SPECIAL 301 SUBMISSION

February 8, 2018

Docket No. USTR-2017-0024
Sung Chang
Director for Innovation and Intellectual Property,
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Mr. Chang,

BSA | The Software Alliance[1] provides the following information pursuant to your request for written submissions on whether US trading partners should be designated Priority Foreign Country, Priority Watch List, or Watch List in the 2018 Special 301 Report.

Pursuant to the Special 301 statutory mandate, Section 182 of the Trade Act of 1974, as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreements Act of 1994 (19 USC § 2242), requires USTR to identify countries based on two separate sets of criteria:

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

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

[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 60 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, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

20 F Street NW, Suite 800
Washington, DC 20011
P 202-872-5500
W bsa.org

Software has a profound impact on the American economy. A recent study from Software.org: the BSA Foundation shows the software industry contributes more than US$1.1 trillion to the US GDP and supports 10.5 million jobs (with significant impact in each of the 50 states), which expands America's economic potential across numerous sectors.[2] This economic progress, coupled with more than US$63 billion in software research and development investments, translates into software serving as a powerful catalyst for economic change – making businesses more effective and the US economy more prosperous.

BSA members strongly rely on the proper protection and enforcement of all forms of intellectual property and on open access to US trading partners' markets in order to continue innovating, creating jobs, and driving the growth of the digital economy. Adequate and effective **copyright, patent, and trade secrets** protection and enforcement remains a critical element for a successful commercial environment in US trading partners for BSA members. In addition, eliminating the **market access barriers** of US trading partners that discriminate against or impede BSA members in overseas markets is also critical for the continued health and growth of the software sector. Increasingly these barriers take the form of data localization policies that restrict the ability of companies to transfer data out of the country where it is collected.

BSA members face significant challenges due to the availability and extensive use of unlicensed software products, especially **unlicensed use of software** products or services **by governments, state-owned enterprises (SOEs), and business entities.**

In the following sections, BSA provides specific country reports on US trading partners that do not provide **fair and equitable market access** to BSA members, fail to provide **adequate and effective protection of intellectual property**, or both. We recommend these countries be listed on USTR's Priority Watch List or Watch List. We also request that the European Union (EU) be noted in the report as a Region of Concern due to increasing market access barriers that impact BSA members' ability to compete effectively in that market.

Priority Watch List:	**Argentina, Chile, China, India, Indonesia, Ukraine, and Vietnam**
Watch List:	**Brazil, Greece, Kazakhstan, Korea (Republic of Korea), Mexico, Nigeria, Romania, and Thailand**
Region of Concern:	**European Union**

The country reports immediately following this introduction set out BSA's specific concerns related to intellectual property protection and market access barriers in each of the countries cited. BSA can provide additional information with respect to each market as needed.

In addition to the country reports provided, we also make reference to specific concerns we have about **Taiwan** and **Poland** in this introduction and request that they be noted in the 2018 Special 301 Report.

Market Access

Cross-border data flows: The ability of US companies to continue to lead global advances in innovative technology is under a rising threat from government policies hampering their business models, especially the crucial role played by the international movement of data. Barriers to cross-border data flows are often disguised as privacy or security measures. Cross-border data flows are key to the current and future success of the US economy, and their importance will only increase in coming years. Immediate attention to these threats is urgently needed. Unfortunately, a number of markets, including **Brazil, China, India, Indonesia, Korea, Nigeria, and Vietnam**, have

[2] The Growing $1 Trillion Economic Impact of Software study available at https://software.org/reports/2017-us-software-impact/

adopted or proposed rules that prohibit or significantly restrict companies' ability to provide data services from outside their national territory. We are also closely following developments in the **EU** that could pose significant barriers to providing digital services in that market.

Data-related market access barriers take many forms. Sometimes they expressly require data to stay in-country or impose unreasonable conditions in order to send it abroad. In other cases, they require the use of domestic data centers or other equipment. Sometimes the barriers are justified as necessary to protect privacy or security, or to obtain jurisdiction over these services, but too often, there is also an element of protectionism, as the means chosen by these governments tend to be significantly more trade-restrictive than necessary to achieve any legitimate public policy goal.

Due to the trade-disruptive impact of measures that impede cross-border data flows and mandate data localization, BSA urges the US Government to work with its trading partners to prevent or remove such practices. All available trade mechanisms, including Special 301, should be leveraged for this purpose.

Procurement Restrictions: Governments are among the biggest consumers of software products and services, yet many are imposing 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 **Brazil, China, India, Indonesia, Korea, Nigeria, and Vietnam.** In addition to these countries whose procurement restrictions practices are detailed in this submission, **Taiwan** also restricts procurement of cloud computing services, requiring that all government data must reside in the country, which represents a barrier to companies that do not have servers in the country.

Security: Governments have a legitimate interest in ensuring that the software products and services and the equipment deployed in their countries are reliable, safe, and secure. However, a number of countries are using or proposing to use security concerns to justify *de facto* trade barriers. Such countries include **Brazil, China, Korea, Nigeria, Thailand, and Vietnam**. Furthermore, as mentioned above, **Taiwan** does not allow government agencies to procure cloud services from companies that store data outside the country, citing security concerns. Requiring cloud service providers to confine data in-country does not improve security, but rather hampers it, as it prevents data from being backed up in multiple locations. Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Security is instead a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question.

Standards: Technology standards play a vital role in facilitating global trade in 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, a number of countries have developed or are developing country-specific standards to favor local companies and protect them against foreign competition. This creates a *de facto* trade barrier for BSA members, raises the costs of cutting-edge technologies to consumers and enterprises, and places the domestic firms these policies are designed to protect at a disadvantage in the global marketplace. Countries adopting nationalized standards for IT products include **China, India, Korea, Nigeria, and Vietnam**.

Intellectual Property

Patents: BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for businesses, governments, and consumers. It is therefore critical that countries provide effective patent protection to eligible computer-implemented inventions, in line with their international obligations. Some countries have adopted or are considering policies that could significantly constrain the freedom of patent holders to negotiate licenses for their inventions.

For example, **China** has proposed a variety of policies that could unfairly restrict the ability of patent holders to exercise their legitimate rights to enforce their patents or to negotiate mutually acceptable licensing terms.

Trade Secrets and Other Proprietary Information: BSA members also rely on the ability to protect valuable trade secrets and other proprietary information to maintain their competitive position in the global marketplace. US trading partners that fail to implement and enforce strong rules protecting trade secrets against misappropriation or unauthorized disclosure put BSA members' business operations at risk and prevent them from having legal recourse when misappropriation or unauthorized disclosure occurs. Given the ease by which such information can be transmitted, this presents serious market challenges not only in the specific country in question, but globally as well. Current or proposed policies that require the disclosure of sensitive information as a condition for market access represent enormous market access barriers for BSA members. Countries with weak trade secret protection rules, or that have or are proposing policies requiring disclosure of sensitive information include **China, Indonesia, and Nigeria.**

License Compliance/Illicit Use of Software: The use of unlicensed software by enterprises and governments is one of the major commercial challenges for BSA members. According to the latest information, the commercial value of unlicensed software globally is at least US$52 billion, a staggering sum.[3] Not only does the use of unlicensed software impact the revenue stream of BSA members, deterring investments in further innovation, but it also exposes enterprises and agencies engaged in such activity to higher risks of malware infections and other security vulnerabilities.[4]

BSA has engaged with US trading partners in an effort to reduce the incidence of unlicensed software use by enterprises and government entities, with varying degrees of success. These efforts include promoting voluntary compliance measures, such as promoting effective, transparent, and verifiable software asset management (SAM) procedures, where enterprises and government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed. Governments can lead by example and adopt such measures for their own procurement and IT maintenance systems, which can send a powerful example to enterprises in their countries. **Mexico** has been a leader in this regard.

Voluntary measures are only part of the solution. In order to have a meaningful impact on reducing the use of unlicensed software, US trading partners must adopt and enforce effective legal mechanisms to enable BSA members to enforce their rights and compel license compliance. The legal mechanisms need to be efficient, without overly burdensome procedures or undue delays, and must result in penalties or damages that are sufficient to compensate the right holder and deter future infringements.

BSA remains highly concerned about the inadequacy of enforcement in a wide variety of countries. Often this is the result of deficiencies in the legislative framework, or of the inability or unwillingness of authorities to enforce the law. In addition to the countries explicitly cited in this submission, BSA is concerned about the inadequate enforcement against enterprises using unlicensed software in **Taiwan**. The agency that oversees intellectual property enforcement is understaffed, underfunded, and unequipped to investigate digital infringements.

The judiciary also has an important role to play to ensure right holders have access to proper remedies against intellectual property infringement. For example, triple damages were available for copyright infringement under **Poland's** copyright law, but in 2015, the Polish Constitutional Tribunal declared that the triple damages provision was unconstitutional. As a result, Polish Copyright Law

[3] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[4] For example, see "Unlicensed Software and Cyber Security Threats", IDC 2014 available at http://news.microsoft.com/download/presskits/dcu/docs/idc_031814.pdf.

lacks clarity regarding the availability of multiple damages, which hampers enforcement efforts in the country. In December 2017, a decision issued by the Polish Supreme Court approved damages equivalent to double the value of the proper license fee. Although the recent Supreme Court decision is a welcome development, and it may have a positive impact on future court decisions, the lack of clarity remains.

Government and SOE Legalization: The use of unlicensed software by governments is particularly challenging to BSA members. Because these are the entities upon which BSA members rely to provide protection and enforcement of their intellectual property rights, if the governments themselves are unwilling to comply with the law there is often little that BSA or our members can do on our own. We urge the US Government to use all available trade mechanisms, including Special 301, to aggressively engage with US trading partners on behalf of US companies on this important issue.

Some governments, like **Mexico**, have taken commendable steps to establish mechanisms within government agencies to ensure that only licensed software is purchased and used. Other governments have made commitments to ensure licensing compliance in government agencies and government-funded entities, including SOEs. **China** has made multiple commitments to the United State to ensure the legal use of software by government agencies and SOEs. BSA remains concerned that software legalization programs are not being implemented in a comprehensive manner in **China**.

Conclusion

BSA welcomes the opportunity to provide this submission to inform the development of the 2018 Special 301 Report and the US Government's engagement with important trading partners in 2018. We look forward to working with USTR and the US agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee to achieve meaningful progress in ensuring that BSA members and others that rely on intellectual property receive **fair and equitable market access** to important US trading partners and **adequate and effective protection and enforcement of their intellectual property rights.**

TABLE OF CONTENTS

Priority Watch List

ARGENTINA

Due to sustained high levels of unlicensed software use by enterprises and a lack of political commitment to make necessary changes to the legislative framework, BSA recommends that Argentina remain on the Priority Watch List.

Overview/Business Environment

Despite economic and fiscal reforms that have been recently implemented, Argentina's inflation rates are still very high, and the country's economy is improving slowly. Although President Macri's Administration has recently implemented some sensible economic and fiscal policies, they have not yet resulted in significant improvements and the business environment in Argentina for BSA members remains challenging.

Market Access

BSA has previously noted that Argentina's Customs and Tax Authority (the Administración Federal de Ingresos Públicos, or AFIP) refuses to apply the special rules that the Income Tax Act provides for "authors' rights" to international transfers of author's rights. The AFIP contends that the legal nomenclature "author" is limited to physical persons, and that a legal person (e.g., a corporation) cannot be an author; as a result, a corporation cannot hold these "authors' rights." This problem could be solved by amending the Income Tax Act to establish a concrete withholding rate for software license payments, similar to what was done several years ago for music and motion pictures. President Macri has pledged to implement income tax reforms and this may present an opportunity to implement the necessary changes to address the issue, but the issue remains unaddressed so far.

There is also a clear need for the United States and Argentina to reach an agreement on a treaty to avoid double taxation.

Copyright and Enforcement

According to the most recent data, the rate of unlicensed software use in Argentina is 69 percent. This rate has remained static since 2011 and is significantly higher than the regional average. This represented a commercial value of US$554 million in unlicensed software in 2015.[1]

Enterprise Licensing/Legalization: Enterprise use of unlicensed software remains a significant challenge, especially for small- and medium-sized companies. The changes are even more acute in certain provinces of lesser economic development.

Government Licensing/Legalization: With respect to government legalization efforts, the software industry continues to seek from the Argentine Government (in particular, from the Subsecretaría de la Gestión Pública – the Under Secretariat for Public Administration) an executive decree that would mandate legal software use in government agencies. The decree should also require government agencies to implement verifiable software asset management procedures when government agencies conduct audits of the software they have installed. This procedure would ensure, among other things, that all copies in use are properly licensed. While the Argentine Government has issued several guidelines on this issue, these have not been effective at addressing the continued use of unlicensed software in government agencies.

Statutory and Regulatory Provisions: BSA members have identified the following important elements that would benefit from clarifications or express incorporation in Argentine copyright law:

- Extend the scope of reproduction rights to explicitly cover temporary copies;

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

- Protect against the act of circumvention, as well as the manufacture or distribution of devices aimed at circumventing technological protection measures (TPMs);
- Establish effective statutory damage provisions in civil infringement cases; and
- Recognize intellectual property (IP) ownership by legal entities on the same footing with natural persons to comport with international practice.

Compliance and Enforcement: BSA only engages in civil actions in Argentina. In general terms, provisional injunctions are available and are one of the most favorable characteristics of the domestic system. BSA brought 38 cases in 2017 and has approximately 30 cases currently pending in the courts of Buenos Aires, neighboring jurisdictions, and the Córdoba Province.

The criminal system is not an effective tool for enforcement against unlicensed use of software by enterprises. IP is not a priority for prosecutors and effective remedies are not available. Similarly, IP enforcement is not a priority for customs authorities.

Recommendation

Due to sustained high levels of unlicensed software use by enterprises and a lack of political commitment to make necessary changes to the legislative framework, BSA recommends that Argentina remain on the **Priority Watch List.**

CHILE

Due to ongoing challenges in enforcing against unlicensed software use by enterprises and Chile's failure to make meaningful progress in improving its laws and policies, BSA recommends that Chile remain on the Priority Watch List.

Overview/Business Environment

The overall business environment for software in Chile remained largely unchanged in 2017. According to the most recent data, the rate of unlicensed software in Chile has dropped only marginally from 59 percent in 2013 to 57 percent in 2015. This represents a commercial value of US$296million in unlicensed software.[1]

President Bachelet's Administration has not issued or changed any policies to specifically address unlicensed use of software. Inadequacies in the law remain unaddressed and remedies for unlicensed software use are inadequate. The business community hopes that President-Elect Piñera, who will take office in March 2018, will be more inclined than his predecessor to promote reforms to better protect intellectual property (IP) in Chile.

Copyright and Enforcement

The fundamental issue of concern for BSA members in Chile is the very high rate of unlicensed use of software by enterprises and the absence of meaningful actions by the government to address the problem.

