Improve alignment with international best practices: China's Standard Contract Provisions should reflect international best practices, and should be revised for greater alignment and interoperability with standard contractual clauses (SCCs) under the EU General Data Protection Regulation (GDPR), such as by aligning definitions and transfer scenarios with the EU GDPR SCCs.

(b) Adopt Document Retention Requirements: Article 3 requires filing of standard contracts with CAC. To align with the international practice, we would propose that CAC instead require data controllers to retain the original agreement and produce a copy to CAC regulators upon request.

(c) Reevaluate disqualifying conditions: Article 4 conditions for disqualifying companies from using Standard Contract Provisions do not align with any known international practice, including those relating to critical information infrastructure, as well as volume limits for personal and sensitive personal data. Accordingly, we recommend that CAC (1) revise disqualifying thresholds (thresholds required for CAC security assessments are very low (representing transfers covering 0.07% [seven hundredths of 1 percent] and 0.0007% [seven 10,000ths of 1 percent] of China's population over a 12-24 month period); and (2) revise overbroad exclusions (given that China's TC260 definition of "critical information infrastructure" sweep in a wide array of computing equipment typically used for ordinary and non-sensitive international business transactions)

- a Power of Attorney appointing an agent handling the application related matters – a template of this is included in the Guidelines;
- a certified copy of the appointed agent's ID card;
- a completed Application Form for Security Assessment of Cross-border Data Transfers – a template of this is included in the Guidelines;
- a certified copy of the agreements or other legal documents with the overseas data recipients. (In practice, it may be preferable to fulfill this requirement by submitting a copy of a China-approved standard contract (if and when they are published. However, the viability of this approach remains to be seen);
- a Report of Self-assessment of Risks in Cross-border Data Transfers – a template of this is included in the Guidelines (including an explanation, and risk/compliance/mitigation analyses for each transfer); and
- other supporting documents and materials

[67] GDA, Global Industry Statement on Draft China Standard Contract Provisions, https://globaldataalliance.org/wp-content/uploads/2022/08/en07282022gdachdftcontractprov.pdf

[68] Article 38 of the Personal Information Protection Law (PIPL) introduces standard contracts as a cross-border data transfer mechanism, noting that such contracts may be used only by processors that:

1. are not critical information infrastructure operators;
2. handle personal information for fewer than 1 million persons;
3. have transferred personal information for fewer than 100,000 persons since January 1 of the prior calendar year; and
4. have transferred sensitive personal information for fewer than 10,000 persons since January 1 of the prior calendar year.

Processors must file standard contracts (and Data Protection Impact Assessments) with provincial CAC authorities within 10 business days of the effective date of the contract.

Standard contracts must contain, among other things: (1) basic information on the parties, (2) the purpose, scope, category, sensitivity and volume of data transfers, (3) the respective obligations and liabilities of the transferor and transferee, (4) information on the laws of the destination country, (5) protections afforded to data subjects, and (6) provisions regarding termination, liability and dispute resolution.

Data Protection Impact Assessments must evaluate: (1) the purpose, scope, and method of processing by the processor and overseas recipient; (2) risks of leakage of personal information and whether data subjects have legal means to safeguard their rights and interests; (3) the impact of personal information protection policies and laws in the overseas country on the performance of the contract (Art 5).

(d) Refine transfer impact assessment procedures: Article 5 of the Standard Contract Provisions contains prescriptive review requirements relating to – among other things – the volumes, scope, sensitivity, and categories of information (categories that have not yet been clearly defined in Chinese law), as well as the laws and practices of the recipient's home country; regional or global organizations to which the country or region is a member; and binding international commitments made. It would be helpful for CAC to look for ways to streamline and rationalize these requirements, including by citing to neutral and factual legal summaries, and by developing a list of categories of low-risk data transfers for which no formal, or a less detailed assessments would be required.

(e) Clarify that parties may tailor the language of contracts to specific circumstances

Cybersecurity Law: In November 2016, the National Peoples' Congress passed the Cybersecurity Law (CSL), which went into effect in June 2017.[69] The Cyberspace Administration of China (CAC) and other authorities continue to issue measures and standards to implement the CSL. Many of these measures leave important issues vague and unclear (e.g., the definition of critical information infrastructure (CII) or "important information") or appear to expand the scope of the law — exacerbating the negative impact of these rules on the software industry. Broadly speaking, the impact of the CSL and related data regulations is to require that important information and personal information collected in China (by CII operators and others) must be held in-country.

Procurement

In January 2020, the Cybersecurity Review Measures became effective. A revised version of the Measures came into force in February 2022. Under the measures, all "network products and services" purchased by CII operators will be subject to a cybersecurity review by the CAC. The CAC can unilaterally trigger a review that can potentially be a disguised barrier to trade and market access, given the lack of transparent and object criteria and the wide discretion afforded to governmental authorities to deny approval. BSA and its members remain concerned that the measures and the review process will be used as a disguised market access barrier to foreign products and services.

Foreign Direct Investment Restrictions

US businesses seeking to operate in China are subject to a range of foreign direct investment restrictions, including equity caps, and in-country hosting requirements, as well as challenging processes for obtaining licenses and other prerequisites for entering the market. These restrictions are particularly acute for cloud computing services. For example, under China's Telecommunications Service Catalog and related measures,[70] China incorrectly classifies a wide range of technologies and services as value-added telecom service (VATS) or basic telecom service (BTS), when in fact they are computer or business services that utilize the public telecommunications network as a method of delivery. For example, the catalog classifies cloud computing, content delivery networks, and online interactive platforms (called information services) as telecommunications services. Foreign firms that provide value-added services in China can only operate through joint ventures, of which they may own no more than 50 percent for VATS and 49 percent for BTS. In short, because of the update, foreign firms that provide a range of IT services are now subject to explicit limitations on market access, which also apply indirectly to local partners of joint ventures.

Standards and Technical Regulations

[69] CSL
[70] *Classification Catalogue of Telecommunications Services (2015 Edition)*, December 28, 2015 (Chinese), as revised in June 2019, at: http://www.miit.gov.cn/n1146290/n4388791/c69928928/content.html.

Cybersecurity Classified Protection Scheme: In May 2020, China posted the final version of the Cybersecurity Classified Protection Scheme (CCPS),[71] a de facto cybersecurity protection baseline for network operators and a universal compliance framework for the CSL. The CCPS is a continuation of the Multi-level Protection Scheme (MLPS).[72] Like the MLPS, the CCPS ranks the importance of network and information systems, based on their importance to China's national security, social order, public interests, and the legitimate interests of individuals and organizations and unnecessarily excludes access to foreign technology to the networks of moderate to high national importance — constituting a significant point of concern for the industry at large. The Government of China continues to release supporting standards and guidance on implementing the CCPS. For example, the September 22, 2020 "*Guiding Opinions on Implementing CCPS and CII Protection Scheme*"[73] which includes new concepts such as supply chain security and applies the CCPS to critical infrastructure protection. The CCPS came into effect on November 1, 2020.

Encryption: The China National Information Security Standards Technical Committee (TC-260) continues to release a myriad of draft cybersecurity standards involving encryption for public comment. A consistent and worrying trend exhibited by these standards is the extent to which they can be used to make it more difficult to participate in China's market, by creating a basis for favoring locally developed products over those developed outside of China. Such changes to algorithms or encryption mechanisms create technical barriers to trade and undermine interoperability.

In late 2019, the Government of China enacted the Cryptography Law.[74] BSA is concerned with the law for several reasons. First, while the updated Law states that commercial cryptography would not be subject to import licensing or export controls, the subsequent draft implementation regulations released suggest otherwise. Certification requirements for commercial cryptography are also being introduced. This overall regulatory framework could potentially restrict foreign competition in commercial cryptographic products. In implementation, it will also be important to avoid unwarranted source code disclosure requirements and to ensure that safeguards protect any trade secrets or other proprietary information. It is necessary for the USG to address the serious concerns of the software industry regarding privacy, security, and trade secret protection.

Intellectual Property

Compliance and Enforcement: BSA and its members have had some success with China's IP Courts and tribunals. Unfortunately, we are observing capacity issues as the limited resources of those IP Courts and tribunals are tested against the growing backlog of cases. Given the positive experience BSA and our members have had with the existing system, BSA encourages the Government of China to establish additional specialized courts and provide more resources to the existing courts and tribunals.

Significant hurdles to effectively address the use of unlicensed software in China remain. In civil cases, most courts have relaxed excessively high burdens for granting evidence preservation orders, but others remain highly reluctant to issue such orders. Courts should also increase the amount of damages awarded against enterprises found using unlicensed software. China also needs to increase statutory damages beyond those currently proposed in the draft amendments to the Copyright Act.

