SPECIAL 301 SUBMISSION

February 9, 2017

Docket No. USTR-2016-0026
Christine Peterson
Director for Intellectual Property and Innovation,
Office of the United States Trade Representative
600 17th Street, NW
Washington, DC 20508

Dear Ms. Peterson,

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 2017 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, CA Technologies, CNC/Mastercam, DataStax, IBM, Microsoft, 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 BSA study shows the software industry contributes more than $1 trillion to the US GDP, nearly 10 million jobs, and $52 billion in research and development (with significant impact in each of the 50 states), which expands America's economic potential across numerous sectors[2]. This economic progress, coupled with tens of billions of dollars 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 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 unlicensed use of their 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, or 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 Spain be noted in the report as a Country of Concern because of a number of ongoing enforcement issues. Finally, we 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 the market.

Priority Watch List:	**Argentina, Chile, China, India, Indonesia, Russia, Ukraine, and Vietnam**
Watch List:	**Brazil, Greece, Kazakhstan, Korea, Mexico, Nigeria Romania, Thailand, and Turkey**
Country of Concern:	**Spain**
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 **Azerbaijan and Belarus** in this introduction and request that they be noted in the 2017 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 governmental measures 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

[2] The Economic Impact of Software study available at http://softwareimpact.bsa.org/

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, Nigeria, Russia, and Vietnam**, have 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 the market.

Data 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 they 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 revert such practices. All available trade mechanisms, including Special 301, should be leveraged for this purpose.

Procurement Discrimination: 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 against public procurement for foreign software products and services include **Brazil, China, India, Indonesia, Nigeria, Russia, and Vietnam.**

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, India, Indonesia, Nigeria, Russia, and Vietnam**.

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 market place. Countries adopting nationalized standards for IT products include **China, India, Nigeria, and Vietnam**.

Intellectual Property

Patents: BSA members invest enormous resources to develop cutting-edge technologies and software-enabled solutions for business, governments, and consumers. It is therefore critical that countries provide effective patent protection to eligible computer-implemented inventions, in line with their international obligations. Unfortunately, a number of countries have established or are considering policies that make obtaining patent protection for such inventions impossible or difficult. For example, in early 2016, **India** issued guidelines on the patentability of software-enabled inventions that are out of step with international practice and Indian patent law, and will and prevent most software-enabled inventions from receiving patent protection in the country.

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 or proposing such policies include **Brazil, 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 $52 billion USD, 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 licensing 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 rights 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, examples of countries where enforcement against enterprises that use unlicensed software in the course of their commercial activities is inadequate include **Azerbaijan** and **Belarus**. In **Azerbaijan**, an enforcement moratorium of two years was enacted in 2015, which poses a major impediment to enforcement actions by law enforcement agencies. In **Belarus**, copyright infringement is not considered a violation of criminal law unless it occurs within a year after the imposition of an administrative penalty for the same offense, or is associated with the receipt of "large-scale" income. The number of administrative convictions reported in 2016 is insufficient to ensure infringement deterrence.

[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.

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. Despite commitments to the United States under the US-Korea Free Trade Agreement (KORUS FTA)[5], some government agencies in **South Korea** continue to under-license the software they use. **China** has made multiple commitments to the United State in bilateral fora, such as the Joint Commission on Commerce and Trade (JCCT) and the Strategic and Economic Dialogue (S&ED), 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 2017 Special 301 Report and the US Government's engagement with important trading partners in 2017. 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.**

[5] US-Korea Free Trade Agreement – Article 18.4(9), available at https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file273_12717.pdf.

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

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. There was very little political will to elevate the importance of the protection and enforcement of intellectual property (IP) during former President Kirchner's tenure, and law enforcement authorities did not consider IP infringements a priority.

Market Access

Previous currency controls that impacted the payment of dividends and royalties to foreign parties have been lifted by President Macri's Administration. However, despite economic and fiscal reforms that have been recently implemented, Argentina's inflation rates are still very high and the country's economy has not improved.

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. 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.

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 represents a commercial value of $554 million USD 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 Undersecretariat 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, these have not been effective at addressing the continued use of unlicensed software in government agencies.

[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: 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;
- 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 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 79 cases in 2016 and has approximately 40 cases currently pending in the courts of Buenos Aires, neighboring jurisdictions, and in 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 2016. 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 $296 million USD in unlicensed software.[1]

The Nueva Mayoría Government has not issued or changed any policy to specifically address unlicensed use of software. Inadequacies in the law remain unaddressed and remedies for unlicensed software use are inadequate.