***Enterprise Licensing/Legalization*:** Most service industry sectors, including architecture, design, engineering, and media continue to exhibit high rates of unlicensed software use. Problems also persist with the unauthorized pre-installation of software by hardware retailers, as well as in-house and external IT service providers that often load unauthorized copies of software onto computers or networks.

Government and State-Owned Enterprise Licensing/Legalization: The US-Chile Free Trade Agreement (FTA) obligates the Government of Chile "to actively regulate the acquisition and management of software for such government use."[2] Although there has been some progress on government software legalization in Chile, further steps are necessary. Chile should implement changes to its domestic regulations to comply with its US-Chile FTA commitments.

Establishing and implementing appropriate provisions to regulate the acquisition and management of software by the government is critical to real success. The adoption of effective, transparent, and verifiable software asset management procedures — during which government agencies conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed — could also provide a powerful positive example to private enterprises.

Statutory and Regulatory Provisions: The FTA also contains detailed requirements for legal protections against the circumvention of technological protection measures used by BSA members to ensure that only licensed users are able to access their software products and services.[3] Chile has still not implemented necessary legislation and regulations to meet its obligations under this provision. Therefore, in Chile it is easy to obtain illicit activation keys and services that offer the circumvention of technological protection measures.

---

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[2] United States – Chile Free Trade Agreement Article 17.7.4

[3] United States – Chile Free Trade Agreement Article 17.7.5

Compliance and Enforcement: BSA enjoys a good relationship with the main Chilean IP agency, INAPI (Instituto Nacional de Propiedad Industrial). In 2017, BSA conducted almost 75 civil compliance inspections of a variety of enterprises on behalf of its members.

In order to conduct civil inspections, civil *ex parte* actions remain a critical remedy for BSA. Unfortunately, these are hampered by a provision in Chilean law that requires filing *ex parte* search requests through a public electronic registry, allowing companies under investigation to learn about a search request before the inspection takes place. This notification requirement can significantly undermine the effectiveness of the search.

Damages awards remain too low to deter users of unlicensed software and there are no provisions for statutory damages. The FTA requires the availability statutory damages.[4]

Recommendation

Due to ongoing challenges in enforcing unlicensed software use by enterprises and Chile's failure to make meaningful progress in improving its laws and policies, BSA recommends that Chile remain on the **Priority Watch List**.

[4] United States – Chile Free Trade Agreement Article 17.11.9

CHINA

Due to a deteriorating market access environment for the software and IT sectors and continuing high levels of unlicensed software use by enterprises, BSA recommends that China be maintained on the Priority Watch List.

Overview/Business Environment

We have seen encouraging progress on judicial enforcement of intellectual property (IP) rights. However, the commercial environment in China for software and IT remains very challenging, especially with respect to policies and regulations that substantially hamper market access.

The Government of China has been building more effective judicial enforcement mechanisms for the protection of IP. Steps taken by China include: implementing court procedures supporting evidence preservation; issuing guidance by the Supreme People's Court (SPC) on awarding higher damages for IP infringements; and establishing three new specialized IP courts in Beijing, Shanghai, and Guangzhou, as well as 10 IP tribunals in Suzhou, Nanjing, Wuhan, Chengdu, Hangzhou, Ningbo, Hefei, Fuzhou, Jinan, and Qingdao.

We continue to urge the Government of China to adopt effective, transparent, and verifiable software asset management (SAM) procedures. Such procedures would include having government agencies conduct audits of the software they have installed. This would help ensure that all copies in use by agencies are properly licensed and relevant software is used efficiently and cost-effectively. By creating an inventory of software in use and reducing the instances of unauthorized or unlicensed software on government networks, implementing SAM will also help to reduce cybersecurity threats.

BSA is monitoring developments related to competition policy and the utilization of patents and other IP, as well as patent law reform. As do other industries, BSA urges meaningful reforms in the protection and enforcement of trade secrets in China, including how sensitive proprietary information that is required by government agencies for regulatory approval purposes is protected.

While the challenging commercial environment is not unique to the software industry,[1] it is particularly acute for BSA members and other foreign technology providers.

In 2017, the Government of China issued numerous policies and standards designed to implement the Cybersecurity Law, which went into force in June 2017. The law raises significant market access challenges for US and other foreign software and IT companies related to data localization, security, and privacy, which could be worsened or mitigated depending on how the implementing measures (many of which are still in draft form) are finalized.

In addition, various government agencies have proposed sector-specific cybersecurity regulations that require firms to replace existing IT systems with "secure and controllable" products and services. The term "secure and controllable" is associated with a number of vague or unreasonable requirements and has been frequently interpreted by regulated entities as an instruction from the government to procure domestic products and services. These policies are not in keeping with China's international commitments to avoid implementing security regulations that act as trade barriers.

China's existing regulatory regime also makes it extremely difficult for BSA members to participate in the digital market. China has proposed further restrictions to the existing system, which already effectively excludes foreign participation in cloud computing and other data services in China. While there have been some openings in the electronic commerce field, China continues to regulate Internet and cloud computing services as value-added telecommunications services (VATS) and precludes granting licenses to wholly owned or majority-owned foreign entities.

[1] AmCham China: China Business Climate Survey Report at http://www.amchamchina.org/policy-advocacy/business-climate-survey/

These policies, combined with broader "indigenous innovation" policies, contribute to an increasingly challenging market access environment for many BSA members.

BSA urges the US Government to continue to closely engage 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

BSA seeks a fair and level playing field for competition in the software and related technologies market. Market access restrictions are often imposed under the guise of ensuring the security of government systems and important economic sectors. While these are important priorities for all countries, the challenge is to ensure that security-related policies are directed toward achieving their goals and are not used as a pretext for adopting measures that act as unnecessary and illegal barriers to market access. Furthermore, market access for software and other IT products and services should not be limited to those with IP that is locally owned or developed, nor should it depend on the transfer of IP to domestic firms.

Security: In November 2016, the National Peoples' Congress passed the Cybersecurity Law, which went into effect in June 2017. The law imposes a variety of obligations on "network providers;" imposes additional security and testing requirements and national security "reviews" on the procurement of certain software and IT products and services for "Critical Information Infrastructure" operators; limits data flows; and establishes a prescriptive personal data protection regime. Since early 2017, the Cyberspace Administration of China (CAC) and other authorities have been issuing draft or final measures and standards to implement the law. Many of these measures leave important issues vague and unclear (e.g., the definition of "critical information infrastructure" or "important information" – see below), or appear to expand the scope of the law exacerbating the negative impact of these rules on the software industry (e.g., requiring that personal information and important information collected in China, and not just by critical infrastructure operators, must be held in China – see below).

BSA urges the Government of China to adopt rules implementing the Cybersecurity Law that enhance the cybersecurity capabilities of enterprises and other institutions in a manner consistent with international standards and approaches, and that do not impose unnecessary administrative compliance burdens nor discriminate against BSA members.

In April 2017, China's State Cryptography Administration (SCA) published a draft Encryption Law for public comment. The draft law is concerning for several reasons. First, it would fully or partially bar foreign competition in various categories of cryptography. Of the three categories defined by the law (core, common, and commercial cryptography), foreign businesses would only be allowed to participate in the commercial cryptography market, and even then only under strict regulations. Second, the draft law lacks a clear definition of the scope of commercial cryptography, leaving significant uncertainty about which products and services foreign companies might provide. Third, the licensing scheme for foreign commercial cryptography providers, as envisioned by the draft law, would require such providers to disclose source code to state licensers, putting their IP at significant risk. Finally, the draft law requires the government to develop and apply mandatory national technical standards, which would run counter to China's commitments under the World Trade Organization's Agreement on Technical Barriers to Trade.

Restrictions on Cross-Border Data Transfers: The Government of China has put in place a number of laws and regulations restricting the free flow of data across borders and forcing data to be stored locally. 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. Below, we summarize key laws and regulations impeding cross-border data flows.

The Cybersecurity Law requires "personal information and other important data gathered or produced by critical information infrastructure operators during operations" to be stored within China. In 2017, the CAC issued draft Critical Information Infrastructure Protection regulations that contain an exceptionally broad

definition of "critical information infrastructure" that would include cloud computing services. These regulations, if enacted as drafted, would effectively require that all cloud computing services providers (CSPs) operating in China store data from their operations in China, thus creating additional operational costs and access challenges for foreign providers.

In April 2017, the CAC issued draft Security Assessment Measures for Cross-Border Transfers of Personal Information and Important Data for public comment. The draft measures contain obligations relating to security assessments, impose additional localization requirements and restrictions on the transfer of "personal information" and "important data" across borders, and restrict remote access to such data stored in China from outside of China. The draft measures – if adopted in their current form – create unacceptable legal risk for CSPs dependent on cross-border data flows for their business operations and will serve as another key barrier to digital commerce.

In November 2016, the Ministry of Industry and Information Technology (MIIT) published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Cloud Service Regulation Notice). BSA and other associations submitted comments to the Government of China raising concerns[2] about the Draft Cloud Service Regulation Notice and its implications for the operation of foreign cloud computing businesses in the country. While the Draft Cloud Service Regulation Notice has not yet been finalized, it contains several provisions that would serve as highly problematic market barriers to foreign CSPs. These include provisions that, among other things, require CSPs to physically construct and maintain infrastructure in China; subject cross-border data transfers to a range of restrictions; limit the ability of foreign companies to market their services in China under their own brand; and create duplicate copies of all key equipment, business systems, and data. This potentially makes it cost-prohibitive and operationally impractical for foreign CSPs to operate in China, prevents them from participating on equal terms within the Chinese market, and impedes their ability to partner on reasonable terms with Chinese companies.

Procurement: In May 2017, the CAC issued the Interim Measures for the Security Review of Network Products and Services. Under the measures, all "important network products and services" purchased for national security-related networks and information systems will be subject to review by third-party assessors operating under the auspices of a cybersecurity review office, to be established by the government. The measures do not define "important network products and services" or delineate what systems are national security related. They also fail to specify how the third-party assessors will be designated, the steps that an applicant should follow to have products or services reviewed, or what remedies are available for any wrong decisions made by the cybersecurity review office. 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.

There are also long-standing procurement measures in place, such as the Multi-Level Protection Scheme (MLPS). The MLPS imposes significant restrictions on procurement of software and other information security products for an overly broad range of information systems the government considers sensitive. Among other requirements, procurements of such products are limited to those with IP owned in China. This applies to procurements by the government and increasingly to procurements by state-owned enterprises (SOEs) and the private sector, restricting market access for foreign information security products. As a result, many entities in China are unable to procure the most effective security tools to meet their needs.

Foreign Direct Investment Restrictions: US businesses seeking to operate in China are subject to a range of foreign direct investment restrictions, including equity caps, investment restrictions, in-country hosting requirements, and other similar regulations, as well as challenging processes for obtaining licenses and other prerequisites for entering the market. These restrictions are particularly acute for the telecommunications and IT industries, including for cloud computing services.

In December 2015, the MIIT issued China's Telecom Services Catalogue, which continues to treat cloud computing and other Internet-based services as VATS. The designation carries significant restrictions on

[2] Comments available at http://www.bsa.org/~/media/Files/Policy/Trade/CloudRegComments.pdf

foreign investments. For example, companies wishing to provide cloud computing services (in particular, infrastructure-as-a-service or platform-as-a-service offerings) must acquire an Internet Data Center (IDC) license. By regulation, foreign firms wishing to acquire such a license must establish a foreign invested telecommunication entity (FITE), which must contain no more than 50 percent foreign equity. BSA understands that the MIIT issues very few new IDC licenses to FITEs.

The MIIT's Draft Cloud Services Regulation Notice (discussed in the context of restrictions on cross-border data transfers, above) would further constrain the ability of foreign businesses to partner with domestic entities, introducing an unprecedented level of government interference into these partnerships without articulating any clear rationale. The Draft Cloud Services Regulation Notice would place a number of restrictions on technical partnerships between foreign technology companies and domestic IDC license holders. For example, it would mandate that the foreign company cannot lease or transfer its VATS license, or provide resources, premises, or facilities to its partner. These restrictions could undercut many, if not most, agreements that foreign technology companies currently have in place for providing cloud computing services in partnership with IDC service providers.

Finally, while these policies themselves create specific concerns, particularly in relation to licensing requirements that bar foreign businesses from competing in China on equal terms with domestic entities, the implementation of these policies can be equally concerning, and far more difficult to document. BSA members attempting to provide cloud computing or other VATS services must navigate a licensing process that can be lengthy, unpredictable, burdensome, and discriminatory. Businesses have encountered requirements or pressure to disclose IP, inconsistent interpretation of regulations between central and local regulators, lengthy or open-ended approval timelines, and a lack of transparency around decision-making while navigating the licensing process. These concerns represent a significant barrier to foreign access to the Chinese market.

Intellectual Property

Intellectual Property and Competition: Several agencies under the State Council, the National Development and Reform Commission, the State Administration of Industry and Commerce, the Ministry of Commerce, and the State Intellectual Property Office are in the process of developing rules regarding the abuse, or misuse, of IP under the Anti-Monopoly Law (AML). BSA members remain concerned that there may be divergent approaches to AML enforcement regarding IP, increasing business uncertainty and exposing right holders to administrative abuse, and allowing AML enforcement agencies to use AML enforcement for industrial policy or other protectionist purposes. Specific concerns include applying rules tailored to standard-essential patents to non-essential patents not encumbered with voluntary "fair, reasonable and non-discriminatory" licensing commitments. The US Government should continue to urge China to avoid using AML enforcement to undermine or prevent the normal and legitimate exercise of IP rights.

In November 2017, China passed a revised Anti-Unfair Competition Law (AUCL), which took effect on January 1, 2018. BSA members are concerned about the broad definition of "unfair competition" in the AUCL and the overlap with the AML. BSA urges the Government of China to set out more detailed implementation regulations to provide for clear and detailed definitions and unified scope of application.

In addition, technology businesses are subject to insufficient and contradictory laws relating to contracts and liability for infringement. China's Contract Law generally permits contracting parties to negotiate on who will bear the liability for infringing products. However, for technology import and export contracts, the Contract Law states that the position under the Technology Import and Export Regulations will apply instead – where technology importers must indemnify their customers and bear the liability for infringing products. This lack of freedom to contract discriminates against overseas licensors and could be viewed as a non-tariff technical barrier.

Source Code and Enterprise Standards Disclosure Requirements: Through a series of draft and final legislative documents on various topics spanning the last several years, the Government of China has made clear its intention to establish a legal basis for requiring the disclosure of source code and enterprise

standards associated with foreign software products across a wide range of uses. Requirements for the disclosure of source code and enterprise standards pose significant inherent risks to IP, with little security value. It is critical that the US Government intervene to eliminate current disclosure requirements and arrest further advancement of draft requirements.