The Criminal Case Transfer Regulations do not adequately address existing challenges to the effective transfer of administrative cases to criminal investigations and prosecution authorities. Some

---

[71] *Cybersecurity Classified Protection Regulations (Draft for Comment)*, June 27, 2018 (CCPS) (Chinese), at: http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html?from=timeline&isappinstalled=0.
[72] *Administrative Measures for the Multi-level Protection Scheme of Information Security*, June 22, 2007 (MLPS) (Chinese), at: http://www.mps.gov.cn/n2254314/n2254409/n2254431/n2254438/c3697388/content.html.
[73] *Guiding Opinions on Implementing CCPS and CII Protection Scheme,* September 2020 (English) at: https://www.mps.gov.cn/n6557558/c7369310/content.html.
[74] *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://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html#:~: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.

enforcement authorities have interpreted the regulations as requiring proof of illegal proceeds, rather than allowing transfer upon reasonable suspicion. Administrative authorities, however, do not employ investigative powers to ascertain such proof. We recommend that the regulations be updated to expressly include the “reasonable suspicion” rule.

D. European Union

Overview/Business Environment

Over the past several years, the European Union has modernized its digital economy regulatory and policy framework relevant to software and data service providers, in particular with regards to privacy, cybersecurity, data transfers, and copyright. The new European Commission is actively pursuing an assertive digital policy agenda, guided by at times competing ambitions to promote Europe's "digital sovereignty" while pursuing "open strategic autonomy." The European Strategy for Data adopted in February 2020 clearly endorses that the EU will maintain an open, but assertive approach to international data transfers and pledges that the EU will continue to address unjustified obstacles and restrictions to data transfers in bilateral discussions and international fora. However, calls for data localization or for measures that seek to ensure EU organizations are immune from third countries' extraterritorial legislation continue to have traction at EU level and in some Member States, especially in the wake of the CJEU Schrems II decision and in light of the increased reliance on global digital technologies during the pandemic. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, and in harnessing the value of data, some of the measures considered, including in the areas of data privacy, cybersecurity, data governance, and cloud resilience in the financial sector (the so-called the 'Digital Operational Resilience Act' (DORA)), may constitute *de facto* market access barriers or dramatically hinder the ability of US organizations to move data across border.

The EU-US Trade and Technology Council can be an important asset to the transatlantic digital policy debate. BSA encourages both sides to use the TTC to exchange on common priorities and seek joint outcomes on *inter alia* Artificial Intelligence, data governance and international data transfers.

Market Access

As the EU co-legislators develop and implement new proposals, BSA asks that the US Government closely follow these developments, work intensively to protect existing transatlantic data transfer mechanisms, and push back against policies that pose the most significant market access barriers.

Cross-Border Data Transfers: Measures that impede the transfer of data across borders impose substantial burdens on US service providers and negatively impact US jobs. European authorities are historically focused on data transfers to the United States. The Commission has recently applied similar levels of scrutiny to the United Kingdom and the Republic of South Korea as both Third Countries sought an adequacy decision, but has not yet done so to data transfers relating to other markets such as China or Russia. It also has yet to evaluate existing adequacy decisions granted to markets including Canada, Argentina, Israel and Uruguay.

On July 16, 2020, the European Court of Justice in the Schrems II case invalided the EU-US Privacy Shield agreement. The Court also confirmed the validity of Standard Contractual Clauses (SCCs) which remain one of the main mechanisms under EU law to legally transfer personal data from the EU to third countries, especially in the absence of an adequacy decision. However, the Court also ruled that controllers and processors are required to verify, on a case-by-case basis, whether the law of the third country where the recipient is based ensures an "essentially equivalent" level of protection of the personal data transferred.

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

The *Schrems II* case led to an increase in decisions by local Data Protection Authorities (DPAs) on the subject of data transfers. For example, in a September 2022 decision, the Danish DPA ordered the Aarhus municipality to cease transferring data to the United States pending certain internal changes. This decision followed the same DPA's August 2022 Helsingør decision, which imposed similar cross-border data transfer restrictions. In a separate September 2022 decision, the Danish DPA also declared that certain US-based data analytics software solutions "cannot be used legally without additional safeguards." These

rulings follow other DPA rulings on the use of digital tools that implicate US-EU data transfers in: (1) Austria (Oct. 2021, April 2022), (2) Germany (Berlin DPA) (3) Denmark (July 2022, Jan. 2022) (5) France (CNIL ruling), (6) Guernsey (DPA ruling), Italy (Garante June 23 ruling), and the Netherlands (Dutch DPA statement).

A New US-EU Data Privacy Framework: In October 2022, the United States the Biden Administration issued an Executive Order (EO) on Enhancing Safeguards For United States Signals Intelligence Activities,[75] which was first announced in March 2022.[76] The EO creates new safeguards on US signals intelligence activities, establishes a new redress mechanism, and enhances US oversight of signals intelligence. The EO will form the basis of an adequacy decision by the European Commission, which would create a successor agreement to the Privacy Shield and facilitate data transfers across the Atlantic.

EU Standard Contractual Clauses for Data Transfers: The European Commission released a new set of SCCs in June 2021. The new set of SCCs contains general clauses that will be common to all future SCCs and in addition to the general clauses, controllers and processors should select between four different modules the most applicable to their situation. This is meant to allow the parties to tailor their obligations under the standard contractual clauses to their corresponding role and responsibilities in relation to the data processing at issue. The final SCCs anticipate that companies will assess the laws of the country to which data is transferred – and now specify that both the laws and "practices" of that country are relevant to such an assessment. Notably, the SCC implementing decision recognizes that companies may consider the absence of government access requests in their sector and their own practical experience in making these assessments. Paragraph 20 states that: "different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer." The final SCCs also make two meaningful changes on government access concerns by: (1) narrowing the circumstances in which notification to supervisory authorities is required, and (2) deleting the draft language that would have required companies to "exhaust all available remedies" to challenge a request. In June 2022, the European Commission released its long-awaited Q&A document on the practical use of SCCs (both on the "Article 28 SCCs" and the "transfer SCCs"). The purpose of these Q&As is to provide practical guidance on the use of the SCCs to assist stakeholders with their compliance efforts but does not constitute legal advice.[77]

The implications of the Schrems II ruling have had significant bearing on US companies that operate in Europe and / or act as service providers for customers in Europe. The ruling added significant uncertainty with regards to the robustness and durability of the SCCs, a mechanism used by 90 percent of companies that transfer data internationally to some 180 countries. It is hoped that the new US-EU Data

[75] White House, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities (Oct. 2022), at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

[76] White House, Announcement of Transatlantic Data Privacy Framework (March 2022), at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[77] On the specific aspect of use of SCCs for international data transfers, the Q&A document does not provide more information on how companies should conduct "transfer impact assessments" than the one already contained in the SCCs themselves. Moreover and unhelpfully, for the additional safeguards that should be included in the SCCs in case the parties allocate a "negative assessment" to the Third country to which the data will be transferred, the document refers to the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data as the source for practical information for additional safeguards to be included in the SCCs. On a more positive note, the Q&A document stresses that the data importer IS NOT contractually required to challenge each request for disclosure it receives from a public authority in a Third country. However, the data importer has to review whether the requests it receives are lawful under the applicable domestic legal framework. If the importer considers that there are reasonable grounds to consider the request unlawful, it should make use of the procedures available under its domestic law to challenge the request. If the data importer has challenged a request and considers that there are sufficient grounds to appeal the outcome of the procedure in first instance, such appeal should be pursued.

Privacy Framework and the accompanying EU adequacy decision will help ameliorate some of this uncertainty.

Cybersecurity Certification Scheme for Cloud Services (EUCS): In September 2022, three German Federal Ministries (Interior; Economics and Technology; and Transport, Building and Urban Affairs) sent a joint letter to the European Commission urging that the discussions on so-called "immunity requirements" under the EUCS should not be conducted in the standardization bodies of the European Union Agency for Cybersecurity (ENISA), but in a Council working group, as these are political and not technical issues. This is a positive development, as currently the EUCS, being drafted by ENISA, involve major possible implications for the Cloud Service Providers which go beyond the Cyber Resilience Act. Among those implications are the requirements on immunity of Cloud Service Providers with regard to non-EU law and sovereignty requirements (including data localisation requirement restricted to EU territory). German Ministries letter follows extensive engagement by BSA/GDA and governments across the EU and third countries. This would have an impact on all sectors relying on cloud computing.