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, and in-house and external IT service providers that often load unauthorized copies of software onto computers or networks.

Government and SOE 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. As a consequence, in Chile it is easy to obtain illicit activation keys and services that offer the circumvention of technological protection measures.

Compliance and Enforcement: BSA enjoys a good relationship with the Chilean intellectual property agency, INAPI (Instituto Nacional de Propiedad Industrial). In 2016, BSA conducted almost 65 civil compliance inspections of a variety of enterprises on behalf of its members.

---

[1] Data on the rates on unlicensed software use and commercial values are taken from the 2014 BSA Global Software Survey at http://globalstudy.bsa.org/2013/downloads/studies/2013GlobalSurvey_Study_en.pdf. This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2013 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

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 in a public electronic register, 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 information technology sectors and, and continuing high levels of unlicensed software use by enterprises, BSA recommends that China be maintained on the Priority Watch List.

Overview/Business Environment

The commercial environment in China for software and information technology (IT) is very challenging, especially with respect to policies and regulations that substantially hamper market access for BSA members. We have seen limited progress on judicial enforcement of intellectual property rights, but unlicensed software use remains very high: while rates of use of unlicensed software have declined slightly, 70 percent of the software used in China is unlicensed according to the latest information[1].

The Government of China has shown a growing interest in building more effective judicial enforcement mechanisms for the protection of intellectual property (IP). Steps taken by China include: implementation of court procedures supporting evidence preservation; guidance issued by the Supreme People's Court (SPC) on awarding higher damages for intellectual property infringements; and, the establishment of five new specialized intellectual property courts (IP Courts) in Beijing, Shanghai, Guangzhou, Suzhou, and Nanjing.

While the commercial environment is not unique to the software industry[2], it is particularly acute for BSA members and other foreign technology providers. For example, there continues to be unclear instructions from senior Chinese policymakers directing Chinese agencies, Chinese state-owned enterprises (SOEs), and domestic firms to generally prefer domestic software. Such measures are often rationalized as a combination of cost-savings measures and as efforts to promote the domestic software industry.

In 2016, the Government of China issued policies that effectively act as discriminatory preferences and other market access barriers, such as sweeping security-related legislation. At the end of 2016, China enacted a new Cybersecurity Law that could impose data localization, security and privacy requirements that significantly restrict market access for US software and IT companies. Sector-specific cybersecurity regulations for the banking and insurance sectors, which request or require firms in these sectors to replace existing systems with "secure and controllable" products and services have been proposed or are pending further revision. Like other industry associations, BSA is very concerned that these policies could effectively block BSA members and other US suppliers from an increasing number of important sectors in the Chinese economy. These policies are not keeping in with China's commitment in the US-China Joint Commission on Commerce and Trade (JCCT) 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 especially in cloud or other data-services in China. While there have been some openings in the electronic commerce field, China continues to regulate Internet services as Value-Added Telecommunications Services (VATS) and precludes granting licenses to wholly-owned or majority-owned foreign entities.

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

As noted above, there have been positive steps on IP enforcement. However, in other IP areas, the environment remains quite challenging. 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

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

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.

We continue to urge the Government of China to adopt effective, transparent and verifiable software asset management (SAM) procedures. Such procedures would include government agencies conducting audits of the software they have installed to ensure not only that all copies in use are properly licensed, but also that the organizations are using relevant software efficiently and cost-effectively, as well as to reduce cybersecurity threats associated with using unlicensed software.

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 on this submission to ensure fair and equitable market access for BSA members and other US and foreign companies. We recognize the incoming Administration is looking at bilateral vehicles such as the JCCT, and BSA members welcome the opportunity to consult on the best ways forward.

Market Access

BSA seeks a fair and level playing field for competition in the software and related technologies market. Ensuring the security of government systems and important economic sectors is an important priority for all countries. The challenge, however, is to ensure that security-related policies are directed toward achieving their goals and are not be 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 December 2015, China passed the Counter-Terrorism Law. BSA, like other associations, provided comments, including raising concerns that some provisions impose vague and/or burdensome requirements on companies that may not be the most efficient way to curb terrorism. For example, telecommunication business operators and Internet service providers are generally obliged to “provide technical support and assistance, such as technical access and decryption” to law enforcement agencies, and appear to be required to monitor content for extremist communication. It remains unclear whether these measures will require companies to use weaker forms of encryption in their products than are currently available, thereby making their products more vulnerable to cyber theft.