The most significant measure relating to source code disclosure is China's Cybersecurity Law, which includes requirements that products associated with "critical infrastructure information" be subject to security reviews. Current implementing measures under the law contemplate that source code disclosures can be required as part of the security reviews, but leave the mechanism for this to future legislation. The possibility of such mandated source code disclosures is cause for substantial concern among BSA members and other US companies.

Additionally, as mentioned above in the area of cryptography, foreign commercial cryptography providers would be required to disclose source code to state licensers under the SCA's draft Encryption Law.

Equally concerning are revisions that China enacted to the Standardization Law on November 4, 2017. The revised law appears to require public disclosure of enterprise standards (which are described as an individual company's proprietary product or services specifications). Enterprise standards represent highly proprietary and confidential information that often is protected by trade secret law or other forms of IP.[3] Their public disclosure would prove exceptionally damaging to the integrity of IP held by US technology companies.

No other country in the world requires public disclosure of comprehensive lists of technical standards used in products or services. Not only would such disclosure compromise valuable IP, it would also establish a significant cost burden on businesses. Because the application of certain specifications and standards varies from product to product, the engineering and legal verification overhead for such a disclosure requirement would be significant, likely driving some companies out of the market altogether.

Copyright and Enforcement

According to the latest information, the rate of unlicensed software use in China declined from 74 percent in 2013 to 70 percent in 2015. However, this rate remains extremely high, far above the regional (61 percent) and global (39 percent) rates. The estimated commercial value of unlicensed software in China was nearly US$8.7 billion in 2015, the largest value by far among all US trading partners.[4]

Government and SOE Licensing/Legalization: BSA remains concerned that software legalization programs are not being implemented in a comprehensive manner. We urge the Government of China to implement comprehensive legalization programs for the government itself and SOEs that include: (1) audits, certification, and other credible processes to verify software license compliance; (2) SAM best practices; (3) sufficient budgets to properly procure licensed legal software; (4) performance indicators to hold government and SOE officials accountable for ensuring measurable progress on software legalization; and (5) a prohibition on mandates or preferences for the procurement of domestic software brands as part of the legalization process.

Statutory and Regulatory Provisions: Draft amendments to the Copyright Act remain under review by the State Council Legislative Affairs Office. There is an urgent need for China to update and modernize its Copyright Law. BSA urges the Government of China to quickly enact copyright reform that:

[3] China does not currently have a standalone trade secrets law, and trade secrets remain one of the most at-risk types of intellectual property for US businesses operating in China. While companies do have legal recourse to pursue cases of trade secrets violations, existing procedures make it difficult for victimized businesses to achieve any favorable legal resolution. This most significant challenge is difficulty companies face under the Chinese court system in establishing a valid and effective evidence chain, due to the complexity of evidence rules and rules governing the burden of proof. It is critical that China develop a standalone trade secrets law to afford adequate protections to foreign businesses, provide clear and fair rules regarding evidentiary chains and burden of proof, and ensure sufficient enforcement.

[4] Data on the rates of unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

- Clarifies that use of unlicensed software by enterprises is a violation of the reproduction right;
- Clarifies that unauthorized temporary reproductions, in whole or in part, are violations of the reproduction right (this will likely become increasingly important to BSA members as business models shift to providing software in the cloud);
- Increases statutory damages, at least so that they are in line with the revised Trademark Act and ongoing amendment of the Patent Act;
- Ensures that protections for technological protection measures (TPMs) extend to access controls, that the unauthorized sale of passwords and activation codes are explicitly defined as TPM circumvention, and that constructive knowledge circumvention is sufficient to demonstrate a violation of the law; and
- Strengthens procedural provisions; for example, to explicitly grant courts more authority to compel evidence preservation and grant preliminary injunctions.

BSA notes that recent amendments to China's Criminal Code do not address the widespread use of unlicensed software by enterprises in China. The Government of China has not made the necessary changes to the IP-related provisions of the Criminal Code (e.g., Articles 217 and 218 and accompanying judicial interpretations) and other related provisions. This represents an important missed opportunity to apply appropriate criminal remedies to copyright infringements, which undermine the market and the incentives to bring to, or develop in, China cutting-edge software solutions. BSA continues to urge the Government of China to reconsider the decision not to amend the IP-related provisions of the Criminal Code. BSA urges China to impose criminal liability on enterprises that use unlicensed software, consistent with international best practices. BSA urges that the following issues be addressed and improved:

- Reduce thresholds that are too high (e.g., in the case of illegal income) or unclear (e.g., in the case of the copy threshold);
- Provide all commercial scale infringements with a criminal remedy. Because the requirement to show that the infringement is carried out "for the purpose of making profits" is not clear, law enforcement authorities have been reluctant to impose criminal liability on commercial enterprises using unlicensed software in the course of their business operations; and
- Define, distinct from copyright infringement, criminal violations for unauthorized circumvention of TPMs and trafficking in circumvention technologies, software, devices, components, and services, particularly the unauthorized sale of passwords or product activation codes or keys.

In addition to correcting the scope of criminal liability for IP violations, the Government of China should also amend the Criminal Code to lift the jurisdictional bar limiting foreign right holders from commencing a private civil claim against those being prosecuted for copyright crimes in local district courts, like Beijing and Jiangsu.

Compliance and Enforcement: The Government of China is building more effective judicial enforcement mechanisms for the protection of IP by establishing three specialized IP Courts in Beijing, Shanghai, and Guangzhou, as well as 10 IP tribunals in Suzhou, Nanjing, Wuhan, Chengdu, Hangzhou, Ningbo, Hefei, Fuzhou, Jinan, and Qingdao. BSA and its members have had some success with the IP Courts and tribunals.[5] 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 addressing the use of unlicensed software in China remain. In civil cases, several critical improvements are needed. 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. While

[5] For example, Adobe & Autodesk vs. Beijing Ourpalm Technology Co.; Adobe & Autodesk vs Shanghai Fengyuzhu Exhibition Co.; Dessault & Autodesk vs. Zhongshan Xinhai Precision Manufacture.

some courts have increased damages awards based on SPC guidance, others, when facing similar infringement situations, grant much smaller statutory damages in lieu of a proper compensatory award. This problem highlights the need to increase statutory damages beyond those currently proposed in the draft amendments to the Copyright Act. Additionally, in cases in which a civil order is issued, right holders and authorities often face on-site resistance against evidence preservation and have only a limited amount of time to conduct software infringement inspections.

The amended Criminal Transfer Regulations are well intentioned, but do not adequately address existing challenges to the effective transfer of administrative cases to criminal investigation and prosecution. The Regulations leave unclear whether transfers are required upon reasonable suspicion that the criminal thresholds have been met. Thus, some enforcement authorities believe reasonable suspicion is insufficient to result in a transfer, instead requiring proof of illegal proceeds. Administrative authorities, however, do not employ investigative powers to ascertain such proof. The "reasonable suspicion" rule should be expressly included in amended transfer regulations.

Recommendation

Due to a deteriorating market access environment for the software and IT sectors and continuing high levels of unlicensed software use by enterprises, BSA recommends that China be maintained on the **Priority Watch List**.

INDIA

BSA members continue to face challenges in providing products and services to the Indian market and experience persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends that India remain on the Priority Watch List.

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 impact cross-border data flows, the preference for domestic products and services contained in certain procurement policies could restrict market access for BSA members.

Government procurement policies remain outmoded and inefficient because of local content preferences and technology preferences. Most recently, the Department of Industrial Policy and Promotion (DIPP) issued the Public Procurement (Preference to Make in India) Order 2017[1] (Make in India Order), which requires government departments to give preference to local suppliers in procuring goods and services. In addition, the Draft National Policy on Software Products[2] would promote the use of domestically developed software products in public sector procurements and strategic sectors like defense, telecom, power, and healthcare. Such policies do not offer a level playing field to US technology providers, who are bringing cutting-edge technologies and services to India.

The existing and future software and IT market in India also remains at risk because of a variety of existing or proposed data localization requirements. From legacy policies on government-owned weather data, to proposals regarding machine-to-machine (M2M) systems and existing public procurement requirements, the Government of India appears to be considering requiring the localization of data sets within India for a variety of reasons. These policies are ineffective at promoting security, unfairly disadvantage firms that provide or rely on global cloud computing services, and will harm India's economic growth and development.

The Government of India is in the process of developing a personal data protection framework for India. This is an important step for improving the legal underpinnings of the digital economy in India, but the policy must be carefully crafted to maximize privacy protections and facilitate innovation and digital trade. A high level expert committee on personal data protection (Data Protection Expert Committee) recently released a white paper for public consultation. The Data Protection Expert Committee will prepare a draft Data Protection framework, which is expected to address issues around the scope and definition of "personal data," obligations and liabilities for data controllers and processors, international data transfers, and personal data breach notifications, among other issues. We estimate that the legislative process may take approximately two years to complete. During this time, BSA looks forward to continued dialogue with the Government of India to ensure that the eventual personal data protection regime adopted in India is enforceable and equitable to all stakeholders.

There appear to be positive developments with respect to the patentability of software-related inventions. In July 2017, the Office of the Controller General of Patents, Designs, and Trade Marks (CGPDT) issued Revised Guidelines for Examination of Computer Related Inventions Guidelines (2017 CRI Guidelines). The Guidelines removed the "novel hardware" requirement for patent eligibility in applications relating to computer-related inventions. This is encouraging, as it is in line with international practice and Indian patent law and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how this revision is implemented in practice.

The use of unlicensed software by enterprises in India remains high. The most recent information indicates that the rate of unlicensed software use in India is 58 percent, representing a commercial value of

[1] http://dipp.nic.in/sites/default/files/publicProcurement_MakeinIndia_15June2017.pdf

[2] http://meity.gov.in/sites/upload_files/dit/files/National%20Policy%20on%20Software%20Products.pdf

(…continued)

unlicensed software of over US$2.6 billion.[3] This alarming figure highlights the scope of the problem and underscores the importance of making more progress against the use of unlicensed software by enterprises in India.

Market Access

The Government of India, at the central and state levels, has adopted a variety of policies affecting the commercial environment for BSA members and the IT sector more generally.

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, issued by the DIPP in June 2017 in an effort to promote local manufacturing, requires every government department to give preference to local suppliers when procuring goods and services. Previous attempts at introducing a preferential market access policy in India include the Public Procurement Bill in 2012 and the draft National Policy on Software Products. However, 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.

Recently, the Government of India has sought to implement policies with respect to electronics[4] and cybersecurity products.[5] In relation to cybersecurity products and services specifically, the Ministry of Electronics and Information Technology (MEITY) is the entity responsible for implementing the Draft Public Procurement (Preference to Make in India) Order 2017 – Notifying Cyber Security Products in furtherance of the Order,[6] released in September 2017 (Draft Cybersecurity Products Notification).

"Local supplier" requirements under the Draft Cybersecurity Products Notification raise several challenges for BSA members. The requirements include mandatory incorporation and registration in India, ownership of intellectual property (IP) rights by the Indian entity (use, distribution, and modification), domestic revenue accrual from exploitation of such rights, and ambiguity with respect to computation of value addition, among other implementation challenges. Moreover, the scope of products and services enumerated in the notification is extremely wide and may be subsequently revised to include other types of software products and services.

Such developments could significantly affect India's ability to acquire best-in-class products and services, and impact the investment environment in India, particularly in the context of cybersecurity products. For BSA members, such policies would directly impact their ability to effectively participate in public procurement exercises on an equal footing with domestic competitors.

In an effort to highlight these challenges and advocate for a fair and reasonable policy environment with respect to public procurement, BSA submitted written comments on the Draft Cybersecurity Products Notification[7] and participated in stakeholder meetings organized by the government.

---

[3] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[4] See http://meity.gov.in/writereaddata/files/PPO_Electronics%20Product%20Notification.pdf

[5] See http://meity.gov.in/commentssuggestions-invited-draft-public-procurement-preference-make-india-order-2017-notifying

[6] See http://meity.gov.in/writereaddata/files/Draft%20Notficationn_Cyber%20Security_PPO%202017.pdf

[7] See http://www.bsa.org/~/media/Files/Policy/Data/10262017BSACommentsonIndiaMEITyDraftCyberSecurityProductsNotification.pdf

(…continued)

Data Localization: There are a variety of examples where the Government of India imposes, or proposes to impose, data localization requirements. In 2015, the Department of Electronics and Information Technology (the predecessor to MEITY) issued a request for proposal for provisional accreditation of cloud service providers (CSPs), which mandated that "all services including data will have to reside in India."[8] In May 2017, MEITY released an open empanelment invitation for new cloud service offerings from CSPs, which also included a requirement for data localization of all eligible service providers.[9]

The draft M2M Roadmap, issued by the Department of Telecommunication (DOT) in January 2015, proposed to require that all M2M gateways and servers be located only in India "in the interest of national security." While the DOT removed this unnecessary and counter-productive requirement in the final M2M Roadmap,[10] data localization requirements are once again under consideration for implementing rules that the Government of India is currently working on.[11]

Even in the context of personal data protection, the Data Protection Expert Committee poses specific questions about the value and scope of introducing data localization requirements in Chapter IX of the white paper out for public consultation.[12]

There is strong evidence that such policies are harmful to India, as they reduce productivity and dampen domestic investment in the country.[13] The US Government should use all available mechanisms, including formal bilateral dialogues, to urge the Government of India to carefully consider the narrow circumstances where it may be important for certain data to be maintained in India, and to refrain from imposing broad requirements that hinder innovation and digital trade without enhancing privacy or cybersecurity.

Cloud Computing: In June 2016, the Telecom Regulatory Authority of India (TRAI) released a consultation paper requesting stakeholder input on a range of important questions regarding cloud computing. In its submission to the TRAI, BSA noted that many of the issues raised in the consultation paper, such as interoperability and platform-to-platform migration, are best addressed by CSP-to-customer arrangements (such as contracts) rather than through a regulatory approach. Furthermore, BSA raised our concern that the TRAI or other government agencies in India might recommend data localization norms or impose India-unique standards or approaches to address the questions raised in the consultation paper.

The TRAI released its recommendations in August 2017.[14] It is encouraging that the TRAI recommended a "light touch" approach to cloud computing regulation and emphasized the need for flexibility and choice by way of contractual agreements between CSPs and end-users.

Unfortunately, it is unclear whether the TRAI is still considering potential server and data localization mandates.