EU Data Act: BSA is concerned with drafting ambiguities in the draft EU Data Act relating to cross-border data transfers. To mitigate interpretative challenges for EU judicial and administrative authorities, we would recommend that the Commission seek to clarify the ambiguity and breadth of the text of Article 27.1 of the Data Act. Such legislative clarification could help forestall alternative interpretations that data transfer or access must be blocked on the basis of a wide and undefined scope of potential "conflicts" with EU law or member state law. Indeed, if data transfer or access were halted in this unpredictable and broad manner, it could raise questions regarding the EU's compliance with its international obligations and impede the future ability of EU and foreign entities to engage in cross-border commerce, R&D, and other activities.

France's Cloud Strategy: In July 2021, the French Government formally approved its Cloud Strategy for the public sector ("doctrine cloud de l'Etat"), which was announced earlier this year. The strategy aims at addressing the perceived lack of protection against cybersecurity threats and trust concerns related to Third Countries' governments access to data, and has been presented by government officials as a direct response to concerns highlighted by the CJEU in the Schrems II ruling.

While cloud services are essential to modernize the Government and the administration, the French government also suggests that when the administration chooses to rely on commercial solutions from the private sector (especially from French and European providers), they should bear in mind data protection principles and the localization of data in Europe.

The strategy revolves around the following axes:

- The strategy aims at developing a "cloud culture" by instituting automatic reliance on cloud services for new projects within the administration, and emphasizes that the use of commercial cloud services should be aligned with Gaia-X principles;
- When using a commercial cloud service to host/process sensitive data, the service will have to comply with 'Trusted Cloud' requirements, meaning obtain a certification from ANSSI (or an equivalent European qualification) and be immune to any extraterritorial regulation. At this stage the strategy document itself does not mention specifically where the data needs to be localized (in France or in the EU); early announcements mentioned that new types of partnerships, for instance through technology licensing so that foreign technologies licensed to EU companies, could also be eligible to that "Trusted Cloud label;
- The term "sensitive data" is only loosely defined as either personal data, economic data, or data related to the public administration.

Many questions remain which is raising some concern for non-EU providers. The Government has reiterated its commitment to this approach but has yet to offer full clarity on a number of important aspects of definitions and implementation of the Strategy.

Data Transfers in Trade Agreements with Third Countries: In February 2018, the European Commission released data transfer provisions for trade agreements, seeking to address concerns from Member States, trading partners, and industry that EU Free Trade Agreements (FTAs) suffer from a lack of language on the international data transfers. This position is a positive step towards the EU endorsing binding trade commitments specifically focused on cross-border data transfers. However, it raises concerns due to its self-declaratory nature and potentially unlimited scope of exception with regards to privacy safeguards. At present the European Commission tabled this proposal in ongoing FTA negotiations with Australia and New Zealand, in which it is confronted to more advanced CP-TPP data transfer provisions. The EU also tabled its language at the WTO Joint Statement Initiative talks on e-commerce.

In January 2021, the EU reached an agreement with the UK on digital trade provisions in the Trade and Cooperation Agreement governing EU-UK trade post-Brexit. The agreement translates for the first time in a trade agreement the EU's commitment to ensuring cross-border data transfers to facilitate trade in the digital economy. While the agreed upon language on public policy exception remains further apart from more progressive provisions in USMCA or CP-TPP, it is considered by the European trade community as a positive step forward. Indeed, throughout 2020, several groups of Member States have repeatedly called on the Commission to adopt a high-level of ambition on data transfers in the WTO e-commerce negotiations, even if it means diverging from the EU position as formally set by the negotiating directives. Similar letters have also called for an "open strategic autonomy" posture that preserves internal data transfers in order to support the bloc's digital growth ambitions. By adopting forward-looking data transfer provisions, the EU would be able to retain its influence on the multilateral stage and to continue to effectively push back against localization efforts in third countries. It would also bring it closer to its main trading partners—first and foremost the United States—and address some of the friction between trade and privacy following the CJEU Schrems II case.

Proposed e-Privacy Regulation: In January 2017, the European Commission published a Regulation aiming to update the EU's current e-Privacy Regulation (ePR), which regulates the confidentiality of communications and processing of personal data on terminal equipment. The scope of the proposed regulation is very broad, sweeping in any electronic communications service provided with the use of a public communications network, including over-the-top services and machine-to-machine communications (e.g., data transfers between Internet of Things devices). It also would apply extraterritorially, including in circumstances where processing is conducted outside the EU in connection with services provided within the European Union. The draft Regulation built around a consent-only processing model, risks contradicting key provisions of the General Data Protection Regulation ("GDPR"). BSA submitted comments, expressing concern about the wide-reaching and prescriptive rules included in the ePR and the narrow scope and number of exceptions.[78]

In October 2017, the European Parliament adopted its position on the draft Regulation. The Council has adopted its position in early 2021, including additional grounds for processing beyond the consent model for certain data categories, but largely maintaining the structure of the Regulation.

Trialogue negotiations between the European Commission, the European Parliament and the Council have begun in the Spring of 2021 and are ongoing. Not much progress has been achieved on the file, and BSA continues to express concerns on the structure of the proposal and on the very limited grounds for processing communications data.[79]

EU Cybersecurity Competence Centre: Following a proposal in September 2018, the EU Cybersecurity Competence Centre Regulation was formally adopted in May 2021. The regulation

[78] Comments available at: https://www.bsa.org/~/media/Files/Policy/Data/09202017BSAPositionPaperontheEUePrivacyRegulation.pdf.
[79] Comments available at: https://www.bsa.org/policy-filings/eu-bsa-policy-recommendations-on-the-eprivacy-negotiations. .

creates an EU Cybersecurity Competence Centre and Network (CCCN) aiming to ensure that Europe retains and develops essential cybersecurity technological capacities to protect critical networks and information systems, provide key cybersecurity services, and compete more effectively in the global cybersecurity market. As stated in the EU Cybersecurity Strategy released on 16 December 2020, "the CCCN should play a key role, with input from industry and academic communities, in developing the EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reduce dependence on other parts of the globe for the most crucial technologies." During the legislative process, BSA raised concerns with regards to the eligibility criteria of the CCCN in order to ensure that non-EU headquartered organizations and/or individuals would be eligible. The final language of Article 8 (3) reads as follows: "Only entities which are established within the Member States shall be registered as members of the Community." This language, coupled with a political willingness to support the emergence of a European domestic cybersecurity industry, could be interpreted to prevent subsidiaries of global companies from participating in the work of the Community and from benefiting from EU R&D funding instruments that will be governed by the Centre. However, the absence of a clear general definition under EU law of what it means for an entity to be "established" in the EU creates an uncertainty on whether a company that is headquartered outside of the EU, but that has one or multiple affiliates in Member States, is established in the EU and whether it is eligible to the CCCN.

EU AI Act: In April 2021, the EU issued a draft regulation setting out harmonized rules on artificial intelligence (AI), commonly referred to as the "AI Act" (notified to the WTO in November 2021). The stated goal of the AI Act is to foster an environment that protects people's safety and fundamental rights. Under the Commission's proposal, AI deemed to be high-risk would have to comply with requirements related to a range of issues, including data governance, human oversight, transparency, recordkeeping, and security. The Commission has identified a number of AI applications as high-risk, including biometric identification, credit scoring, management of critical infrastructure, access to education, job recruitment, essential private and public services, and law enforcement that may interfere with people's fundamental rights. High-risk AI systems would also have to undergo conformity assessment before being placed in the EU market.

In July 2022, the Czech Presidency issued a revised text for the AI Act. The Czech Presidency has stated that their ambition is to achieve a General Approach by December 2022. The compromise text introduces the following changes: (1) narrower definition of AI, which brings the definition closer to the OECD definition; (2) narrower high-risk use cases in Annex III; and (3) narrower classification of high-risk. However, the revised text continues to include General Purpose AI in the scope of the AI Act, regardless of its classification as high-risk or low-risk.

BSA supports the intention to structure the AI Act under a risk-based approach, and recommends that the EU co-legislators ensure that this approach is reflected in the final version of the AI Act. BSA has made the following four recommendations regarding the AI Act:

- Clarify and refine the scope and definitions of the proposal
- Ensure that the obligations for AI providers and users are outcome and process-based and reflect the nature of AI as a service
- Allocate responsibility between AI providers and users in a manner that reflects the diverse AI ecosystem and ensures legal certainty
- Design a governance and enforcement system that fosters AI accountability without unduly burdening innovation

Digital Operators Resilience Act (DORA): in September 2020, the European Commission adopted a new Digital Finance Package, which includes a proposal for an EU regulatory framework on digital operational resilience, the 'Digital Operational Resilience Act' (DORA). This proposed regulation aims at ensuring that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will require all firms to ensure that they can withstand all types of Information and Communication Technology (ICT) - related disruptions and threats and the proposal introduces an oversight framework for ICT providers, such as cloud computing service providers.