In November 2016, the National Peoples’ Congress passed the Cybersecurity Law that would create a firmer legal basis for the activities of the Cybersecurity Administration of China; impose a variety of obligations on “network providers”, impose 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, limit data flows, and establish a prescriptive personal data protection regime. BSA urges the Government of China to adopt rules implementing the Cybersecurity Law enhancing the cybersecurity capabilities of enterprises and other institutions in a manner consistent with international standards and approaches, that do not impose unnecessary administrative compliance burdens, and do not discriminate against BSA members.

In addition to legislative developments, there have been several security-related regulatory developments that raise significant market access concerns. Sectoral regulators, such as the China Banking Regulatory Commission and the China Insurance Regulatory Commission continue to develop “secure and controllable” policies that require regulated private firms and state-owned entities (SOEs) to procure only designated “secure and controllable” products, software, and services. “Secure and controllable” has been widely interpreted by affected entities as referring to “domestic” as opposed to foreign IT products, software and services.

In November 2016, the Ministry of Industry and Information Technology (MIIT) published a Draft Notice on Regulating Business Operation in Cloud Services Market (Draft Notice). BSA and other associations

submitted comments to the Government of China raising concerns[3] about the Draft Notice and its implications for the operation of foreign cloud business in the country. These concerns include important IP-related issues, requirements to utilize infrastructure and maintain data in China, among other issues.

Furthermore, BSA continues to urge reform of long-standing measures, 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 intellectual property rights (IPR) owned in China. This applies to procurements by the Government of China and increasingly to procurements by SOEs and private sector entities, restricting market access restriction 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.

VATS Licensing: China defines basic telecommunication services (BTS) and value-added telecommunication (VATS) as restricted industries for foreign investment. For VATS, the proportion of foreign investment may not exceed 50 percent, excluding e-commerce. For BTS, the proportion of foreign investment may not exceed 49 percent.

In December 2015, MIIT issued China's Telecom Services Catalogue, which entered into force on March 1, 2016. The revised Catalogue continues to treat cloud computing and other Internet-based services as VATS. The designation carries significant restrictions on foreign investments.

For example, companies wishing to provide web- or cloud-based content services 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 MIIT issues very few new IDC licenses to FITEs.

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 State Intellectual Property Office are in the process of developing rules regarding the abuse, or misuse, of intellectual property rights (IPR) under the Anti-Monopoly Law (AML). BSA members remain concerned that there may be divergent approaches to AML enforcement regarding IPR, enhancing business uncertainty and exposing rights holders to administrative abuse or 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 (FRAND) 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 IPR.

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 $8.7 billion USD 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: (a) audits, certification, and other credible processes to verify software license compliance; (b) SAM best practices; (c) sufficient budgets to properly procure licensed legal software; (d) performance indicators to hold

[3] Comments available at http://www.bsa.org/~/media/Files/Policy/Trade/CloudRegComments.pdf
[4] 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf

government and SOE officials accountable for ensuring measurable progress on software legalization; and (e) a prohibition on mandates or preferences for the procurement of domestic software brands as part of the legalization process.

Statutory and Regulatory Provisions: The third draft of amendments to the Copyright Act remains 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:

- 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, may be 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 Law and ongoing amendment of the Patent Law;
- 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 IPR-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 IPR-related provisions. 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's growing interest in building more effective judicial enforcement mechanisms for the protection of IP has been demonstrated by the establishment of three five specialized intellectual property courts (IP Courts) in Beijing, Shanghai, Guangzhou, Suzhou, and Nanjing. BSA and its members have had some success with the IP Courts, although we are observing capacity issues as the limited resources of the three new IP Courts are tested against the growing backlog of cases. BSA looks forward to continued improvements in the efficiency and quality of judicial decisions from the IP Courts.

There are significant hurdles to effectively addressing the use of unlicensed software in China. In civil cases, several critical improvements are needed. Most courts have relaxed excessively high burdens for granting evidence preservation orders but some still have not done so. Courts should also increase the amount of

damages awarded against enterprises found using unlicensed software. While some courts have increased damage 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 laid out 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, 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

Although there have been some recent positive developments on market access issues and intellectual property enforcement in India, BSA members still face challenges in providing products and services to the market, protecting software inventions, as well as persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends India remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for BSA members remains challenging in India. In addition, in some policy and regulatory matters, such as those related to cross-border data flows and requirements to localize data in-country, there are signs that the environment could deteriorate rather than improve. Government procurement policies remain outmoded and inefficient because of local content preferences and technology preferences, such as for Open Source Software (OSS).[1] Further, the recently published draft National Policy on Software Products[2] promotes the use of domestically developed software products in public sector procurements and strategic sectors like defense, telecom, power, and healthcare. Additionally, some recent changes to the tax regime, such as imposing additional taxes on content downloads and cloud hosting from foreign websites by Indian consumers, might create market barriers for foreign service providers in India.[3] Such policies do not offer a level playing field to US technology providers who are keen to bring cutting-edge technologies and services to India.