Privacy and Data Protection: In August 2017, the Supreme Court of India declared that the citizens of India have a fundamental "right to privacy."[15] This judgment, along with reports of high-profile cyberattacks

---

[8] Page 8 of 13 Guidelines for Government Departments On Contractual Terms Related to Cloud Services http://meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf (last accessed December 20, 2017)

[9] Page 33 of 73 Invitation for Application/Proposal for Empanelment of Cloud Service Offerings http://meity.gov.in/writereaddata/files/Application%20for%20Empanelment%20of%20CSPs.pdf (last accessed 4th January 2018)

[10] See http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

[11] See http://www.trai.gov.in/sites/default/files/Consultation_Paper_M2M%20_18_October_2016.pdf

[12] See http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

[13] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

[14] See http://trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf

[15] See Justice KS Puttaswamy and Another v. Union of India and Others, WP (Civil) No. 494 of 2012, on August 24th 2017.

(…continued)

and a series of legal challenges to India's national identification project called Aadhaar, has triggered strong public interest in personal data protection in India. The Data Protection Expert Committee, under the chairmanship of a retired justice of the Supreme Court and comprising representatives from key ministries and one industry body, has been tasked with developing a new personal data protection law for India.

This is an important development for India. BSA supports the development of a robust personal data protection regime that will facilitate accountability and consumer trust in the digital economy. In December 2017, the Data Protection Expert Committee issued a white paper outlining over 200 questions for public consultation.[16] The white paper considers global personal data protection frameworks from various jurisdictions, including the European Union, United Kingdom, Canada, South Africa, Australia, and the United States. The white paper specifically discusses cross-border data flows, data localization norms, the scope and definition of "personal data," obligations and liabilities for data controllers and processors, and personal data breach notifications.

To ensure that the new personal data protection law achieves the objective of enhancing privacy while ensuring India can remain competitive as an innovation-led economy, it is critical that the Government of India solicit industry views, seek to ensure that the new regime is in alignment with international best practices, and facilitate international data transfers and digital trade.

BSA recently filed comments with the Data Protection Expert Committee and continues to engage with the MEITY and other stakeholders to ensure that the development and implementation of effective data protection policies and privacy rules protect consumers' personal data and also shape the growth of an emerging data-centric economy.

Encryption: In September 2015, India published a Draft National Encryption Policy that was withdrawn shortly after publication. The draft raised a number of concerns, including restrictions on use of commercially available encryption (e.g., by restricting key lengths) and mandates to disclose proprietary information.

India is currently working on a new draft encryption policy that could potentially introduce market access barriers if issues are not properly addressed. However, a new policy for encryption is likely to be formalized only after India develops a dedicated personal data protection law. BSA is currently engaging with relevant Indian authorities to encourage a globally aligned regime in India.

Intellectual Property

Patentability Guidelines for Computer-Related Inventions: The CGPDT's 2017 CRI Guidelines – the product of several years of deliberation, stakeholder engagement, and study – represent an improvement from previous versions and provide some finality to a long public discussion on this issue.

Notably, the 2017 CRI Guidelines removed the "novel hardware" requirement for computer-related inventions. This is encouraging, as it is in line with international practice, and recognizes the possibility of software-enabled inventions receiving patent protection in India. It will be important to monitor how the revised guidelines are applied in practice.

Compliance and Enforcement: The lack of statutory damages and inadequate damage awards in civil enforcement continue to be a challenge for BSA and our members when attempting to enforce our rights against enterprises using unlicensed software in India.

Unfortunately, the potential positive impact of an October 2015 ordinance that established commercial courts with jurisdiction over IP rights and related matters and limited the time the courts can take to decide cases was undermined by a Supreme Court judgement from July 2015,[17] which required software

[16] See http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf

[17] Indian Supreme Court Judgement in IPRS v Sanjay Dalia & Anr.,1st July 2015

companies to file civil license infringement cases in district and high courts. District and high courts have widely varying levels of experience and knowledge for handling such cases, and there is uneven willingness to impose preliminary injunctions and important forms of preliminary relief. Furthermore, the system suffers from significant procedural delays.

Criminal enforcement has also not proven to be practical for enforcing against enterprise use of unlicensed software. A recent draft report from an expert committee on cybercrime in October 2017 recommended the establishment of State Cyber Crime coordinators to improve India's criminal enforcement mechanisms. However, even if a robust criminal enforcement system were established, an effective civil enforcement system will continue to be of importance in dealing with compliance-related issues.

Recommendation

BSA members continue to face challenges in providing products and services to the Indian market and experience persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends that India remain on the **Priority Watch List**.

INDONESIA

Due to a poor market access environment for the software and IT sector, and rampant levels of unlicensed software use, BSA recommends that Indonesia remain on the Priority Watch List.

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 raise the cost of providing digital products or services to the Indonesian market. In addition, the use of unlicensed software by enterprises in Indonesia is among the highest in the region, affecting the legitimate market and putting these enterprises at risk for security vulnerabilities and malware.

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.

Data Localization Requirements and Cross-Border Data Flows: The Government of Indonesia issued Government Regulation 82 on the Operation of Electronic System and Transaction (GR82) in October 2012. The Indonesian Ministry of Communication and Information Technology (MCIT) subsequently issued two implementing regulations under GR82: (1) Regulation No. 36 of 2014 on the Registration Procedure for Electronic System Operators; and (2) Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems in December 2016 (Electronic Data Protection Regulation). These regulations all raise concerns regarding data and IT infrastructure localization mandates, unreasonable obligations on data service providers, and other matters. Such requirements will increase costs, harm the quality of data services, and interfere with the assurance of data security without enhancing information security or protection. The MCIT has verbally conveyed that the Government of Indonesia is in the process of revising GR82 to relax the requirements such that the most stringent localization rules will apply only in relation to data concerning national security. However, to date, no revisions have been released even as GR82 came into force in October 2017.

In addition, in October 2015, the Government of Indonesia initiated a draft bill on the Protection of Private Data (Draft Privacy Law), which remains with the Indonesian House of Representatives. Should it pass, the bill would represent Indonesia's first overarching law on data privacy. Thus far, however, the Government of Indonesia has not consulted the public on the Draft Privacy Law. It is also presently unclear how it would interact with the Electronic Data Protection Regulation.

In addressing the issue of information security and personal data protection in Indonesia, BSA encourages the Government of Indonesia to reconsider its various regulations (including GR82 and its implementing regulations) according to the comments and recommendations that BSA has submitted to date. BSA also encourages the Government of Indonesia to seek public comments on the Draft Privacy Law, and to ensure that the Draft Privacy Law and all other laws concerning personal data protection (including the Electronic Data Protection Regulation) are aligned. BSA urges the Government of Indonesia to ensure that Indonesia's overall framework for information security and personal data protection will facilitate, rather than impede, the cross-border data transfers that are critical to growth and innovation in the global digital economy.

Source Code Disclosure Requirement: The MCIT is also considering two other GR82 implementing regulations on: (1) information security management; and (2) software used in electronic systems. If implemented, these regulations would require the disclosure of software source code by electronic system providers responsible for managing or operating computer systems used in connection with public services. BSA is deeply concerned about this requirement. Many global companies of leading-edge security technologies would withdraw from bidding opportunities that require them to turn over or disclose sensitive intellectual property, such as source code and other design information.

Over-the-Top Regulation: In mid-2016, the MCIT published a draft regulation (which the MCIT updated in mid-2017) regarding the Provision of Application and/or Content Services Through the Internet. This draft regulation threatens to impose unreasonable requirements on virtually all Internet-enabled services and service providers, including local physical presence and registration mandates, content filtering and censorship requirements, and mandatory use of local payment gateways, among others.

E-Commerce Regulation: In June 2016, the Government of Indonesia published a draft regulation on Electronic System Based Trade Transaction. This draft regulation threatens to impose unreasonable requirements on e-commerce providers relating to physical presence and registration, security clearance, infrastructure localization, and product liability, among others. It also contains provisions on personal data protection that need to be aligned with the Draft Privacy Law and Electronic Data Protection Regulation discussed above.

Copyright and Enforcement

According to the latest data, 84 percent of the software used in Indonesia is not licensed. This is one the highest rates in the region and represents a commercial value of US$1.1 billion in unlicensed software.[1]

Statutory and Regulatory Provisions: Indonesia enacted a new copyright law in 2014. The law clarifies that software is copyrightable and that "compilations of creations or data in a format that can be read by computer programs or other forms of media" are protected. Because the law provides circumstances in which temporary reproductions are not considered infringement, it appears to implicitly accept that some temporary reproductions are considered infringement. Importantly, the law now provides prohibitions against the circumvention of technological protection measures (TPMs), including both access controls and copy controls. However, the law does not include clear provisions prohibiting trafficking in devices, technologies, and services primarily designed to circumvent TPMs. The copyright law doubles criminal penalties for copyright infringement.

Recommendation

Due to a poor market access environment for the software and IT sectors, and rampant levels of unlicensed software use, BSA recommends that Indonesia remain on the **Priority Watch List**.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

UKRAINE

Due to the continuing weak software copyright protection, lack of implementation of state government intellectual property rights plans and reforms, ineffective enforcement, and continuing high volume of unlicensed software use by both public sector entities and commercial enterprises, BSA recommends that Ukraine remain on the Priority Watch List.

Overview/Business Environment

The Ukrainian economy has only experienced minimal growth, largely because of stagnated structural reforms to address land markets, the financial sector, anti-corruption measures, and privatization, coupled with the ongoing burden of the conflict in Eastern Ukraine. The fiscal deficit is projected to widen to 3.5 percent of GDP in 2017.[1] The Government of Ukraine failed to attract foreign investment due to insufficient and incomplete government reform efforts. Furthermore, the Government of Ukraine has experienced challenges cooperating with the International Monetary Fund, support of which is crucial for the local economy. In addition to the bleak economic situation, the lack of effective intellectual property rights (IPR) enforcement continues to negatively impact the Ukraine software industry.

Copyright and Enforcement

According to BSA's most recent Global Software Survey published in 2016, the estimated rate for unlicensed software use in Ukraine is 82 percent, representing a commercial value of US$129 million in unlicensed software.[2]

Government Legalization: In 2017, the Government of Ukraine continued to fail to effectively address the high level of unlicensed software use by government agencies. Required resources, financial and otherwise, were not allocated to facilitate software legalization in the public sector. Many government agencies in Ukraine continue to use unlicensed software. There were no discussions or events dedicated to this topic in 2017, and no government official or specific agency was empowered to handle related issues.

The number of computer hardware public tenders have been increasing in Ukraine. On August 18, 2017, the Ukrainian Government adopted Resolution No. 647 that eliminated the previously set maximum for state funds that some agencies are allowed to spend on purchases of computer hardware.[3] Public tender documents related to computer hardware public tender demonstrate that many government entities seek to acquire computers without any software, including without operating systems, which creates a significant risk that unlicensed software will eventually be installed onto such "naked" computers.

Another problem arising from public procurement procedures is that the winners of the tenders are not required to verify in any way that they are selling genuine products. As a result, the state budget is not used to purchase products that are efficient and secure in many instances. Government customers and the software industry are negatively affected by this practice.

Statutory and Regulatory Provisions: The planned IPR reforms announced by the Ukrainian Government in 2015 have not been implemented.

The Law on State Support of Cinematography in Ukraine was adopted in March 2017. This new law includes provisions that apply to the software industry and address online copyright infringement. The law also implements a notice and takedown system in Ukraine. However, the system implemented is very

[1] http://pubdocs.worldbank.org/en/994131507019473787/Ukraine-Economic-Update-October-2017-en.pdf

[2] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[3] Original text of Resolution 647 is available at http://zakon3.rada.gov.ua/laws/show/647-2017-%D0%BF .

cumbersome for right holders and, therefore, very few notices have been sent since March 2017. Websites offering unlicensed software content continue to flourish in the country.

Although much work remains to be done, there were several positive developments in Ukraine in 2017. On December 15, 2017, a new Procedural Code came into force and some of its provisions address IPR protection. These provisions could have a positive impact if they are effectively implemented by the courts. Furthermore, Presidential Decree No. 299/2017 (September 29, 2017) created the Highest Intellectual Property Court that will focus on disputes related to the protection of IPRs. Until the Highest Intellectual Property Court is functional, however, all IPR cases will continue to be decided by the courts of common jurisdiction, which unfortunately are not able to address these cases in timely manner.

Compliance and Enforcement: In 2017, there was a notable decrease in the number of IPR enforcement actions conducted by the Ukrainian police. BSA members report only five criminal raids against commercial end-user companies suspected of unlicensed software use, and three criminal raids conducted against resellers suspected of distributing unlicensed or counterfeit software. These figures are even lower than the seven criminal raids initiated against end-user companies and the 11 raids against resellers in 2016.

This decrease in enforcement is a direct result of the elimination of IPR protection from the top priorities of the Ministry of Internal Affairs, and from the lack of *ex officio* cases related to copyright infringements. Right holders cannot effectively rely on law enforcement agencies' assistance in protecting their rights in Ukraine.

In 2017, the special Cybersecurity Police Department declared that it focused on specific online enforcement tasks, such as combating websites offering unlicensed content, but no significant results have been reported by this agency.

In addition, in 2017, the State Intellectual Property Services agency (SIPS) ceased its activities, but no new trademark and patent office was created to replace it. As a result, the SIPS' former activities will be handled by the Ministry of Economic Development and Trade (MEDT), but to date the MEDT has not implemented any noticeable IPR protection initiatives or provided practical support to right holders.

Recommendation

Due to the continuing weak software copyright protection, lack of implementation of state government IPR plans and reforms, ineffective enforcement, and continuing high volume of unlicensed software use by both public sector entities and commercial enterprises, BSA recommends that Ukraine remain on the **Priority Watch List.**

VIETNAM

Due to extremely high levels of unlicensed software use by enterprises and government institutions, the lack of criminal enforcement against willful use of unlicensed software by enterprises, and a number of increasingly troubling IT regulatory measures, BSA recommends that Vietnam be placed on the Priority Watch List.

Overview/Business Environment

Over the past several years, Vietnam has enacted, implemented, or proposed measures for regulating the IT sector, which are likely to reduce fair and equitable market access for BSA members wishing to provide software products and online services in Vietnam. Vietnam has recently adopted market access restrictions on server location, which threaten the ability of foreign IT service companies to compete in the marketplace.

BSA receives good support from the Ministry of Culture, Sports, and Tourism (MCST) and the High-Tech Crimes Department of the Public Security Ministry (High-Tech Police) in enforcing against the unauthorized use of software by enterprises in Vietnam. Unfortunately, the use of unlicensed software remains very high, both in the private and public sectors.

Market Access

Vietnam has enacted, implemented, or proposed several laws or regulations that impose restrictions on the cross-border transfer of data or require server localization in Vietnam. In 2017, Vietnam proposed business requirements including unwieldy local cybersecurity standards and compliance and certification requirements for IT service professionals in a draft Law on Cybersecurity. These measures hamper the ability of BSA members and others in the IT sector to provide innovative products and services to the Vietnamese market.