This proposal, which builds on the European Banking Authority guidelines for outsourcing to cloud providers, could have potentially negative consequences for cloud computing service providers to financial services companies, and the current recommendations from the guidelines would become mandatory. Those would include, among others, the imposition of model contract clauses that would cover inspection and audit rights, termination rights and exit strategies; a new EU supervisory body to oversee large cloud providers, or large penalties for non-compliance. Moreover, Non-EU headquartered providers may be subject to higher levels of scrutiny.

E. India

Overview/Business Environment

The commercial environment for BSA members remains challenging in India. In addition to certain policy and regulatory developments that may require data localization and hinder cross-border data transfers, preferences for domestic products and services contained in certain procurement policies could restrict market access for BSA members.

Digital India Act

The Government of India is considering developing a comprehensive set of laws that would be in "sync with today's digital economy"[80] and "make the online world more accountable".[81] To achieve these objectives, the Government of India is considering substantial revisions to the two decades old Information Technology Act, 2000, last amended in 2008.[82] This is an important opportunity to update a rapidly aging law and create a new, modern legislative framework for India. Accordingly, BSA recommends that the Government keep in mind the following key principles as it considers this important legislative reform:

- Ensure policy predictability and regulatory accountability;
- Adopt a coherent policy approach;
- Recognize differences between enterprise and consumer facing companies;
- Identify policy priorities for cybersecurity; and
- Harmonize with the upcoming data protection law.

Personal Data Protection Bill

In August 2022, the Ministry of Electronics and Information Technology (MeitY) withdrew the Personal Data Bill 2019 (PDP 2019)[83] from the Indian Parliament. MeitY is expected to present a new personal data protection bill for public consultation in December 2022. Concerns with the PDP Bill 2019 include requirements to localize critical data and to maintain copies of sensitive data in India (definitions of what type of data would constitute critical or sensitive data are not provided). It is uncertain whether the new privacy bill will continue to include requirements to localize data and cross-border data transfer restrictions.

In our comments on an earlier version of the Bill, [84] BSA describes our concerns that the Bill lacked the conceptual clarity and consistency that is crucial for the Indian digital economy to effectively integrate with the global data economy. In terms of regulatory capacity, although the Bill established an independent regulator called the Data Protection Authority, BSA was concerned this regulating body would not be properly resourced, would be asked to do too much, and may therefore prove ineffective. These challenges, coupled with serious concerns about data localization, disproportionate criminal penalties, lack of flexibility for personal data fiduciaries, uncertain accountability requirements, lack of an institutional framework for enforcement, nonflexible security safeguards, improper liability allocation, and lack of harmonization pertaining to the personal data of children, are broken down in greater detail in our comments.

---

[80] Comprehensive legal framework is in the works: Ashwini Vaishnaw accessible at: https://www.livemint.com/news/india/comprehensive-legal-framework-is-in-the-works-ashwini-vaishnaw-11659552785859.html

[81] Govt working on new Data Protection Bill, Digital India Act: IT Minister Ashwini Vaishnaw, accessible at: https://www.financialexpress.com/industry/technology/govt-working-on-new-data-protection-bill-digital-india-act-it-minister-ashwini-vaishnaw/2657315/

[82] Information Technology Act 2000, https://www.meity.gov.in/content/information-technology-act-2000

[83] *Personal Data Protection Bill, 2019,* http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[84] BSA Submission to the Joint Parliamentary Committee on India's Personal Data Proteciton Bill, 2019, https://www.bsa.org/policy-filings/india-bsa-submission-to-the-joint-parliamentary-committee-on-indias-personal-data-protection-bill-2019

The Government of India should consider these concerns and recommendations as they develop revised privacy and personal data protection related legislation.

Non-Personal Data Governance

On September 2019, MeitY constituted a Committee of Experts to develop a governance framework for non-personal data (NPD Framework). In August 2020, the Committee released its report.[85] In December, the Committee published the revised report.[86] In our written comments, BSA highlighted numerous concerns including mandatory sharing of proprietary non-personal data, restrictions on cross-border data transfers and local storage requirements.[87] Such mandatory obligations are counterproductive throughout the data ecosystem, and present additional complications if applied to "data processors," including enterprise software and cloud service providers. The framework proposes additional compliance obligations for businesses by creating a new regulator in addition to the proposed Data Protection Authority (DPA) under PDP 2019 and the proposed e-commerce regulator. The mandatory data-sharing framework proposed in the NPD framework is in addition to the sharing requirements proposed in the PDP 2019, which was withdrawn by MeitY by August 2022. These proposals have a chilling effect on innovation and investment in the digital economy.

Intermediary Guidelines

In December 2018, MeitY issued the Draft Information Technology [Intermediary Guidelines (Amendment) Rules] ("Draft Guidelines").[88] The Draft Guidelines include problematic filtering obligations that will create significant privacy and data protection concerns for consumers. BSA has highlighted these concerns and urged MeitY to eliminate unnecessary obligations imposed on businesses.[89] The revised Draft Guidelines were issued in February 2021 by placing heightened obligations on a new category of intermediaries called the 'Significant Social Media Intermediaries (SSMIs)' which partially addressed concerns raised by BSA.

CERT-In Directions

In April 2022, the Indian Computer Emergency Response Team (CERT-In) released *'Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*' (Directions).[90] The Directions mandated many onerous obligations on cyber incident reporting including reporting of all cyber incidents within six hours besides validating all user information collected by service providers. Based on stakeholder feedback, CERT-In released FAQs which provided additional clarifications on some of the onerous provisions, but the Directions continue to remain a challenge to implement for companies. [91] BSA highlighted these challenges in a letter to MeitY.[92]

Telecommunications Act Amendments

---

[85] Report by the Committee of Experts on Non-Personal Data Governance Framework, August 2020, https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf
[86] Report by the Committee of Experts on Non-Personal Data Governance Framework, Dec 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf
[87] BSA Submission on Revised Non-Personal Data Governance Framework, January 2021, https://www.bsa.org/policy-filings/india-bsa-submission-on-revised-non-personal-data-governance-framework
[88] The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 – Draft available at: https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf
[89] BSA Submission on Draft Information Technology [Intermediary Guidelines (Amendment) Rules] 2018 available at: https://www.bsa.org/files/policy-filings/01312019BSAResponseDraftIntermediaryGuidelinesMeitY.pdf
[90] Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet by CERT-In, MeitY accessible at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[91] Frequently Asked Questions (FAQs) on Cyber Security Directions of 28.04.2022 accessible at: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf
[92] BSA concerns on the CERT-In Directions on Information Security Practices accessible at: https://www.bsa.org/files/policy-filings/05302022meitycertin.pdf

In September 2022, the Department of Telecom released a draft of the Indian Telecommunications Bill, 2022 for consultation.[93] While public consultation is still underway on the bill, preliminary review indicates that there are key concerns with the Bill including an overbroad definition of "telecommunication services" to include a wide-range of internet-enabled digital services.

Public Procurement Preferences

Technology mandates and domestic preferences for government procurement have been clearly demonstrated as part of a larger "Make in India" initiative adopted by the Government of India.

The Make in India Order,[94] issued by the India Department for Industrial Policy and Promotion (DIPP) in June 2017 and revised in 2020 and 2021, aims to promote local manufacturing, requires every government department to give preference to local suppliers when procuring goods and services. The Make in India Order is the first enabling framework for preferential market access in software products and services. The order places an emphasis on the *situs* of manufacturing or provision of service (based on a definition of "local content"). However, government departments are granted the discretion to implement the Make in India Order according to their own requirements. By pegging procurement preference to 'local content', the order creates uncertainty and difficulty for foreign software companies to participate in any government tenders/procurement processes.

Subsequently, MeitY issued the Draft Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order for public comment.[95] In July 2018, MeitY issued the final notification with only minor changes.[96]

The Notification and similar developments could significantly affect India's ability to acquire best-in-class products and services and negatively impact US companies' ability to effectively participate in public procurement opportunities.