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 unlicensed software of over $2.6 billion USD.[4] 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.

In October 2015, an ordinance was enacted that brought into force the Commercial Courts, Commercial Division and Commercial Appellate Division of High Courts Bill, 2015. The ordinance also clarifies that commercial courts have jurisdiction over intellectual property rights (IPR) and related matters, and imposes limits on the time the Courts may take to decide cases. Both of these considerations are important because they may allow IPR-related cases, including those related to the use of unlicensed software, to be brought before a specialist court, and may also solve the very long case pendency problem in related civil litigation in India. This is particularly relevant since cases can drag on for many years and undermine the incentives to bring IPR-related cases in the first place or to settle them in a timely fashion. Implementation of this ordinance has already begun and BSA is hopeful that implementation of these reforms will have a positive and practical impact on enforcement of IPR in India.

Unfortunately, enforcement against enterprises using unlicensed software remains a challenge. Due to a recent Supreme Court judgement, [5] software companies experiencing license infringement are forced to file cases across the country in district and high courts, where the experience and knowledge to handle such cases varies, and we find uneven willingness to impose preliminary injunctions and important forms of preliminary relief.

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 information technology (IT) sector more generally.

[1] http://deity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf
[2] http://meity.gov.in/sites/upload_files/dit/files/National%20Policy%20on%20Software%20Products.pdf
[3] In November, India's Ministry of Finance issued service tax amendments aimed at taxing the delivery of online services by persons located in non-taxable territories to Indian entities and individuals. See http://www.cbec.gov.in/resources//htdocs-servicetax/st-notifications/st-notifications-2016/st48-2016.pdf
[4] 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.
[5] Indian Supreme Court Judgement in IPRS v Sanjay Dalia & Anr.,1st July 2015

Domestic preferences and technology mandates in public procurement, and existing or proposed rules regarding security and privacy that may limit cross-border data flows or require server localization, act as *de facto* barriers to further investment by leading technology firms in the Indian market.

Cross-Border Data Flows: Data and server localization requirements are imposed in a heterogeneous manner across regulatory structures and procurement contracts in India. For example, in 2015 the Department of Electronics and Information Technology, which is now the Ministry of Electronics and Information Technology, issued a request for proposal for provisional accreditation of cloud service providers (CSPs), which mandates that all data and services provided by the CSPs need to be located in India. There is strong evidence that such policies are harmful to India, as they reduce productivity and dampen domestic investment in the country.[6]

Similarly, the draft Machine-to-Machine (M2M) Roadmap, issued by the Department of Telecommunication (DOT) in January 2015, proposed to require all M2M gateways and servers be located in India only "in the interest of national security." BSA was grateful that the DOT listened to the views of BSA and other stakeholders,[7] and removed this unnecessary and counter-productive requirement in the final M2M Roadmap, issued May 12, 2015.[8] However, India is currently working on implementation of the roadmap and data localization mandates are once again being considered.

Another example is the 2012 National Data Sharing and Accessibility Policy, issued by the Ministry of Science & Technology, which imposes onerous data localization requirements for weather data. This localization requirement undermines the ability of global information and communications technology companies to offer cutting-edge smarter cities and disaster management solutions as part of Digital India initiative.

Encryption: India lacks a uniform and effective encryption policy. Most countries allow the use of strong encryption standards ranging from 128-bit to 256-bit to ensure the security of sensitive information exchanged via the Internet and other networks. In India, however, only 40-bit encryption can be used without additional regulatory approval, according to DOT's Guidelines for the Grant of License for Operating Internet Service (ISP Guidelines). Each regulatory agency has its own specific encryption standards, with great differences between each agency. In September 2015, India published a 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. BSA is currently engaging with relevant Indian authorities to encourage a globally aligned regime in India.