Information Security: Vietnam's legislative body, the National Assembly, enacted the Law on Network Information Security on November 19, 2015. The law has been in force since July 1, 2016. BSA's concerns with the law and several implementing rules include obligations to disclose proprietary information as a condition to entering the market, overly broad definitions of personal information, and overly broad provisions requiring "cooperation with the Government" regarding access to data, which include requirements to decrypt encrypted information held by third parties. These provisions impact the ability of BSA members to provide services in Vietnam.

Cross-Border Data Flows and Server Localization: On September 1, 2013, Decree No. 72[1] went into effect. The decree imposes onerous server localization requirements and restrictions on cross-border data flows that will undermine the ability of BSA members to provide digital services in Vietnam. In early 2015, the Government of Vietnam proposed further elaborations on these requirements in a Draft Circular. The Draft Circular also requires companies providing certain online services to establish a local entity in Vietnam. These measures may impact the ability of BSA members to provide software-based services online (e.g., cloud computing), which offer many economic benefits, especially to small- and medium-sized enterprises in Vietnam.

Cybersecurity: In 2017, the Ministry of Public Security issued a series of drafts for a proposed Law on Cybersecurity. The various drafts all propose to require IT product and service providers to comply with local cybersecurity standards and regulations and to apply for certification by local agencies. This would significantly raise the cost of doing business in Vietnam without improving cybersecurity. BSA urges the Government of Vietnam to adopt policies, standards, and methods developed by industry and adopted internationally. BSA, together with like-minded trade associations, has proposed in formal comments that the Government of Vietnam align *ex-ante* measures with industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards or the US

[1] Decree No. 72 72/2013/ND-CP on the Management, Provision, and Use of Internet Services and Online Information.

National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

Copyright and Enforcement

The rate of unlicensed software use is extremely high in Vietnam, far exceeding the global (39 percent) and regional (61 percent) averages. The latest data indicates that the rate of unlicensed software use in Vietnam is 78 percent, representing a commercial value of unlicensed software of US$598 million.[2]

Enterprise Licensing/Legalization: Enterprises in Vietnam, including foreign-invested enterprises, tend to place a very low priority on purchasing and using licensed software. Both the MCST and the High-Tech Police are supportive of BSA efforts to enforce against the unauthorized use of software by enterprises in Vietnam.

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code, the Criminal Code, and the Administrative Violations Decree.[3] The Civil Code operates in parallel.

The Criminal Code, as currently in force, 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. Further, while Article 170a of the current Criminal Code improved Vietnam's statutory framework in some respects, it is now weaker than the previous provision, the February 2008 Criminal Circular.[4] The lack of criminal enforcement against copyright infringement over the years is also due to the fact that the Criminal Code only applies to natural persons, not to entities.

In November 2015, Vietnam adopted a new Criminal Code, which came into effect on January 1, 2018. The new 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 new 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 intellectual property 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: BSA significantly relies on administrative enforcement to combat the unlicensed use of software by enterprises in Vietnam. BSA is working in partnership with the Vietnam Copyright Office and the Inspectorate of the MCST to address the use of unlicensed software in Vietnam. The Partnership in Protection of Software Copyright was established in 2008. Unfortunately, fines issued in administrative actions to date remain too low to constitute an effective deterrent against future infringements. The fines were in the range of VND20-50 million (roughly US$1,000 – US$2,000), which is

[2] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[3] 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).

[4] The 2008 Circular criminalized all acts of "infringement" by referring to Articles 28 and 35 of the Intellectual Property Code, including all acts of infringement defined therein, as well as violations involving circumvention of technological protection measures, decryption of encrypted satellite signals, and other acts.

less than 10 percent the maximum applicable fine. The Government of Vietnam should use existing authorities including the amendments to the Criminal Code (Article 225) to enhance the fines imposed on commercial infringers, as greater fines can act as a strong deterrent against unlicensed software use.

While BSA received good support from government agencies in 2017 for a National Crackdown Campaign, 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 has managed to bring only two cases to civil court since 2015. 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.

Recommendation

Due to extremely high levels of unlicensed software use by enterprises and government institutions, the lack of criminal enforcement against willful use of unlicensed software by enterprises, and a number of increasingly troubling IT regulatory measures, BSA recommends that Vietnam be placed on the **Priority Watch List**.

Watch List

BRAZIL

Due to a challenging market access environment for BSA members and continued challenges with high levels of unlicensed software use by enterprises, BSA recommends that Brazil remain on the Watch List.

Overview/Business Environment

President Temer's Administration has demonstrated a certain willingness to engage in a more open dialogue with stakeholders, which could result in an improvement in the current policy framework, but, the overall market environment in Brazil remains challenging. A variety of existing and proposed measures related to cybersecurity, privacy, and domestic procurement preferences have created, or threaten to create, *de facto* market access barriers to BSA members' products and services. In 2018, discussions and implementation of relevant policies may also be delayed as a result of the general elections that will take place in October. On the other hand, the environment for intellectual property (IP) protection and enforcement has generally improved in Brazil, with BSA and its members enjoying cooperation with law enforcement and working within a generally satisfactory judicial system. More remains to be done, however, to improve the efficiency and reduce the costs of IP enforcement, and to bring down the high rates of unlicensed software use in the country.

Market Access

A variety of existing and proposed measures related to privacy and public procurement preferences have created, or could bring about, *de facto* market access barriers to BSA members' products and services and may prevent them from providing the cutting-edge technologies and services increasingly demanded by Brazil's growing businesses. Concerns about privacy and security have been used to justify a variety of barriers to foreign software. This situation may, paradoxically, increase risks of security vulnerabilities and decrease the confidence of Brazilian consumers that their sensitive personal data will be appropriately protected.

Privacy Legislation: Brazil's long-debated personal data protection regulation reflects the perceived need for legislation that will govern the personal data of Brazilian citizens. Since industry and civil society successfully urged the Brazilian Congress to drop onerous provisions for data center localization from the final text of the Internet Framework Law (Marco Civil da Internet), focus has shifted to the Personal Data Protection Bill to address outstanding aspects of personal data and privacy protection.

BSA provided comments to the Government of Brazil on both the proposed Personal Data Protection Bill that was drafted by the Ministry of Justice and subsequently introduced in the Brazilian House of Representatives, and on a separate version of the bill that is being analyzed by the Brazilian Senate. Eventually, both texts will be consolidated. BSA has been urging Brazil to ensure that the framework for protecting personal information that it ultimately adopts will facilitate, rather than impede, the cross-border data transfers that are critical to growth and innovation in the global digital economy.

Although current drafts of the Personal Data Protection Bills under consideration by the Brazilian Congress have been improved, concerns still remain. Concerns include extra-territorial application of the Brazilian law; potential for explicit consent being required to legitimate a wide range of data treatment operations; restrictions on cross-border data flows; unreasonable liability on data processors; and other issues referring to the implementation of the law that could create legal uncertainties. These issues need to be addressed to avoid adverse impact on US companies operating in the Brazilian market.

Data and Server Localization Requirements: The Guidelines on Government Procurement of Cloud Services were issued in draft format in early 2017 and are currently pending. If finalized and implemented as drafted, the guidelines will create server and data localization requirements that will negatively impact procurement of cloud computing services by all Federal agencies. BSA submitted comments on the draft guidelines urging the Government of Brazil to remove the localization requirements but, unfortunately, there are no indications that the regulation will be modified to address the issue.

Finally, in late 2017, the Brazilian Central Bank proposed a new regulation that would prohibit all organizations it regulates from procuring cloud services that involve data storage or other types of data processing outside Brazil. BSA urged the Brazilian Central Bank to modify the regulation and remove the prohibition. The regulation is expected to be finalized in 2018.

Government Procurement Restrictions: Presidential Decree 8135/2013 (Decree 8135) regulates the use of IT services provided to the Federal government by privately and state-owned companies, including the provision that Federal IT communications be hosted by Federal IT agencies. In 2015, the Ministry of Planning developed regulations to implement Decree 8135, which include technical specifications for standardized services; contract rules, conditions, and prices; interoperability standards; management of agency solicitation of services; and periodic price review. The regulations present multiple serious problems for BSA members, especially the deviation from global standards and requirements to disclose source code and other IP. In 2016, the then new Secretary of Information Technology for the Ministry of Planning announced that the Federal government would revoke Decree 8135. A new decree was expected to be published by the end of 2016, but the new decree is still pending to this date. The new decree and implementing regulations should allow Federal agencies to procure innovative IT products and services, including cloud computing, and avoid restrictive data localization policies.

Government Procurement Preferences: Presidential Decree 8186/2014 establishes an 18 percent price preference for the following categories: software licenses, software application development services (customized and un-customized), and maintenance contracts for applications and programs.

Public procurement preference for local products and services, as well as technologies developed in Brazil, would also be required by the pending Guidelines on Government Procurement of Cloud Services, which were published in draft format in early 2017.

In addition, the Brazilian Congress is currently discussing potential changes to Brazil's Procurement Law. According to current law, the public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems can only be limited to local goods and services if such products and/or services are classified as "strategic" by a decree published by the government. A bill currently pending Congressional approval could remove the need for a decree classifying products and services as strategic. Should the bill be approved, any public procurement of IT and automation products and services used for the implementation, maintenance, and improvement of IT systems could be limited exclusively to local goods and services, creating a market access barrier for foreign companies.

Copyright and Enforcement

According to the most recent data, the rate of unlicensed software use in Brazil is 47 percent. This represents a commercial value of US$1.7 billion in unlicensed software.[1] This is a far greater value of unlicensed commercial software than what has been measured in any other country in the region. Although improvements have recently occurred, BSA's enforcement programs in Brazil are still being negatively impacted by a very slow court system that prevents cases from being settled quickly and efficiently.

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 software asset management procedures, where enterprises conduct audits of the software they have installed to ensure, among other things, that all software in use is properly licensed.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

BSA's efforts in Brazil also include a comprehensive risk awareness communication campaign called "Changing Perception." 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 the use of unlicensed software while giving individuals the opportunity to proactively report unlicensed use.

BSA's relationship with the enforcement authorities in the past year improved due to increasing 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 not sufficient 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.

As the software industry transitions to subscription-based software services and continues to devise other innovative ways to meet customers' changing demands for software (such as leveraging cloud computing and other Internet-enabled data services) the ability to enforce software licensing in the digital environment will continue to be key. BSA and its members look forward to working with the Brazilian Government to advance the enforcement of licenses in the digital environment.

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. Although the entity has the support of the Minister of Justice, the level of funding for the activities promoted by the agency is much lower than it used to be in past years. It is critical that the CNCP be properly funded, and that the agency continues to work closely with industry and vigorously expand its work beyond its traditional focus of counterfeiting and piracy of physical goods.

Recommendation

Due to a challenging market access environment for BSA members and continued challenges with high levels of unlicensed software use by companies, BSA recommends that Brazil remain on the **Watch List**.

GREECE

Due to persistent and growing high levels of unlicensed software use in public and private sectors, still insufficient (although growing) enforcement activity, and the continuing need to implement policies to ensure that government agencies use only licensed software, BSA recommends that Greece remain on the Watch List.

Overview/Business Environment

The rate of unlicensed software use in Greece is among the highest levels for European Union (EU) member states, requiring urgent implementation of policies to encourage both the private and public sectors to procure and use properly licensed software.

Copyright

The rate of unlicensed software use in Greece rose to 63 percent in 2015 (from 62 percent in 2013, 61 percent in 2011, and 58 percent in 2009). This represents a commercial value of US$189 million in unlicensed software.[1] The effects of this trend are fewer job opportunities and decreased revenues for local software and IT businesses, further contributing to the huge financial problems faced by the country in recent years. The sale of unlicensed software through online platforms contributes to the high rate of unlicensed software use in the country.

Government and State-Owned Enterprise Licensing/Legalization: The Government of Greece should implement a policy requiring all government agencies to use properly licensed software. Consistent with government-led working group discussions, this policy should assign the General Inspector of Public Administration the responsibility of overseeing an audit of the government's use of software and the development of an awareness campaign to educate public officials about the risks associated with the use of unlicensed software. The adoption of effective, transparent, and verifiable software asset management procedures – through which government agencies conduct regular audits of the software they have installed to ensure, among other things, that all software in use is properly licensed – would also provide a powerful positive example to private enterprise.

Statutory and Regulatory Provisions: An amendment to the Greek Copyright Law that includes a section titled "Sanctions Against Copyright Infringements Over the Internet" was enacted in 2017. The amendment provides right holders with an expedited process through which a special committee may order the removal of copyright infringing content or that access to such content be denied. However, the provision does not apply to violations conducted by end-users regarding materials that can be downloaded or streamed, to files that can be exchanged through peer-to-peer networks, or to materials stored in the cloud.

Under previous law, Internet service providers were not allowed to disclose the Internet Protocol addresses of their users who infringed copyrights. This prohibition hindered enforcement activities. The law was amended, and it now allows the disclosure of such addresses and other data, such as traffic and location data, when a copyright infringement amounts to a felony. This amendment is a positive development.

BSA advocates for amendments to the relevant laws related to the certification of tax compliance by third-party auditors. Specifically, BSA recommends that the assessment of the firms that must undergo third-party audits for tax compliance purposes also include an assessment on software license compliance.

Compliance and Enforcement: Although further improvements including an increase in raids are still needed, the Financial and Economic Crimes Unit (SDOE) was much more active in 2017 than it was in 2016. It conducted approximately 30 raids, the vast majority of which were successful. The SDOE imposed administrative penalties to infringers amounting to approximately EU€ 200,000 for the use of unlicensed

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

software. In addition, BSA was notified of raids that involved software whose rights are held by its members and this information was used to file claims for damages against raided infringers. It is critical that the SDOE continues to improve its performance.

The SDOE should increasingly focus its efforts on large-scale violators. Unfortunately, the SDOE has avoided investigating enterprises potentially using more than 50 illegal software products (i.e., larger enterprises), apparently to avoid triggering the legal threshold for criminal liability that would require initiating complicated and time-consuming criminal investigations and prosecutions. This policy needs to change and BSA urges the SDOE to refocus its efforts to pursue large enterprises using unlicensed software.

In addition, it is important that the Special Intellectual Property Rights and Electronic Commerce Department receives the funding it needs to carry out its mission. Although it uses external resources to conduct raids, it would be important for the SDOE to be able to rely on its own properly trained staff to conduct inspections. Industry is prepared to work with the SDOE in training programs, but the SDOE needs to be able to hire additional staff. For example, in 2017, BSA and other stakeholders conducted several training programs targeting SDOE staff.

The Special Intellectual Property Rights and Electronic Commerce Department should also resume issuing letters to companies requesting inventories of software in use along with respective licenses and invoices, as well as follow-up warning letters in cases of non-responsive companies. When appropriate, the Department should conduct inspections targeting such companies. The Department should also readopt the practice of publishing the results of raids on its website and issuing public releases to raise public awareness. Furthermore, the Department should more efficiently enforce the policy that inspectors check software license compliance, in addition to tax compliance, in daily tax inspections.