Government procurement policies remain outmoded and inefficient because of local content and technology preferences. In 2020, DIPP (now the Department of Promotion of Industry and Internal Trade – DPIIT) revised the Public Procurement Order 2017 (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services.[97] The Ministry of Electronic and Information Technology (MeitY)'s guidelines to government departments on cloud services contracts also contain requirements for data to be localized in India.[98] In addition, the Draft National Policy on Software Products would promote the use of domestically developed software products in public sector procurements and strategic sectors like defense, telecommunications, energy, and healthcare. Such policies do not offer a level playing field to US technology providers that are bringing cutting-edge technologies and services to India.

---

[93] Draft Indian Telecommunication Bill, 2022 accessible at: https://dot.gov.in/sites/default/files/Draft%20Indian%20Telecommunication%20Bill%2C%202022.pdf
[94] *Public Procurement Order 2017 (Make in India Order)* at: http://dipp.nic.in/sites/default/files/publicProcurement_MakeinIndia_15June2017.pdf
[95] *Public Procurement (Preference to Make in India) Order 2017- Notifying Cyber Security Products in furtherance of the Order* (Draft Notification) at: http://meity.gov.in/writereaddata/files/Draft%20Notficationn_Cyber%20Security_PPO%202017.pdf.
[96] *Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products* at: http://meity.gov.in/writereaddata/files/public_procurement-preference_to_make_in_india-order_2018_for_cyber_security_products.pdf.
[97] *Make in India Order*
[98] *Guidelines for Government Departments On Contractual Terms Related to Cloud Services* at: https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.

F. Indonesia

Overview/Business Environment

The commercial environment for the software and IT sector in Indonesia is very challenging. A variety of authorities have issued, or are in the process of developing, policies that will make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Market Access

A variety of policies affecting the IT industry have been developed or proposed over the last several years that make, or threaten to make, it increasingly difficult to provide digital products and services to the Indonesian market.

Duties on Digital Products: In February 2018, the Ministry of Finance (MOF) issued Regulation 17, which amended Indonesia's Harmonized Tariff Schedule (HTS) to add Chapter 99 "[s]oftware and other digital products transmitted electronically."[99] Although Chapter 99 is currently duty free, Chapter 99 effectively treats electronic transmissions as imports, to which customs requirements apply, including requirements to comply with all customs laws that attach to imports, prepare and file import declarations, and pay 10 percent value-added tax (VAT) and 2.5 percent income tax.

These compliance obligations are already burdensome for physical goods and require companies to have compliance departments composed of specialized trade professionals that can determine proper customs valuation, country of origin, HTS classification, and other requirements. Complying with Chapter 99 would not only prove very costly for companies, but in most cases these obligations simply cannot be applied to electronic transmissions.

Personal Data Protection: Indonesia has been developing a draft Personal Data Protection (PDP) Bill since 2014 and successfully enacted the PDP Bill on October 17, 2022. Based on BSA's reading of the law, it draws from several principles and aspects of the European Union's General Data Protection Regulation (GDPR), focusing on five main areas: data collection, data processing, data security, data breach, and the right for individuals to have their personal data erased. BSA's chief concerns with the law relate to potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors. The law provides for a two-year grace period for data controller and data processors to adjust their practices to comply with the law. A data protection authority that reports to the President will be set up within this period.

[99] *Regulation No. 17/PMK.010/2018 (Regulation 17)* (Indonesian) at: https://jdih.kemenkeu.go.id/fullText/2018/17~PMK.010~2018Per.pdf.

G. Japan

Overview/Business Environment

Japan has a strong market for software-enabled products and services with a comprehensive suite of modern laws that support and facilitate the digital economy. However, the Government of Japan must accelerate the uptake of cloud services and digital transformation in the public and private sectors.

In 2021, Japan established the Digital Agency,[100] which functions as the control tower to promote digital transformation across society, including management and oversight of central government information systems, standardization of local government information systems, improving administrative services utilizing the My Number (personal number) system, and digitalization in various fields including education, disaster prevention, and medical care through better use of data.

Prime Minister Kishida created a new ministerial post for economic security in the Cabinet, aiming to strengthen Japan's "strategic autonomy" and promulgated the "Act on Promotion of Ensuring Security by Taking Economic Measures in an Integrated Manner"[101] in May 2022 which includes the introduction of a new system by the Government to pre-examine the installation and consignment/management of designated facilities/equipment used in designated core infrastructure services to ensure that they are not used as means to "interfere the stable provision of services from outside Japan". While specific coverage of business and facilities/equipment that will come under the new system is still under discussion, BSA has raised concerns to the Government, recommending the policies are cohesive and holistic; embrace clear and well-defined criteria; and are narrowly tailored involving a process of robust public consultation and frequent review. Also, heightened awareness on cyber risks could lead to misguided understanding that locally hosted data is safer, when in fact it is subject to many of the same cyberattacks as cloud services.

Cloud Security Assessment

The Government of Japan launched the Information System Security Management and Assessment Program (ISMAP)[102] in 2020 , a cloud security assessment program for government procurement, creating a register of cloud services that have met security requirements for central government procurement. While the Government's commitment to promote a "cloud-by-default' principle is a positive move, the ISMAP imposes significant compliance burdens and prohibitive costs on cloud service providers (CSPs) wishing to be registered on the ISMAP Cloud Service List. BSA has urged the Government to reduce repetitive auditing process by exempting the application of security controls that are duplicative with internationally recognized standards for which certifications have already been received. Given that many global CSPs already have internationally accredited certifications (e.g., ISMS-JISQ/ISO 27000 series, SOC2), acknowledging them and eliminating repetitive procedures and requirements to reuse evidence already provided in prior certifications from ISMAP will contribute to alleviating the burden on the Government of Japan and on CSPs.

Physical Network Separation

The Ministry of Internal Affairs and Communication (MIC) issued "Guidelines on Information Security Policy for Local Governments (Guidelines)"[103] which continue to support the use of physical network separation as a cybersecurity solution. This guidance discourages government agencies from adopting the latest commercial cloud computing and related services. BSA has highlighted the need to modernize security approaches through public-private sector collaboration and to promote policies supporting a "cloud-native" architecture that are not based on physical network separation. The same guidelines recommend, when storing highly confidential information, businesses and governments

---

[100] https://www.digital.go.jp/en
[101] https://elaws.e-gov.go.jp/document?lawid=504AC0000000043_20230517_000000000000000 (Japanese) https://static1.squarespace.com/static/5eb491d611335c743fef24ce/t/627dec876ba75369ad752dc6/1652419721341/Economic+Se_(unofficial English translation)
[102] https://www.ismap.go.jp/csm?id=csm_ismap_index
[103] https://www.soumu.go.jp/main_content/000805453.pdf

should select data centers that operate within the scope of Japanese laws and regulation, which may be interpreted as a de facto data and server localization requirement in these instances. BSA will continue to monitor development as MIC works to update the Guidelines.

G. Republic of Korea

Overview/Business Environment

The overall commercial environment in the Republic of Korea (South Korea) for BSA members and the software sector is mixed. South Korea has a strong market for software-enabled products and services and a mature legal system. However, the Government of South Korea has policies that present substantial market access barriers to foreign software products and services. Such policies include local testing requirements and requirements to comply with national technical standards even when commonly used internationally recognized standards are available. Data residency, physical network separation, and other requirements for industry sectors, such as government/public services, finance, healthcare, and education, hamper the ability to provide cloud-based services to users in these sectors. These requirements may also be institutionalized by the National Assembly, with a bill recently proposed to create legal bindings to Cloud Security Assurance Program (CSAP).

Market Access

The adoption of procurement preferences for domestic firms and imposition of additional burdensome measures, often with security concerns cited as justification, have decreased market access for BSA members in South Korea. These policies especially affect those providing software-enabled services, such as cloud-computing and data analytics services.

Cross-Border Data Transfers and Server Localization: It remains very difficult for commercial cloud services providers (CSPs) to offer cloud services to entities in South Korea's very broadly defined public sector. This is due to onerous certification requirements imposed by the Korea Internet Security Agency (KISA) under the Cloud Security Assurance Program (CSAP) on CSPs that provide cloud services to public sector agencies and requirements for physical network separation. Similar guidelines and regulations requiring physical network separation or data onshoring apply to healthcare sectors.[104] Thus, significant barriers to providing cloud computing and related services in South Korea remain. Given the emergence of different third party security assessment requirements in Australia and Japan, it would be helpful to promote greater alignment and potentially cross-recognition of these requirements.

Physical Network Separation: Although the Government of Korea is committed to promoting the adoption of cloud computing, security concerns by the National Intelligence Service (NIS) have resulted in policies requiring physical network separation. Physical network separation requirements prevent or discourage government agencies and other regulated sectors (e.g., healthcare) from adopting commercial cloud computing and related services.