Cloud Computing: In June 2016, the Telecommunications Regulatory Authority of India (TRAI) released a draft Cloud Computing Consultation Paper. The consultation paper requested stakeholder input on a range of important questions regarding cloud computing, and BSA was grateful for the opportunity to review the questions and present responses on behalf of its members. Many of the questions' topics, such as interoperability, platform-to-platform migration, and others, are currently best addressed by CSP-to-customer arrangements (such as contracts) and would not benefit from broad government intervention. We would be particularly concerned if TRAI or other Indian government agencies determined that requirements to localize data or impose India-unique standards or approaches were necessary to address the questions raised in the consultation paper. Cloud computing remains in a relatively early stage of development, and for many of the issues raised in the consultation paper an overly regulated approach is likely to inhibit development, deployment, and growth of cloud computing services, which would be detrimental to India's economic development.

[6] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.
[7] http://ww2.bsa.org/country/News%20and%20Events/News%20Archives/hi/2015/hi-05192015-Machine-to-MachinePolicyIndia.aspx?sc_lang=hi-IN
[8] http://www.dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf

Intellectual Property

Patentability Guidelines for Computer-Related Inventions: The Office of the Controller General of Patents, Designs, and Trade Marks (CGPDT) issued Revised Guidelines for Examination of Computer Related Inventions Guidelines (CRI Guidelines) on August 21, 2015. The CRI Guidelines – the product of several years of deliberation, stakeholder engagement, and study – were an improvement over earlier versions and appeared to settle uncertainty over whether software-enabled inventions were eligible for patent protection in India. Unfortunately, in late 2015 the CRI Guidelines were suspended after the Government of India received concerns from groups representing civil society and other stakeholders. In February 2016, without any formal public consultations, the CGPDT issued significantly revised guidelines. The revised guidelines appear to require an application for a computer-related invention (CRI) to include novel hardware in order to be eligible for patent protection. This is out of step with international practice and Indian patent law, and will and prevent most software-enabled inventions from receiving patent protection in India. Patent protection is vital to the software industry and it is important that the CRI Guidelines provide clarity to patent examiners on how to properly apply the Patent Act to applications for CRIs. As the Government of India continues to consider further revisions to the examination guidelines, BSA urges the US Government to continue engaging the Government of India to ensure that the patent protection available for CRIs is consistent with global practices.

Compliance and Enforcement: The lack of statutory damages and inadequate damage awards in civil enforcement continues to be a challenge for BSA and our members when attempting to enforce our rights against enterprises using unlicensed software in India. The willingness of Indian courts to grant preliminary or interim injunctions varies, and the system suffers from significant procedural delays.

Criminal enforcement has also not proved a practical approach for enforcing against enterprise use of unlicensed software. This makes establishing an effective civil enforcement system all the more important.

Recommendation: Although there have been some recent positive developments on market access issues and intellectual property enforcement in India, BSA members still face challenges in providing products and services to the market, protecting software inventions, as well as persistently high rates of unlicensed software use by enterprises. For these reasons, BSA recommends India remain on the **Priority Watch List**.

INDONESIA

Due to a poor market access environment for the software and information technology sector, rampant levels of unlicensed software use, and continuing deficiencies in legal enforcement mechanisms, BSA recommends that Indonesia remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for the software and information technology (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.

Intellectual property (IP) enforcement remains extremely difficult. Because damage awards tend to be so low, civil litigation is quite costly to plaintiffs and does not effectively deter future infringements.

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 Indonesian Ministry of Communication and Information Technology (MCIT) issued Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems in December 2016. The regulation raises concerns regarding data 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 the enhancement of personal information protection.

In addition, in October 2015, the government initiated a draft bill on the Protection of Private Data (hereinafter "Draft Privacy Law"), which remains with the House of Representatives. Should it pass, the bill would represent Indonesia's first overarching law on data privacy. Thus far, however, the government 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 data protection in Indonesia, BSA encourages the Government of Indonesian to reconsider Regulation No. 20 of 2016 mentioned above according to comments and recommendations BSA submitted before the regulation was finalized, to seek public comments on the Draft Privacy Law, and to ensure that there is close alignment between the two aforementioned pieces of legislation. BSA also urges Indonesia 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.