BSA commends Greece for changes to its Code of Civil Procedure, which entered into force on January 1, 2016, and improved the efficiency and timeliness of civil infringement suits. While parties typically settle the cases out of court, the Special Intellectual Property Departments within the Civil Courts of First Instance of Athens and Thessaloniki, and within the Court of Appeals of Athens, are valuable tools for efficient and quality final judgments. BSA hopes to see this program extended to other cities in Greece. The changes in the Code of Civil Procedure aim to expedite court procedures. The Special Intellectual Property Departments within the Civil Courts of First Instance of Athens and Thessaloniki, and within the Court of Appeals of Athens have been maintained. These departments are staffed with experienced and qualified judges and it is crucial that they are kept to ensure the benefits of the new Code of Civil Procedure are fully leveraged.

On the other hand, BSA observes persistent problems with criminal enforcement in Greece. Criminal cases are beset with delays and in the rare instance that a defendant is ultimately convicted, courts are reluctant to issue adequately deterrent sentences and penalties. In addition, the overall lack of intellectual propertyexpertise in the judiciary branch is an issue that should be addressed through training to improve IP enforcement and protection in the country.

Recommendation

Due to persistent and growing high levels of unlicensed software use in public and private sectors, insufficient (although growing) enforcement activity, and the continuing need to implement policies to ensure that government agencies use only licensed software, BSA recommends that Greece remain on the **Watch List**.

KAZAKHSTAN

Due to ongoing legislative and enforcement challenges, as well as Kazakhstan's high rate of unlicensed software use, BSA recommends Kazakhstan be placed on the Watch List.

Overview/Business Environment

The overall business environment for the software industry in Kazakhstan remained largely unchanged in 2017. According to the most recent data, the rate of unlicensed software installation in Kazakhstan has dropped only marginally from 74 percent in 2013 to 73 percent in 2015. This represents a commercial value of US$89 million in unlicensed software.[1]

Kazakhstan was admitted to the World Trade Organization (WTO) in November 2015 after lengthy negotiations with WTO members. It is clear from the Working Party Report and Protocol that Kazakhstan has committed to be compliant with WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) from accession, which includes intellectual property rights (IPR) enforcement commitments. IPR enforcement is an issue that will continue to be the subject of scrutiny as the US Administration and Congress deliberate on granting Permanent Normal Trade Relations to Kazakhstan.

Progress against distribution and use of unlicensed software has been insufficient due to lack of effective enforcement. Many issues remain unchanged, in particular because the initiatives proposed in the IPR plan are not fully supported by state officials.

Copyright and Enforcement

BSA's primary concern in Kazakhstan remains the significant volume of commercial entities that persist in using unlicensed software.

Due to right holders' efforts, government officials in Kazakhstan continue to gain a better understanding of the risks involved in using unlicensed software and the importance of intellectual property (IP) to the economy. In particular, the Council for Improvement of the Investment Environment, chaired by the Prime Minister and consisting of representatives from various state agencies and foreign investors, created a special IPR working group, of which BSA is a member. Certain amendments to the Criminal, Civil, and Administrative Procedural Codes of Kazakhstan concerning civil *ex-parte* searches and criminal and administrative liability were proposed and submitted on behalf of the software industry for government review. However, these proposed amendments have not been taken into consideration by the Government of Kazakhstan so far and the IPR working group has not been an effective mechanism to improve IPR protection in the country.

Statutory and Regulatory Provisions: Copyright infringement is a persistent problem in Kazakhstan.

The Criminal Code provides police with *ex officio* authority to commence criminal copyright cases, but this authority is not used against commercial end-user companies suspected of unlicensed software use. In addition, Article 198 of the Criminal Code, which establishes criminal liability for IPR infringement, is interpreted to refer only to the manufacturing and sale of illegal software, while end-user cases (i.e., those involving the reproduction and use, not sale or manufacturing, of unlicensed software) would remain unaddressed by the provision. As a result, police routinely refuse to initiate cases against such end-users, to perform inspections, and/or to secure the necessary evidence of unlicensed software use.

Pursuant to the Criminal Procedure Code of the Republic of Kazakhstan (CPC), a raid referral for an alleged infringement should be done in written form with supporting documents and materials, as and if available. However, in practice, authorities refuse to act based on criminal complaints that are not accompanied by

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

concrete evidence of the alleged offences. In cases involving unlicensed software, securing such evidence would require direct access to alleged infringers' computers and/or business documents. This irrefutable evidence should be gathered by authorities, as only they have the right to search computers and seize relevant documents. Under such circumstances, it is practically impossible for software companies to file this kind of evidence along with the raid referral.

Additionally, neither the Copyright Law, nor the CPC allow judges to adopt *inaudita altera parte* provisional measures (e.g., evidence gathering) that are critical to the successful pursuit of civil enforcement actions.

The Kazakhstani legal system is not compliant with the requirements of Article 50 of TRIPS. Under Kazakhstani law, it is not possible to submit a motion for securing evidence to the court before initiating the court proceedings, i.e., it is not possible to submit the motion prior to submitting the application. That means the motion must go to the court either in conjunction with the application, or at any time during the commenced court proceeding. Further, at the time of filing the application with the court, the right holder or a representative must provide the court with the document confirming the submission, together with a copy of application to the defendant (i.e., the potential violator of the right holder's IPR). Due to this required submission, the effect of "unexpectedness," which is attributable to the *inaudita altera parte* principle of TRIPS, is eliminated, and the potential violator becomes aware that the application was filed with the court and that a court proceeding may be subsequently initiated. This creates a risk that the potential violator may destroy evidence confirming the use of unlicensed software products.

These legislative gaps have led to software right holders' inability to take effective action against suspected infringers either in criminal or civil courts, since without a criminal or civil search it is nearly impossible to secure evidence of unlicensed software use. In order to ensure an adequate level of enforcement of IPR, Kazakhstan should amend its laws to be fully compliant with its obligations under the TRIPS Agreement. Kazakhstan should also clarify its criminal enforcement legal framework, both in terms of offence description and applicable procedure.

Moreover, despite repeated promises, Kazakhstan failed to reintroduce the administrative enforcement of IPR, a mechanism that existed until 2015, and, due to the high volume of cases it addressed, had a positive impact as it helped deter infringement.

Compliance and Enforcement: The law enforcement agencies responsible for IPR enforcement in Kazakhstan (i.e., the Ministry of Interior and the Agency of State Income under the Ministry of Finance) have achieved limited results related to IPR protection in the country. However, the actions undertaken by the Government of Kazakhstan have not impacted the high level of unlicensed software use in the country. The root of the problem, which continues to be the widespread use of unlicensed software both by government organizations and commercial enterprises, remains unaddressed. The number of enforcement actions conducted by Kazakhstani law enforcement bodies against enterprises that infringe upon BSA members' software copyrights dropped from 323 in 2013, to 51 in 2014, to six in 2015 and 2016, and there were only eight in 2017.

In 2017, software publishers faced lengthy procedures and baseless delays on IPR infringement complaint processing. Moreover, law enforcement investigations remain superficial and ineffective in cases of high-volume sales of counterfeit products made by various entities often established temporarily with the sole purpose to facilitate such sales.

Positive steps to address the high level of unlicensed software use in Kazakhstan should include law enforcement officials' capacity building, the establishment of a specialized agency dedicated to enforcing IPR, the use of global best practices to advance IPR enforcement, the implementation of obligations arising from international IPR treaties (e.g., WTO TRIPS Agreement), and other legal amendments, as outlined in the previous section.

Government and State-Owned Enterprise Licensing/Legalization: The use of unlicensed software by government agencies remains a significant concern. There have been multiple instances when a counterfeit product has been purchased through public tenders, followed by the Government of Kazakhstan demanding

the right holder to evaluate the genuineness of the products on unreasonably short deadlines and/or intervene and pressure the reseller to replace the counterfeit product with genuine software.

A new law on public procurement came into force on January 1, 2016, but it failed to provide efficient procedures to ensure that only legal software is purchased by government entities. Most worryingly, by failing to take the necessary steps to avoid purchasing counterfeit software, the government is being exposed to serious cybersecurity risks.

In light of the above, the government should re-evaluate their software acquisition procedures and, at minimum, immediately prepare, publish, and promote specific guidelines to educate government agencies on how to avoid purchasing counterfeit or unlicensed software.

Recommendation

Due to ongoing legislative and enforcement challenges, as well as Kazakhstan's high rate of unlicensed software use, BSA recommends Kazakhstan be placed on the **Watch List.**

REPUBLIC OF KOREA

Due to a challenging market access environment for software and IT products and a decrease in software license enforcement activities, BSA recommends that Korea be placed on the Watch List.

Overview/Business Environment

The overall commercial environment in the Republic of Korea (Korea) for BSA members, and the software and IT sector as a whole, is mixed. Korea has a strong IT market and a mature legal and enforcement system. Over the past several years, however, the Government of Korea has adopted a number of policies that have erected substantial market access barriers to foreign software and IT products. Such policies include local procurement preferences, local testing requirements, and requirements to comply with national technical standards even when commonly used international standards are available. Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains difficult to provide cloud-based services to the Korean market. Data residency, physical network separation, and other requirements for sectors such as government/public services, finance, healthcare, and education hamper the ability to provide cloud-based services to users in these sectors.

Data suggests that the use of unlicensed software by enterprises is declining in Korea (see below). Nevertheless, BSA remains concerned about the continued under-licensing of software in a variety of sectors and industries. This harms the legitimate commercial interests of BSA members, and also raises potential security risks for the entities engaged in such activities. To continue combatting the use of unlicensed software by enterprises, the number of enforcement actions and investigations undertaken by the authorities per year should be increased, and improvements to the current system should be made in order to create a more robust environment for copyright holders to take action against infringers. Such improvements may include improving how evidence is obtained and exchanged in civil actions.

The Government of Korea is actively developing its policies for moving Korea ahead in the digital economy. The Administration constituted a Presidential Fourth Industrial Revolution Committee in September 2017 to formulate and implement a strategic plan for this purpose. Government agencies have been reviewing regulations and considering regulatory reform or deregulation to stimulate innovation and growth in the digital economy. We urge the Government of Korea to use this opportunity to improve the overall business environment in Korea, especially for software and digital services.

Market Access

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

Cross-Border Data Flows and Server Localization: Although the Cloud Computing Promotion Act came into force on September 28, 2015, it remains a significant challenge for commercial cloud services providers (CSPs) to offer cloud services to public sector entities. This is due to the onerous certification requirements imposed by the Korea Internet Security Agency on CSPs providing cloud services to public sector agencies, including a requirement for physical network separation. Similar guidelines and regulations requiring physical network separation or data on-shoring exist in the finance[1] and healthcare[2] sectors. We remain concerned that, even after enactment of the Cloud Computing Promotion Act, significant barriers to cloud computing service adoption continue to exist.

[1] E.g., under the Financial Services Commission's Regulation on the Supervision of Electronic Financial Activities there is a physical network separation requirement for information processing systems used by financial services institutions. The Financial Services Commission relaxed this requirement in 2016 for "non-critical" information processing systems - while network separation is still required for such systems, this requirement can now be met through logical/virtual (instead of physical) separation. The physical network separation for "critical" information processing systems is still required by the regulation and this significantly limits the use of cloud computing in the financial services sector.

[2] E.g., under the Medical Services Act.

Personal Information Protection Regime: Korea's personal information protection (PIP) regime is one of the most stringent in the region and has significantly decreased the ability for BSA members to serve the Korean market. The two relevant pieces of legislation – the Personal Information Protection Act and the Act on Promotion of Information and Communication Network Utilization and Information Protection – impose onerous obligations on organizations with respect to the collection, use, and processing of personal information. These include burdensome and prescriptive security, data breach notification, and notice and consent requirements. Significantly, many of these requirements restrict cross-border transfers of personal information that are necessary for overseas-based service providers to serve the Korean market.

Regulators are currently reviewing and looking to streamline Korea's PIP regime, partly due to Korea joining the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) System. This presents a good opportunity for Korea to recalibrate its regime and adopt measures that allow for more flexible data handling by businesses, which is critical to investment and innovation in emerging technologies like data analytics 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-certified information security products that are procured by government agencies. However, no such requirement is applied to locally certified products. In 2014, the Government of Korea extended similar security conformity testing requirements to international Common Criteria-certified networking products for all central government agencies. The Government of Korea is expected to further extend the policy to all public organizations, local governments, and other government-related agencies, such as educational institutions.

Korea is a member of the Common Criteria Recognition Arrangement (CCRA), and therefore should recognize international certification from accredited laboratories and should not impose further requirements for Common Criteria-certified products. The additional requirements are not consistent with the spirit of CCRA, which is to "eliminate the burden of duplicating evaluation of IT products and protection profiles." To make matters worse, a separate conformity testing is required for each government agency, even if it is the same product that has been procured and verified for another government agency.

This discriminatory application of security testing in public procurements to only international information security products also appears inconsistent with Korea's international commitments to national treatment and non-discrimination, including the US-Korea Free Trade Agreement (KORUS FTA).

While the Government of Korea has indicated that it intends to change the policy, it has yet to issue any formal correction in writing. This has resulted in confusion as to what the applicable requirements are. Although BSA and other organizations have raised this issue several times with the Government of Korea, the issue remains unresolved.

Procurement Preferences: The Government of Korea implements a number of policies to promote small- and medium-sized enterprises. We urge the Government of Korea to avoid procurement preferences, whether based on licensing models or on the nature of the supplier. Such policies unfairly impact BSA members, and, more importantly, may deprive Korean public entities from buying or licensing the best possible solutions available.

Copyright and Enforcement

The rate of unlicensed software use in Korea has continued a slow, but steady decline. According to the latest data, 35 percent of software used in Korea in 2015 was unlicensed, which equates to a market value

of US$657 million in unlicensed software.[3] While this figure is below the regional and global average for unlicensed software use, it remains relatively high compared to similar economies in the region and around the world. BSA acknowledges and supports the Government of Korea's goal to reduce the rate of unlicensed software use to less than 30 percent by 2020.

To achieve this goal, the Government of Korea should lead by example by implementing and showcasing meaningful steps to reduce public sector use of unlicensed software; for example, by adopting effective software asset management systems. This will set a positive example for the private sector and will also help address the serious cybersecurity risks that result from using unlicensed software. To facilitate this, BSA requests that US Government open a dialogue with relevant representatives of the Government of Korea to identify mechanisms to address the issue of under-licensing of software across all sectors and industries.