In 2016, the Ministry of the Interior and Safety (MOIS) and the Ministry of Science and ICT (MIST) adopted the CSAP, announcing certain revisions in 2019.[105] Since 2016, the CSAP has contained problematic physical network separation requirements.[106] In other mature markets, physical network separation requirements are rarely applied throughout the public sector, including in workloads or institutions that handle non-sensitive (and sometimes, public) data, such as public universities. The uniformly applied physical network separation requirements do little to enhance security while undermining the main benefit of cloud computing services, which is the economy of scale and state-of-the-art security capabilities of multi-tenant cloud services. As described in BSA's August 2019

---

[104] On June 1 of 2020, a new certification framework that includes CSAP requirements was applied to electronic medical records. *See* Enforcement Decree of the Medical Service Act (Article 10-5: Standardization of Electronic Medical Records) (indicating that "matters subject to standardization to be determined and publicly notified by the Minister of Health and Welfare pursuant to Article 23-2 (1) of the Act shall be as follows: "2. Facilities and equipment necessary for the safe management and preservation of electronic medical records under Article 23 (2) of the Act").
[105] *See* https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=2093939.
[106] As of the 2019 amendments, the physical network separation requirements stipulate that, "the physical location of the cloud system and data shall be restricted to in country and cloud service area for public institutions shall be physically separated from the cloud service area for private institutions."

comments,[107] these requirements will have a negative impact on South Korea's digital ecosystem and curtail its ability to participate effectively in the global digital economy — raising the cost of providing services and inhibiting the choice of technology available to end-users and procuring entities. The costs associated with such additional infrastructure will need to be recovered, which would ultimately increase the costs for end consumers.

South Korea's regulatory environment for the use of cloud services in the financial services sector has improved somewhat of late. The Financial Services Commission (FSC) recently approved the use of personal credit information by public cloud services and may be considering additional measures to expand the ability to manage financial data on the public cloud. However, the FSC specifically requires that such data be maintained on servers located in South Korea.[108]

Encryption: The revisions to the CSAP require that "cloud computing services providers shall use government-certified standard encryption technology when providing an encryption method for important material created through the cloud service." These kinds of national approaches to encryption requiring the use of locally selected algorithms rather than internationally recognized algorithms, however, constrain the choices of technologies available to organizations and citizens in South Korea, including leading edge security solutions that defend against latest threats. Cryptography certification in South Korea also requires a review of source code, which could raise concerns regarding protection of proprietary information and trade secrets. This is also impractical for many leading cloud service providers, which already use state-of-the-art encryption algorithms that meet internationally recognized standards and are accepted for applications in the most sensitive circumstances in other markets. In fact, as outlined in BSA's comments, this kind of fragmented and piecemeal approach that only allows the use of domestically certified encryption standards may deprive organizations from using best-in-class encryption technologies, and this would weaken rather than strengthen the protection of sensitive data.[109]

Personal Information Protection Regime: South Korea's personal information protection regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the South Korean market.

In January 2020, the National Assembly enacted amendments to the Personal Information Protection Act (PIPA),[110] the Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act),[111] and the Credit Information and Protection Act.[112] The primary result of the legislative package is to consolidate the legal protection and enforcement provisions for personal information primarily in the PIPA, and to elevate the Personal Information Protection Commission (PIPC) to a central government-level agency under the Prime Minister.

The PIPA has subsequently undergone further amendments. and the European Commission has issued "adequacy" recognition to South Korea. However, more work is required to reform South Korea's personal data protection regime. There should be a clearer distinction between data controllers versus data processors to better delineate the roles and responsibilities of different entities. South Korea should also adopt measures that expand the legal basis for processing personal information beyond consent. This would enhance investment and innovation in emerging technologies, like data analytics

---

[107] Comments available at: https://www.bsa.org/files/policy filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.
[108] E.g., under RSEFT Article 14-2-8 (Usage process of cloud computing service), finance companies and electronic finance service providers shall use domestically located information process systems and apply Article 11-12 to process personal credit information or identification information.
[109] Comments available at: https://www.bsa.org/files/policy-filings/en08082019bsarevisedcloudsecurityassuranceprogram.pdf.
[110] *Personal Information Protection Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.
[111] *Act on Promotion of Information and Communication Network Utilization and Information Protection (Network Act)* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.
[112] *Credit Information and Protection Act* (2016). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX.

and machine learning, while ensuring that personal information is appropriately and adequately protected.

Discriminatory Security Certification Requirements Applied for Foreign IT Products: Since 2011, the Government of Korea has imposed additional security verification requirements for international Common Criteria (CC)-certified information security products that are procured by government agencies. In 2014, the Government of Korea extended similar security conformity testing requirements to international Common Criteria-certified networking products procured by any South Korean government agency.

South Korea is a member of the Common Criteria Recognition Arrangement (CCRA) and therefore should recognize international certifications from accredited laboratories and should not impose further requirements for Common Criteria-certified products.[113] The additional requirements are in tension with the spirit of CCRA, which is to "eliminate the burden of duplicating evaluation of IT products and protection profiles."[114]

The NIS revised the Security Evaluation Scheme (SES) in early October 2022, allowing institutions with relatively low security sensitivity, such as basic-level local governments and public schools, to use internationally CC-certified ICT products without additional domestic security verification. However, most major public institutions which account for an overwhelming proportion of the public sector market, including all central administrative institutions and metropolitan local governments, are still required to only use products with domestic security certification, limiting market access for US companies.

Copyright and Enforcement

Compliance and Enforcement: Criminal enforcement has been an effective mechanism for BSA members to protect their rights and enforce against the use of unlicensed software by enterprises in South Korea. The police, the prosecutors' offices, and the special judicial police under the Ministry of Culture, Sports, and Tourism (MCST) are the authorities primarily involved in enforcement activities against enterprises using unlicensed software.

The special judicial police are specifically tasked with investigations and inspections concerning copyright violations and they are relatively active in conducting enforcement activities against enterprises using unlicensed software. However, they have limited resources and BSA members also rely on the enforcement actions of the police. In line with the Government of Korea's goal of reducing the rate of unlicensed software use, BSA recommends that the special judicial police increase its resources with a view to increasing the volume of enforcement activities against infringers.

BSA members also rely on civil litigation to take action against enterprises using unlicensed software. However, more can be done to improve the current system. For example, although preliminary injunctions are available, they are not often issued. It is also difficult to acquire evidence in civil cases without first going through a criminal raid. The option of aggravated damages is also not available to copyright holders under South Korean law. As a result, the damages awarded in civil cases tend to be too low to compensate rights holders or to deter future infringements. South Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules in civil cases.[115]

[113] Common Criteria Recognition Arrangement (CCRA) at: https://www.commoncriteriaportal.org/ccra/
[114] CCRA
[115] *Civil Procedure Act* (2017). English translation at: http://www.law.go.kr/eng/engLsSc.do?menuId=2&section=lawNm&query=cloud+computing&x=0&y=0#AJAX

H. Singapore

Overview/Business Environment

Singapore has a strong market for software-enabled products and services and comprehensive and well-functioning legal system to enable the development and deployment of such technologies.

The Government of Singapore has generally consulted with industry prior to introducing legislative changes. However, in a few important instances, the Singapore Government has tended toward closed consultations with a select group of key industry players without adequately consulting the breadth of stakeholders that will be both affected by, and could contribute to, such legislation and policy making.

Cybersecurity Act

In February 2018, Singapore enacted its first comprehensive law on cybersecurity and critical infrastructure protection, the Cyber Security Act.[116] This was the culmination of several years of intense consultation. The substantial input the Cyber Security Agency (CSA) received from industry and other interested stakeholders led to substantial improvements in the final legislation.[117]

In 2022, the CSA announced revisions to the Cybersecurity Code of Practice (CCoP).[118] Initially, the CCoP were informed primarily by consultations with the affected critical infrastructure (CI) operators, and only later were providers of cloud computing systems and other software-enabled services upon which CI operators rely for many of their cybersecurity and information technology needs consulted.[119]

It is important that consultations involving any further amendments to the Cyber Security Act or its implementing rules involve all relevant stakeholders, especially BSA members that provide globally leading services and security to many sectors and customers, including CI operators. These consultations must provide adequate time for meaningful information exchange.