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 Korea. The police, the prosecutors' offices, and the special judicial police under the Ministry of Culture, Sports, and Tourism 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. They, however, 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 to less than 30 percent by 2020, 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 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. In 2018, Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules in civil cases.

Recommendation

Due to a challenging market access environment for software and IT products and a decrease in software license enforcement activities, BSA recommends that Korea be placed on the **Watch List**.

[3] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

MEXICO

Although Mexico has provided tremendous support in administrative enforcement, persistent concerns about unlicensed software use by enterprises and ongoing concerns regarding judicial enforcement mechanisms lead BSA to recommend that Mexico remain on the Watch List.

Overview/Business Environment

The rate of unlicensed software use in Mexico has declined over the last several years, but unauthorized or counterfeit software remains available in most street markets, including Plaza de la Computación, Plaza del Videojuego, Plaza Meave, Tepito, San Juan de Dios, La Cuchilla, and other notorious markets, both physical and online. Concerns about unlicensed software use by enterprises and about judicial enforcement mechanisms are ongoing. The Government of Mexico should be commended for adopting software asset management (SAM) procedures in certain government agencies that comport with international best practices.

Copyright and Enforcement

The primary concern for BSA remains the unlicensed use of software by enterprises in Mexico. The most recent information indicates that the rate of unlicensed software in Mexico is 52 percent, representing an estimated commercial value of US$980 million in unlicensed software.[1] Illegal software is still commonly available at street markets ("carpeteros"), from online auction sites, and by download through specialized file-sharing sites. Although current concerns with the use of unlicensed enterprise software mostly relate to the digital environment, "white box" vendors (i.e., small local assemblers or non-brand name vendors of computer hardware) continue to pose a considerable problem.

Enterprise Licensing/Legalization: Enterprise under-licensing of software is a significant problem in Mexico. It is common to find companies that share the same software licenses.

Government Licensing/Legalization: Ensuring that government agencies buy and use only legal software according to their licenses should be an ongoing effort for all governments. Mexico has been a global leader in terms of adopting transparent and verifiable SAM procedures in various government agencies, including the Mexican Tax Authority Administration and the Mexican Institute of Industrial Property (IMPI). It is important that this trend continues in Mexico.

Compliance and Enforcement: The IMPI's efficacy and quality of legal analysis, as well as a clear improvement in inspection practices, has represented a very positive development in the enforcement of BSA member intellectual property (IP) rights recently. Legal criteria are clearer and enforcement practices are more effective. The IMPI has appointed law enforcement officers in all of its regional offices: Guadajara, Monterrey, Mérida, León, and Puebla. IMPI precautionary measures have become increasingly effective and time sensitive, and constitute an important infringement deterrent.

However, significant hurdles and challenges impede a truly effective enforcement system. Contrary to the Berne Convention, copyright certificates are still required in administrative and criminal cases in Mexico. Furthermore, a final ruling on a typical IP infringement case, brought to court after an administrative proceeding is concluded, is likely to take up to 10 years. Judicial procedures need to be streamlined to avoid excessive and unwarranted delays.

Notorious markets are well identified, but stronger actions need to be taken against them. Online infringement has been difficult to address because of the lack of basic investigative and prosecutorial tools.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Statutory and Regulatory Provisions: Mexico should move forward quickly to implement the World Intellectual Property Organization's Internet treaties to provide adequate legal protection and effective remedies against the circumvention of technical protection measures (TPMs) that control access to copyrighted works. These protections and legal remedies must apply to the act of circumventing TPMs, as well as the manufacture, import, distribution, offer for sale or rental, or provision of services that facilitate such circumvention. Although the Mexican criminal code punishes the manufacturing of circumvention devices, the circumvention of TPMs and trafficking in TPM tools are not addressed by Mexican law.

The Government of Mexico should aso ensure that legal remedies are available for right holders to address copyright infringement online. This should include implementing procedures, such as notice and takedown to address allegations of infringement. As the Government of Mexico considers the legal changes in this area, it is important to ensure that the appropriate safe harbors be provided to Internet service providers (ISPs) and that such safe harbors are not conditioned on any obligation by the ISP to monitor or filter infringing activity.

In addition, the requirement to have expert opinions for every software infringement criminal case, as well as to provide physical copies of legal and illegal software, complicates criminal prosecution. In many instances, these requirements cause premature termination of cases or undue delays. These requirements have a historic root, but they need to be changed drastically to adjust enforcement practices to current technology. This is a good time to carefully consider and implement these changes because the criminal system is currently undergoing a transition and many changes in criminal prosecution procedures are taking place.

Technical Assistance and Education: In 2017, BSA conducted training programs, and led or participated in a variety of round table discussions and other events that targeted a broad audience, including IMPI officers, officers from the Mexican Attorney General's Office (PGR), customs inspectors, inspectors from the Federal Consumer Protection Commission (PROFECO), judges, certified public accountants, industry association members, police officers, entrepreneurs, students, importers, and exporters. The programs covered a broad range of IP and innovation-related topics including IP rights and software protection, artificial inteligence, big data, the Internet of Things, cloud computing, privacy, innovation, cybersecurity, ISP liability, copyright infringement and damages, software-related tax matters, customs enforcement, licensing, administrative practices, notorious markets, and rule of law, among others. BSA carried out these activities in collaboration with various educational institutions, the Mexican Institute of Public Accountants, chambers of commerce, and associations. BSA also woked with think tanks including the Coalition for the Legal Access to Culture and Mexico Exponencial, and formalized alliances with the federal government by working with the Ministry of Education and the National Council for the Normalization and Certification of Working Competences.

Outreach campaigns launched in 2015 by the IMPI, such as the Expo-Ingenio national tour, proved to be a success in raising awareness regarding innovation and IP, and thus they were replicated in additional cities in 2016 and 2017.

Relationships with IMPI, INDAUTOR (the National Institute of Copyright), CONOCER (the National Council for Standardization and Certification of Labor Competences), PGR, and the Cyber Police improved and now remain on very good terms and with open channels of communication. Specific bridges of cooperation have been opened and built with PGR, specifically with the new cyber unit and the continuous training of their appointed prosecutors.

Recommendation

Although Mexico has provided tremendous support in administrative enforcement, persistent concerns about unlicensed software use by enterprises, and ongoing concerns regarding judicial enforcement mechanisms lead BSA to recommend that Mexico remain on the **Watch List**.

NIGERIA

Due to guidelines that, if fully adopted, would make Nigeria one of the most restrictive and closed markets for software, IT hardware, and services, BSA recommends Nigeria be placed on the Watch List.

Overview/Business Environment

As the largest economy in Africa, Nigeria presents significant opportunities for global IT companies. The country's IT industry has great potential to develop and grow if the government makes policy choices that enable it to integrate with the global digital economy. To that end, the Nigerian Government has made IT-enabled growth a top priority and is actively seeking to build a viable, domestic IT and telecommunications sector.

In 2014, the Nigerian Government released the Guidelines for Nigerian Content Development in Information and Communications Technology (Guidelines). The Guidelines were then issued in revised form in November 2015 by the Buhari Administration. In September 2017, the National Information Technology Development Agency (NITDA) met with a number of representatives of multinational companies and announced that the Guidelines were final, and no more changes or amendments would be made. The NITDA also provided a template for reporting company compliance. If the Guidelines are fully implemented, Nigeria would become one of the most restricted and closed IT markets in the world.

Specifically, the Guidelines impose stringent local content requirements for IT hardware, software, and services for government and private sector procurements; restrict employment of non-Nigerian citizens in the sector; force technology transfer; require the disclosure of source code and other sensitive design elements as a condition of doing business; and impose severe data and server localization requirements. In December 2017, the NITDA released a statement urging use of local data centers. The statement reminded Nigerian government organizations of their obligations under Section 14.1 of the Guidelines for Nigerian Content Development in Information and Communication Technologies, which makes it mandatory for data and information management firms to "host government data locally within the country and shall not for any reason host any government data outside the country without an express approval from NITDA." With this statement there is growing concern that the government may be looking to extend the Guidelines to the private sector soon.

As noted above, the Buhari Administration has announced that it will not consider any changes to the Guidelines and will move forward with immediate implementation, despite the concerns of US companies and the US Government. This has included asking BSA member companies to provide detailed implementation plans to prove compliance with the localization requirements in the Guidelines.

Market Access

Cross-Border Data Flows: The Guidelines impose severe cross-border data and server localization requirements that would impact a wide range of sectors. Section 12.1.4, for example, requires IT companies to "host all subscriber and consumer data" locally. Section 14.1.3 calls for all government data to be hosted "locally inside the country" within 18 months of the Guidelines' publication. Section 14.3.1 calls for the government to support local "data hosting firms" and to establish "appropriate service level requirements and standards for data service provisioning."

Local Content Requirements: The Guidelines impose significant local content requirements for software, IT hardware, and services. Section 10.1 requires manufacturers to obtain certification that IT hardware has been assembled in Nigeria and requires 50 percent of "local content either directly or through outsourcing to local manufacturers." These requirements are not limited to IT hardware; Section 11.4 requires local sourcing of software and directs government agencies to "carry out risk-based due diligence to identify… potential adverse impacts that may arise from using software… conceptualized and developed outside of Nigeria."

Importantly, these local content and sourcing requirements apply to both government and private sector procurements. In some cases, this is a clear violation of Nigeria's World Trade Organization obligations in the commercial sector, as well as national treatment obligations. It is disappointing that these provisions also affect government procurement given the recent renewal of the African Growth and Opportunity Act.

Security: The Guidelines contain problematic requirements from both a business/competition and security perspective. Section 11.3.1 can be interpreted to require multinational companies to reveal sensitive design elements, such as source code. Specifically, it requires multinational companies to "sign affidavits about the origin, safety, source and workings of software" being sold in Nigeria in order to "ascertain the full security of the product and protect national security." Section 11.4.5 further requires "assurances of the full security of source code." This extremely sensitive and proprietary information is at the core of IT companies' products and the compromise of such information would severely harm their continued commercial viability.

The requirement to disclose sensitive information regarding a vendor's software is not imposed on domestic Nigerian companies. Consequently, it would create serious challenges for foreign companies to be able to operate or sell in Nigeria and would diminish the availability of foreign-made leading-edge software for Nigerian customers.

Copyright and Enforcement

According to the latest information, the use of unauthorized software in Nigeria stands at 80 percent, far above the regional and global average. This represents a commercial value of US$232 million in unlicensed software.[1] BSA urges the Government of Nigeria to work with affected stakeholders to take effective steps to address this situation.

Recommendation

Due to guidelines that, if fully adopted, would make Nigeria one of the most restrictive and closed markets for software, IT hardware, and services, BSA recommends Nigeria be placed on the **Watch List**.

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

ROMANIA

Despite government software licensing/legalization efforts and cooperation on education and awareness endeavors, the lack of prioritization of copyright enforcement - particularly in the last three years - and persistently high levels of unlicensed software use by enterprises lead BSA to recommend Romania be placed on the Watch List.

Overview/Business Environment

The commercial environment for the software sector in Romania is changing with the shift to new Internet-based means of deploying software solutions and services to customers. The use of unlicensed software by enterprises remains a significant problem.

Copyright and Enforcement

According to the most recent data, the rate of unlicensed software use in Romania was 60 percent in 2015, representing a commercial value of unlicensed software of US$161 million.[1]

Statutory and Regulatory Provisions: On February 1, 2014, amendments to the Romanian intellectual property (IP) legal framework entered into force as a result of the then new Criminal Code. The amendments had the effect of decreasing the penalties for most copyright crimes.

The Criminal Procedure Code provides that only certified specialists may inspect computers during investigations of suspected unlicensed software use. As a result, police officers from the Economic Crimes Investigation Directorate, who previously conducted these inspections, are no longer permitted to do so. Instead, the inspections must be exclusively performed by the limited number of certified specialists in the Organized Crime Units of the Police or by the Romanian Copyright Office, which has only eight inspectors. This change in procedure significantly impedes enforcement efforts, as the number of organized crime officers available for inspections is considerably low. The way in which forensic analysis is presented frequently lacks clarity and essential information, such as type, version, or edition of software programs installed or stored. This results in a substantial decrease in the quality of evidence in software copyright infringement cases. In sum, the lack of specialists and the often-weak specialist reports result in a profound decrease in the total number of cases.

The amendments to the Criminal Procedure Code, referred to above, regarding the authorities that are allowed to conduct the inspections were adopted in May 2016.[2] Unfortunately, the amendments failed to resolve the problem, perhaps due policymakers' lack of understanding of the issue that needed to be addressed. The original amendment proposal would have allowed "judicial police officers, within the meaning of the law" to conduct inspections. Police officers from the Economic Crimes Investigation Directorate are judicial police officers and the matter would have been resolved had this language been adopted. The final amended language, however, authorizes "specialized police workers" to conduct inspections, which in practice does not change the situation at all. The Government of Romania should further amend the Criminal Procedure Code to allow "judicial police officers" to conduct inspections. In fact, the Ministry of Justice has recently initiated a process targeting major amendments to the Criminal Procedure Code. This is an opportunity to ensure these amendments clearly state that judicial police officers are allowed to conduct inspections, as recommended by BSA on multiple occasions. Despite repeated proposals and submissions filed by BSA in 2017, this issue remains unsolved.

Amendments to the Copyright Law are being considered in Romania. Two legislative drafts were submitted for public consultation in 2016 and two additional drafts were submitted in 2017. These amendments could

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.
[2] Ordinance 18 of May 18, 2016.

resolve the issue of computer search warrants (which are needed separately from and in addition to the premises search warrants), a source of a long-standing problems for BSA when attempting to conduct inspections regarding unlicensed use of software by enterprises. The amendment should also correct the allocation of competence of copyright crimes to the Courts of First Instance, which has negatively impacted copyright enforcement cases. Prior to 2010, the competence for prosecuting and trying IP crimes resided with 42 tribunal courts and their associated prosecutors' offices, where trained prosecutors and judges could focus on software infringement and other such cases. In 2010, this competence was shifted to as many as 188 generalist courts and their respective prosecutors' offices throughout the country. The lack of experience in and knowledge of copyright matters by these generalist courts has made the judicial process more challenging and has all but eliminated the possibility of focusing training resources on specialist prosecutors. Unfortunately, the proposed amendments have been pending for more than four years.

Government Licensing/Legalization: In 2017, some Romanian government institutions increased their focus on IP rights compliance and cybersecurity. Some visible steps were taken in this direction, including the acquisition of software upgrades, new licenses, and legalization. BSA applauds these efforts and urges their continuance. More remains to be done, however. In particular, the Romanian government should take steps to ensure that all national agencies are fully licensed and compliant.[3]

Compliance and Enforcement: In 2017, Romanian law enforcement officials conducted 46 inspections of enterprise end-users and two distribution channel raids in which unlicensed BSA member software were found, a decrease of more than 33 percent compared to 2016. There were five convictions reported by BSA members in 2017, almost half of the number reported in 2016 (nine). Moreover, out of the 48 raids in 2017, more than half were conducted at low-profile targets (i.e., those with only one or two PCs).