Online Safety Bill

The Online Safety Bill is intended to tackle harmful content available on online services in Singapore and is largely targeted at social media services.[120] Similar to CSA's approach with the Cybersecurity Act, the Infocomm Media Development Authority (IMDA) engaged with large social media providers on the Online Safety Bill but did not include other organizations in the eco-system that would potentially be affected by the Bill. For example, enterprise software organizations which deliver online communications services that are adjacent to the social media services that the Bill targets were not consulted, though they were caught by the broad definition of "online communication service" under the Bill. The result is that IMDA did not have the opportunity to hear from other stakeholders on how to better target the Bill's scope and obligations to achieve the stated objectives without interfering with commercial activities.[121]

While these instances do not, in themselves, constitute a trend, it is worth reiterating that Singapore, as a model of good governance in the region and the world, should redouble its efforts to ensure that legislation with wide-reaching effects on the industry at large are subject wider industry consultations that include the range of affected stakeholders.

---

[116] Cyber Security Act, https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312
[117] Joint Association Comments on Singapore Cybersecurity Bill, August 2017, https://www.bsa.org/policy-filings/singapore-joint-association-comments-on-singapore-cybersecurity-bill
[118] CSA Website – Codes of Practice/Standards of Performance, https://www.csa.gov.sg/Legislation/Codes-of-Practice
[119] BSA Submission on the Cybersecurity Code of Practice, May 2022, https://www.bsa.org/policy-filings/singapore-bsa-submission-on-the-cybersecurity-code-of-practice
[120] Online Safety (Miscellaneous Amendments) Bill, https://sso.agc.gov.sg/Bills-Supp/28-2022/Published/20221003?DocDate=20221003
[121] BSA Comments on Online Safety Public Consultations in Singapore, August 2022, https://www.bsa.org/policy-filings/singapore-bsa-comments-on-online-safety-public-consultations-in-singapore

I. Thailand

Overview/Business Environment

The Royal Thai Government (RTG) is pursuing a range of policies under Thailand 4.0 to promote the digital economy. Two important pieces of legislation enacted in 2019 — one on cybersecurity protection of critical infrastructure, and the other on personal data protection — are important elements of this effort, although the Government has yet to release implementing regulations for public consultation across all issues. BSA agrees that it is important for Thailand to have robust and effective cybersecurity and personal data protection legislation. However, we remain concerned that the implementation of both laws could undermine the RTG's efforts to enhance cybersecurity and personal data protection, interfere with the government's broader goals to drive Thailand 4.0, and unfairly impede BSA member companies' ability to effectively provide products and services to the Thai market.[122]

Market Access

BSA shares the goals of the RTG's Digital Economy initiative, Thailand 4.0, and supports the thoughtful implementation of personal data protection and cybersecurity legislation. The RTG should, however, consider measures to minimize the potential unintended effects of recently enacted cybersecurity and personal data protection legislation that could harm the ability of BSA members and other technology sector companies to provide innovative and effective software products and services.

Security: In May 2019, Thailand enacted its Cybersecurity Act to strengthen the capabilities and authorities of government agencies to prevent, cope with, and mitigate the risk of cyber threats, especially with respect to critical information infrastructure. The Cybersecurity Act raises concerns as it gives the National Cybersecurity Committee (NCSC) broad powers to enter into premises, to monitor and test computers and computer systems, and to seize or freeze computers, computer systems, and equipment, without sufficient protections, such as opportunities to appeal or limit such access. Such broad powers would undermine public confidence and trust in information technology (IT) generally and harm the ability of BSA members to provide the most innovative and effective software solutions and services to the Thai market.[123] There is also criminal liability for organizations and individuals who do not comply with executive orders issued under the Cybersecurity Act.[124]

In August 2021, the Ministry of Digital Economy and Society (MDES) issued a new Notification on "Criteria on Storing Computer Traffic Data of Service Providers B.E. 2564 (2021)" ("New Notification") to replace the previous Notification of Ministry of Information and Communication Technology Re: Criteria on Storing Computer Traffic Data of Service Providers B.E. 2550 (2007) (the "Previous Notification"). This Notification took effect on 14 Aug 2021 without any prior industry consultation, giving digital service providers only 180 days from this date to comply. The new regulation will require Data Centers and Cloud Service Providers to collect and retain extensive user information (e.g. identity info and activity logs) to facilitate authorities' access to users' data. This new regulation will increase compliance costs to both service providers and users, reduce competitiveness for small operators, and risk violating users' privacy rights.

Personal Data Protection: The Personal Data Protection Act (PDPA) was enacted in May 2019 and is Thailand's first omnibus legislation on personal data protection. It is designed to build public trust and confidence in the digital economy and to implement the Asia-Pacific Economic Cooperation (APEC)

---

[122] *See generally*, BSA Cloud Scorecard – 2018 Thailand Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Thailand.pdf

[123] See BSA's comments, available at: https://www.bsa.org/~/media/Files/Policy/Data/05062015SubmissionCybersecurityBill_EN_DeputyPrimer.pdf; https://www.bsa.org/~/media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf; and https://www.bsa.org/~/media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

[124] In addition to the foregoing measures, the Ministry of Digital Economy and Society (MDES) also issued a so-called Emergency Decree on Electronic Meetings, stipulating that electronic meetings on confidential matters must be conducted through a meeting control system established within the country. As reported, this measure raises concerns about its ambiguity, as well as concerns regarding the imposition of such a local development condition.

Privacy Framework's principles for cross-border data transfers.[125] It also heavily draws from the General Data Protection Regulation (GDPR) of the European Union. BSA's chief concerns with the PDPA relate to prescriptive and burdensome notification and consent requirements for the collection, use, and disclosure of personal data. There are also potentially challenging breach notification requirements and liability for personal data breaches imposed on data processors.[126]

In May 2020, the Thai Cabinet approved a royal decree granting a one-year exemption from certain provisions of the PDPA 2019 , which had been scheduled to take full effect on May 27, 2020. On 5 May 2021, the Cabinet decided to further extend the fully effective date of the PDPA under the Previous Royal Decree from 1 June 2021 to 1 June 2022. The provisions which are exempted include: consent requirements, notification requirements, establishment of lawful basis, requirements on the collection of personal data from other sources, and processing of minors' personal data. The enforcement of a second list of requirements is also postponed, including observance of data subjects' rights and data erasure or destruction requirements, the implementation of appropriate internal security measures to prevent unauthorized access, provision of data breach notifications, appointment of data protection officers (DPOs), filing complaints, and penalties.

The Personal Data Protection Committee (PDPC) was formally established in January 2022. The PDPC has issued a few sets of draft notifications covering topics such as records of processing activities for data processors, security measures for data controllers, rules for the imposition of administrative penalties by the Expert Committees, international transfers of personal data, responsibilities of data processors, data protection impact assessments and obligations of data controllers related to automated processing. The most recent public hearing was for the Draft Notification of the PDPC on Rules and Principles of Appropriate Personal Data Protection for International Transfer, which closed recently on October 24, 2022.

Copyright and Enforcement

BSA enjoys good cooperation with RTG authorities, including with the Economic Crime Suppression Division (ECD) of the Royal Thai Police, in addressing unlicensed use of software in Thailand.

Compliance and Enforcement: Thailand has a specialized intellectual property (IP) court, which has improved the effectiveness of IP litigation in Thailand. Unfortunately, though damages awarded in civil litigation are occasionally reasonable, award amounts are very inconsistent and often inadequate to compensate the rights holder or deter future infringements. Expenses are often awarded, but only very small amounts, and they do not typically cover the actual legal costs. Preliminary injunctions are not granted regularly enough to be an effective tool. In addition, although criminal cases can be effective in Thailand, the courts should apply more deterrent penalties for convictions. In recent cases, courts imposed only a fraction of the potential fines or refrained from imposing any fines at all — simply suspending sentences — even in cases involving significant infringements.

[125] *APEC Privacy Framework* at: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework
[126] See BSA's comments, available at: https://www.bsa.org/~/media/Files/Policy/Data/03232015BSASubmissiononThaiPersonalDataProtectionAct_EN.PDF

J. Vietnam

Overview/Business Environment

Over the past several years, Vietnam has enacted, implemented, and proposed various protectionist measures to regulate the software sector. These measures are likely to reduce fair and equitable market access for BSA members who wish to provide software products and services in Vietnam.[127] The enactment of the Cybersecurity Law in June 2018, and current efforts to develop implementing rules, only exacerbate the existing challenges and threaten to make Vietnam an even less attractive destination for the delivery of cutting-edge software products and services.[128]

Market Access

Cybersecurity: On June 12, 2018, Vietnam's legislative body, the National Assembly, enacted the 20th version of the Cybersecurity Law (Law). The Law went into effect on January 1, 2019.

The Law raises serious concerns and will likely significantly impact the ability of many BSA members to provide software products and services in Vietnam. The breadth of the Law far exceeds cybersecurity protection and extends to a broad regulation of the Internet generally. The Law also grants vast powers to authorities and imposes stringent requirements on software product and service providers to comply with local cybersecurity standards and regulations and to apply for certification by local agencies. In sum, the Law is a significantly negative development in Vietnam's market access environment for the software sector.

On August 15, 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (Decree 53) that took effect from October 1, 2022. Decree 53 is concerning because it requires domestic enterprises (potentially including domestic customers of foreign service providers) to store data within Vietnam and it is not clear whether domestic enterprises include foreign-invested enterprises or subsidiaries of foreign or multinational corporations with head offices in Vietnam. While Decree 53 is silent on the transfer of data overseas, it requires affected enterprises to store data in Vietnam. This leads to market access issues if domestic enterprises are unable to use cloud-based services that do not or cannot store data in Vietnam as part of their services.

***Personal Data Protection Decree*:**

Following two rounds of public consultations on the draft PDP Decree, in September 2021, the MPS submitted their revised draft PDP Decree to the Ministry of Justice (MOJ) for internal appraisal. However, this version of the draft PDP Decree was kept strictly confidential.

With the issuance of Resolution 27 in March 2022 approving the substantive content of the latest draft PDP Decree, the MPS was assigned to consult the National Assembly on the draft. The draft PDP Decree was expected to be passed in May 2022 following review by the National Assembly. However, this process has been delayed. BSA understands that the draft PDP Decree is still pending at the National Assembly Standing Committee because the lawmakers are waiting on the Central Politburo's comments, which has delayed its passage till now (October 2022).

The MPS has also been assigned to take charge and coordinate with the MOJ to propose the formulation of a Personal Data Protection Law after the PDP Decree has been passed

---

[127] *See generally*, BSA Cloud Scorecard – 2018 Vietnam Country Report, at https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_Vietnam.pdf

[128] *Vietnam National Assembly Passes the Law on Cybersecurity* (July 2, 2018) at: https://globalcompliancenews.com/vietnam-law-cybersecurity-20180702/. Another measure that we continue to monitor is Vietnam's Outline of Draft Decree on Personal Data Protection, which was published for public comments earlier this year, contains registration requirements for processing of sensitive personal data and transfer of personal data of Vietnamese citizens overseas.

Based on previous iterations of the draft PDP Decree, the PDP Decree will likely impose restrictive data transfer and data localization requirements. In addition, there are also burdensome requirements for personal data processors to store data transfer history for three years, register with the Personal Data Protection Commission (PDPC) for cross-border transfers of sensitive personal data with very detailed requirements for registration, and for the PDPC to carry out annual assessments or audit-like exercises on cross-border data transfers by personal data processors. These obligations are not only impractical, they may also create new privacy and security concerns by forcing companies to store and access data they otherwise would not.

Draft Decree on Administrative Penalties in the Field of Cybersecurity: On September 23, the MPS also released a draft Decree on Administrative Penalties in the field of Cybersecurity, to be adopted on the basis of the Cybersecurity Law. Among others the draft details a number of infractions to the draft PDP Decree. The publication of this draft Decree, which is currently open for consultation, came as a surprise because the main PDP Decree is yet to be finalized. It does, however, provide insights in some of the key provisions under the PDP Decree such as data transfers, consent, data breach notification, etc. This draft Decree is expected to take effect in December 2021.

MIC Decisions 1145 and 783: In 2020, under the auspices of Vietnam's National Digital Transformation Strategy by 2025, the Ministry of Information and Communications (MIC) issued Decisions 1145 and 783 to announce a local cloud standard and cloud framework, respectively, for state agencies and smart cities projects. These measures may create a preferential framework for domestic cloud service providers, and measures currently characterized as "voluntary" will be treated as *de facto* requirements.

Decree 72: In July 2021, the Ministry of Information and Communications (MIC) issued a draft decree to amend both Decree No. 72/2013/ND-CP (Decree 72) on the management, provision and use of Internet services and online information and Decree No.27/2018/ND-CP (Decree 27) which amended and supplemented several articles in Decree No.72. The proposed amendments aim to allow the government to tighten control over livestreaming activities that generate revenue on social networks and impose obligations on cross-border social network service providers in Vietnam.

Not only does Decree 72 reinforce the data localization requirements found in other Vietnamese laws, BSA is also particularly concerned that the scope of covered entities could potentially include enterprise service providers even though many of the intended regulations are targeted at consumer-facing entities. There is also a new chapter under Decree 72 requiring providers of data center services to register with the MIC and contains additional obligations for data service providers to develop and implement technical plans and solutions to promptly detect and prevent illegal activities. These requirements place unnecessary and impractical burdens on data center service providers who may have to re-engineer their networks to afford them access to their enterprise customers' sensitive data which would be contrary to their contractual and other legal obligations.

Following public consultations, MIC released an updated draft of the proposed amendments in November 2021 for a second round of consultations. There have been no public updates on the status or progress of the proposed amendments since the second round of consultations concluded, although BSA has heard unconfirmed news that MIC has released a third draft of proposed amendments in October 2022.

Copyright and Enforcement

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code,[129] the Criminal Code,[130] and the Administrative Violations Decree.[131] The Civil Code operates in parallel.[132]

The Criminal Code criminalizes "commercial scale" acts of "[c]opying of works, audio recordings and visual recordings" or "[d]istributing the copies of work, audio or video recording." However, there has been a general lack of criminal enforcement against copyright infringement over the years by the relevant authorities.

On January 1, 2018, amendments to Vietnam's Criminal Code (adopted in 2015) went into effect.[133] The revised Criminal Code includes some improvements in provisions addressing copyright infringements. For example, there are several provisions applying criminal penalties for copyright infringements to commercial entities. Article 225 of the revised Criminal Code specifies that a commercial entity that commits copyright infringement is now subject to criminal penalties and may be fined up to VND3 billion (~US$150,000), and its business operations may be suspended for up to two years. However, the Government of Vietnam has yet to issue implementing guidelines in relation to how exactly Article 225 will be enforced. Such guidelines are required to clarify how Article 225 will supplement the existing regime.

Amendments to the Intellectual Property Code over the years have resulted in several improvements in the overall protection of copyright in Vietnam. However, more can be done to strengthen the legal framework for IP protection. BSA recommends introducing pre-established damages upon the election of the right holder, which can be very important in civil cases when the harm caused by the infringement is difficult to calculate.

Compliance and Enforcement: The lack of criminal enforcement against copyright infringement remains a concern. The general inactivity of the courts in dealing with copyright infringement issues also remains a problem in Vietnam. The Government of Vietnam should issue implementation guidelines on the enforcement of Article 225, which should clarify that the enforcement authorities and the courts are authorized and encouraged to prosecute criminal cases against commercial scale infringement, including against enterprises unlawfully using unlicensed software.

Also, there have been relatively few civil court actions involving copyright infringement in Vietnam. Complicated procedures, delays, and a lack of predictability in the outcome contribute to this problem. BSA remains hopeful that, over time, civil remedies will be available to supplement administrative, and eventually criminal, enforcement. However, the current difficulties in successfully bringing civil software copyright infringement cases coupled with a lack of clarity on how damages will be calculated for unlicensed software use has resulted in an increasing number of infringers being unwilling to settle cases with copyright holders despite clear evidence of rampant unlicensed software use. As a result, it remains challenging for copyright holders to obtain effective redress against infringers in Vietnam.

---

[129] *Law on Intellectual Property (No. 50/2005/QH11) (IP Law)* (2006). English translation at: https://wipolex.wipo.int/en/text/274445
[130] *Criminal Code (No. 100/2015/QH13)* (2016) at: https://wipolex.wipo.int/en/text/446025. English translation at: https://wipolex.wipo.int/en/text/446020
[131] *Decree No. 131/2013/ND-CP on Sanctioning Administrative Violations of Copyright and Related Rights*, entry into force December 15, 2013 (replacing Ordinances No. 47 and 109) at: https://thuvienphapluat.vn/van-ban/So-huu-tri-tue/Decree-No-131-2013-ND-CP-on-sanctioning-administrative-violations-of-copyright-and-related-rights-212865.aspx.
[132] *Civil Code (No. 91/2015/QH13)* (2017) at: https://wipolex.wipo.int/en/text/445451. English translation at: https://wipolex.wipo.int/en/text/445414
[133] *Law No. 12/2017/Q14 (Amended Criminal Code)*, see *Vietnam: 2015 Penal Code to Take Effect on 1 January 2018* at: https://globalcompliancenews.com/vietnam-new-penal-code-20171110/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original