This illustrates a trend triggered by the aforementioned legislative changes (i.e., competence of conducting computer searches and competence to prosecute and judge copyright criminal cases) that constitute a major step backwards compared to the status quo before these amendments were introduced.

While authorities were active in partnering with BSA on education campaigns, enforcement actions have seriously declined over the last years. Formal written instructions from the Government of Romania may be needed to clarify to enforcement officials that the investigation and prosecution of software infringement remains a priority and that copyright infringement is an *ex officio* criminal offense in the Romanian legal system.

There is a high rate of turnover among the police officers appointed to investigate IP rights cases, as well as among prosecutors. Additionally, many prosecutors fail to support search warrant requests in IP infringement cases and, on the rare occasion a search is executed, the evidence from computer searches continues to be substandard and often useless.

Awareness Campaigns: In 2017, BSA, in partnership with the Romanian Police, initiated two campaigns to inform businesses and government agencies about the risks associated with counterfeit and unlicensed software. In addition, BSA and the Government of Romania continue to partner in programs targeting high school and college students to discuss cybercrime and IP rights.

Recommendation

Despite government software licensing/legalization efforts and cooperation on education and awareness endeavors, the lack of prioritization of copyright enforcement - particularly in the last three years - and persistently high levels of unlicensed software use by enterprises lead BSA to recommend Romania be placed on the **Watch List**.

[3] An independent review in June 2016 uncovered extensive improper use of licensed software by a Romanian government agency.

THAILAND

Due to ongoing concerns regarding the level of unlicensed software use by enterprises in Thailand, as well as concerns about the implementation of security-related legislation now pending that may undermine the operations of BSA members, BSA recommends that Thailand remain on the Watch List.

Overview/Business Environment

BSA remains concerned that fair and equitable market access for our members' products and services could be harmed if legislation regarding cybersecurity remains both vague and potentially over-prescriptive. BSA appreciates the opportunities to discuss and address concerns with the National Cybersecurity Bill, particularly with the Ministry of Digital Economy and Society (MDES) and the Electronic Transactions Development Agency (ETDA). We also recommend the timely enactment of the long-pending Personal Data Protection Bill (PDP Bill) that will provide a more solid legal framework for personal information protection. BSA urges the Royal Thai Government (RTG) to continue to conduct and enhance an open and transparent process when developing legislation, including soliciting the input of interested stakeholders including BSA members and taking into consideration industry views before such legislation is presented to the National Assembly of Thailand.

In addition, the persistence of high rates of unlicensed software use by enterprises continues to harm Thailand's software market. This is exacerbated by the widespread use of unlicensed software in the public sector.

In 2017, Thailand's Securities and Exchange Commission (SEC), an independent public-sector regulatory agency, continued to recommend that listed companies adopt software asset management (SAM) practices based on the International Standards Organization's (ISO) SAM standards. In 2015, the SEC set a good example by adopting SAM practices itself. However, other government agencies and most private sector companies have not followed this important lead. BSA appreciates the opportunities to work with the SEC to promote the benefits of SAM, which is the first line of defense against malware attacks and improves cybersecurity. SAM also aids in managing costs and allows enterprises to detect and address the use of unlicensed software.

BSA urges the RTG to develop an action plan with clear goals and strategies to reduce unlicensed software use by enterprises, and to lead by example by adopting SAM practices within all government agencies.

Market Access

BSA shares the goals of the RTG's Digital Economy initiative and supports the thoughtful enactment of necessary legislation regarding privacy and cybersecurity. Before finalizing such legislation, however, the RTG should minimize unintended effects that will harm the ability of BSA members and other technology sector companies to provide innovative and effective IT products and services, including software.

Security: The Council of State is reviewing the National Cybersecurity Bill. The bill is designed to strengthen the cybersecurity capabilities of government agencies and provide appropriate breach notification procedures. However, it raises concerns because it would give the Office of the National Cybersecurity Committee (ONCC) broad powers to access confidential and sensitive information without sufficient protections to appeal or limit such access. Granting the ONCC such broad powers will undermine public confidence and trust in IT generally and harm the ability of BSA members to provide the most innovative and effective software solutions and services to the market in Thailand.

Although the National Cybersecurity Bill remains pending, the RTG established the National Cybersecurity Preparation Committee. The Committee is responsible for, among other tasks, developing a national cybersecurity masterplan. This development raises additional concerns because in the exercise of its responsibilities, the Committee has the power to request state officials, persons, or relevant organizations to clarify and provide facts, opinions, advice, documents, and other information the Committee deems

necessary for its work. This broad and highly discretionary authority raises similar concerns to those regarding the ONCC's broad powers as described above.

Privacy: The PDP Bill is under review by the MDES. It is designed to build public trust and confidence in IT products and services and to implement the Asia-Pacific Economic Cooperation (APEC) Privacy Framework's principles for cross-border data transfers. BSA filed comments on the draft legislation in March 2015, and subsequently had meetings with the RTG to discuss the bill. In those meetings, BSA highlighted the importance of protecting personal information to foster the trust and confidence necessary for growth of the digital economy. BSA thus encourages the MDES to address industry concerns with the PDP Bill and move it to the National Legislative Assembly for enactment.

Copyright and Enforcement

BSA enjoyed very good cooperation with RTG authorities in 2017, including with the Economic Crime Division (ECD) of the Royal Thai Police, in addressing the unlicensed use of software in Thailand. The latest figures, however, indicate that the rate of unlicensed software use in Thailand was 69 percent in 2015, representing a commercial value of US$738 million.[1] The rate of unlicensed software use in Thailand is well above the average of 61 percent for the Asia-Pacific region, demonstrating that much greater efforts must be made. Beyond the use of unlicensed software by enterprises, the failure to fully implement the existing Cabinet resolution on legal software procurement, installation, and use in the public sector remains a problem for BSA members. The use of unlicensed software in the public sector may expose the RTG to unnecessary cybersecurity risks.[2] BSA urges the RTG to adopt SAM practices to eliminate the use of unlicensed software, strengthen enterprise risk management, and reduce cybersecurity risks.

Compliance and Enforcement: Thailand has a specialized intellectual property (IP) court, which has improved the effectiveness of IP litigation in Thailand. Unfortunately, although 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, criminal cases can be effective in Thailand, but the courts should apply more deterrent penalties for convictions. In recent cases, courts imposed only a fraction of the potential fines even in cases involving significant infringements.

Government Engagement: BSA engaged with several RTG agencies to promote sound policies and legislation for the data driven economy in the context of the Thai Digital Economy initiatives, as well as to promote adequate IP protection and enforcement. The agencies BSA engaged with in 2017 include the Department of Intellectual Property (DIP), the Department of International Trade Promotion's New Economy Academy (NEA), the ECD, the Central Intellectual Property and International Trade Court, the SEC, the MDES, and the ETDA. BSA worked with the SEC to organize a series of events to educate listed companies on the benefits of SAM, as well as with the DIP and the NEA to educate startups, small- and medium-sized businesses, and other private enterprises.

Technical Assistance and Education: In 2017, BSA, the DIP, and the ECD continued the joint national campaign "Safe Software, Safe Nation" to promote the use of licensed software. The campaign also explains the security risks posed by unlicensed software. BSA continued to promote SAM practices based on ISO standards and the effort targeted over 10,000 enterprises. BSA implemented campaigns to explain the benefits of SAM, including IT costs savings, reduction in cybersecurity and legal risks, and enhancement of corporate governance. Implementation of SAM practices would help reduce the use of illegal and

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

[2] The "*Unlicensed Software and Cybersecurity Threats*" report available at http://bsa.org/malware and the "Seizing Opportunity Through License Compliance" report available http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf demonstrate the link between unlicensed software and malware on personal computers (PCs).

unlicensed software in Thailand and would bring about many benefits to the enterprises themselves and to Thailand's economy in general.

Recommendation

Due to ongoing concerns regarding the level of unlicensed software use by enterprises in Thailand, as well as concerns about the implementation of security-related legislation now pending that may undermine the operations of BSA members, BSA recommends that Thailand remain on the **Watch List**.

Region of Concern

EUROPEAN UNION

Continuing concerns regarding a growing number of measures that create market access barriers lead BSA to highlight the European Union as a Region of Concern.

Overview/Business Environment

American data service providers are confronting growing challenges to providing innovative digital services in Europe. European authorities, both at the member state level and at the European Union (EU) level, are considering or adopting measures that represent *de facto* market access barriers. Several of these measures may significantly restrict data flows. While BSA members fully respect and share the EU's strong interest in protecting the security and privacy of EU citizens, these policies would block US firms from offering digital services in the EU without increasing either. Moreover, there are legal challenges underway that could invalidate important existing mechanisms for transatlantic data transfers, such as the US-EU Privacy Shield and standard contractual clauses, adding further uncertainty for US data services providers.

Market Access

The number of current or proposed policies that act as barriers to data services and digital trade are increasing in the EU and are of major concern to BSA members. BSA asks that the US Government closely follow these developments in Europe, work intensively to protect existing transatlantic data transfer mechanisms, and push back against policies that pose the most significant market access barriers.

Data Flows: Measures that impede the flow of data across borders impose substantial burdens on US providers of such services and negatively impact US jobs. European authorities are focused on data transfers to the United States and have not applied the same scrutiny to data transfers to any other market — large or small — including key markets such as China, Japan, South Korea, and Russia.

The US-EU Privacy Shield, which replaced the former Safe Harbor framework for data transfers from Europe to the United States, took effect on August 1, 2016, and represents a strong agreement to foster transatlantic data transfers while safeguarding consumer privacy. It was immediately challenged before the European Court of Justice (ECJ) in cases brought by two privacy activist groups (Digital Rights Ireland and La Quadrature du Net). While Digital Rights Ireland's challenge has been dismissed, the General Court is looking at the merits of the second challenge. Moreover, despite the European Commission's conclusions in the first annual review that the Privacy Shield framework has ensured adequate protection and safeguards for personal data transferred from the EU to the United States, further challenges before the national courts of EU member states are expected. These groups contend that the Privacy Shield should be invalidated for the same fundamental rights reasons that were the basis for the ECJ's 2015 invalidation of the previous Safe Harbor framework; specifically, they contend that US practices on law enforcement and national security access to data lack sufficient privacy safeguards. These legal challenges mean US companies will face continuing uncertainty in relying on the Privacy Shield for transatlantic data transfers.

The validity of standard contractual clauses, a second major mechanism used to transfer data from Europe to the United States and other countries, will be referred to the ECJ for review in 2018. The referral, which originates from the Irish Data Protection Commissioner, contends that standard clauses also are inconsistent with EU fundamental rights law when they are used as a basis for data transfers to the United States. Thus, companies relying upon standard clauses for this purpose are also at substantial risk in their European operations.

Both sets of legal challenges are predicated on the assumption that US surveillance laws do not effectively protect the personal data of EU citizens. However, no other country's surveillance practices have been scrutinized regarding their implications for the validity of data transfers from Europe, nor has the EU scrutinized or applied the same standards on the surveillance practices of its own member states.

Proliferating data localization laws in EU member states pose a barrier. The European Commission responded to this development by proposing, in September 2017, a Regulation for the Free Flow of non-

personal data. While the Commission proposal provides that national measures derogating from the proposal should only be permitted if there is a justified concern on public security grounds, member states are trying to broaden the scope of the exception to include all "public sector data," and permit exceptions for any "public policy." This would pave the way for data localization requirements and render the regulation effectively irrelevant.

Proposed e-Privacy Regulation: In January 2017, the European Commission proposed a sweeping revision of its existing e-Privacy Directive that would transform it into a regulation. The scope of the proposed regulation is very broad, sweeping in any electronic communications services 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 EU.

Moreover, many service providers that handle communications data may be unable to continue doing so based on their classification. This will lead to a prohibition on the processing of communications data for many important services, such as cybersecurity defenses. In addition, the regulation, as currently drafted, would create a foreseeable conflict of law regarding the obligations to respond to data requests from EU governments. It also raises questions about how it will operate in conjunction with the General Data Protection Regulation (GDPR), i.e., which rules will apply in particular circumstances. Violations of the proposed regulation's provisions would carry heavy administrative penalties at the level of the GDPR (see below).

GDPR Implementation: The GDPR was adopted in April 2016 and will apply across the EU in May 2018. EU member state data protection authorities and the Commission have begun to issue implementing measures. It is critical for both the United States and EU economies that the GDPR strike the right balance between protecting privacy and fostering the transatlantic digital economy. However, the data protection authorities have declined to establish a formal mechanism for consulting stakeholders on implementing measures. Moreover, we have concerns that there may be significant differences in how member states interpret and implement GDPR, further increasing compliance burdens and uncertainty for BSA members and other companies operating in the market. Clear implementing measures grounded in practical experience are extremely important, as companies need to be able to comply with them or risk heavy fines that could reach up to 4 percent of annual global corporate turnover.

Copyright -- Text Data and Mining: Text and data mining (TDM) involves the automated computational analysis of information in digital form to uncover patterns and underlying facts from large datasets. US companies are leaders in data analytics research and development, including in the EU.

TDM performed on lawfully accessed works neither conflicts with the normal exploitation of such works nor undermines the legitimate interests of authors. In 2016, however, the European Commission proposed a digital copyright directive that would create uncertainty about the legality of TDM under the existing copyright framework. The Commission proposal would permit only public interest research organizations engaged in scientific research to conduct TDM, thereby creating an implication that such activity, when performed by commercial entities, is infringing. Any entity that has lawful access to data should be permitted to perform TDM and analytics on that data, regardless of the entity's status as a research organization or commercial entity. Uncertainty about whether this rule would continue to prevail in the EU operates as a market access barrier to US data analytics companies.

Cybersecurity Act: In September 2017, the European Commission put forward a proposal for a Regulation on Information and Communication Technology (ICT) Cybersecurity Certification (Cybersecurity Act, for short). This proposal lacks clarity and could create market access barriers to US cybersecurity providers. While the proposed cybersecurity certification schemes are intended to be voluntary, they could in effect become mandatory, particularly in instances where a member state authority (national, regional, or municipal) may require them for public procurement purposes. Moreover, while the European Commission correctly recognizes that the growth of the cybersecurity market in Europe is restricted by overlapping standards and a lack of uniformity, it does not emphasize that the schemes should identify and align with

an existing international standard and conform to international best practices. The value of an EU certificate to an organization that seeks to do business within and outside the EU would be undermined unless it hinges on equivalent, internationally accepted standards.

Recommendation: Continuing concerns regarding a growing number of measures that create market access barriers lead BSA to highlight the European Union as a **Region of Concern**.