Local Content and Local Manufacturing Requirements: In 2015, MCIT issued the Ministerial Decree on Local Content for LTE Technology, which imposes onerous local content requirements on a wide range of technology devices and products. The Ministerial Decree was signed jointly by MCIT and the Ministries of Trade and Industry in early July 2015. The rules require that all covered products must contain 30-40 percent (depending on the particular product) local content in order to be sold in Indonesia. The Ministry of Industry confirmed in July 2015 that local content includes both hardware and software.[1]

[1] The Ministry of Industry is still formulating the methodology for calculating the local content percentage. While the methodology will allow for software (e.g. apps) to count towards (and even comprise the entire) local content percentage, this will only be for software that is locally produced and run out of local data centers. It will not be possible, for example, to take into account the overall economic contributions that foreign software corporations make to the Indonesian economy (e.g. software donations or other investments).

The Ministry of Trade also imposes requirements for importers of certain IT products — including smartphones, laptops, and tablets — to establish local manufacturing facilities within three years of obtaining their import licenses. If strictly enforced, this will effectively prevent the import of foreign-made IT products into Indonesia.

The stated purpose of these policies is to encourage local manufacturing and industry development. However, by blocking foreign companies without local production or development facilities from the Indonesian market, these policies will effectively reduce the supply of innovative devices and products in Indonesia, and will also hinder local companies from learning and developing the necessary experience to compete globally. This will harm Indonesia's broader economic development objectives in the long run. We believe that Indonesia can better achieve its economic objectives through regulatory policies that incentivize the development of knowledge-based industries, such as software and application development, rather than adopting market access barriers such as local content and local manufacturing requirements.

Accreditation of Auditors and Certification of Security Requirements: The Government of Indonesia released a Draft Information Security System Regulation in July 2015. The draft regulation requires strategic and high-electronic system providers to undergo a risk assessment to obtain certification against the ISO/IEC 27001 standard. However, certification must be performed locally by an in-house Indonesian expert or by an expatriate. BSA urges the US Government to work with the Government of Indonesia to stress the importance of recognizing the validity of certifications obtained from internationally accredited testing organizations. Requiring duplicative in-country testing will ultimately drive up the cost of computer and information systems, creating market access barriers without advancing any corresponding security benefits.

Source Code Disclosure Requirement: The Government of Indonesia published a draft Regulation on Electronic Systems Software and Information Security System Management in July 2015. If implemented, the regulation would require electronic system providers responsible for managing or operating computer systems used in connection with public services to disclose software source code. BSA is deeply concerned about this requirement. Many global companies of leading-edge security technologies would need to withdraw from bidding opportunities that would require them to turn over their IP or make it available, such as source code and other design information.

OTT Regulation: In early 2016, the MCIT published draft regulations regarding the Provision of Application and/or Content Services Through the Internet, referred to as OTT Rules. These rules threaten to impose unreasonable requirements on virtually all Internet-enabled services and service providers, including local permanent establishment mandates, use of local payment gateways, and unclear data retention policies among others.

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 $1.1 billion USD in unlicensed software.[2]

Statutory and Regulatory Provisions: Indonesia enacted a new copyright law in 2014. The law clarifies that software is copyrightable and provides protection for "compilations of creations or data in a format that can be read by computer programs or other forms of media." 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.

[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.

Compliance and Enforcement: There was little improvement in enforcement in 2016. Criminal enforcement against software copyright infringements are rare and prosecutors rarely receive cases from police or the Intellectual Property Office's enforcement officers.

Civil judges in Indonesia often award only very low damages, and legal expenses are not recoverable so the plaintiff must bear the costs of bringing proceedings. Therefore, rights holders tend to initiate few civil copyright infringement cases.

The courts in Indonesia remain largely ineffective for civil and criminal enforcement against software copyright infringement and enterprise use of unlicensed software. To improve matters, it is critical for the Commercial Court to improve the quality and consistency of its civil rulings. The Commercial Court should, like the Supreme Court, publish its decisions and provide official copies to the parties as a matter of course to improve transparency and reduce irregularities. Second, Commercial Court judges should receive training to improve their understanding of how IP cases are conducted. The training should address such matters as calculating damages, issuing provisional orders, and implementing injunctions, and should be expanded to the Commercial Courts of Indonesia beyond Jakarta, especially in Medan, Semarang, Surabaya, and Makassar.

Recommendation: Due to a poor market access environment for the software and IT sectors, rampant levels of unlicensed software use, and continuing deficiencies in legal enforcement mechanisms, BSA recommends that Indonesia remain on the **Priority Watch List**.

RUSSIA

Due to recently enacted onerous market access restrictions, persistently high levels of unlicensed software use, a lack of political will to prioritize intellectual property enforcement, ongoing challenges in the administrative and judicial systems, and onerous market access barriers, BSA recommends that Russia remain on the Priority Watch List.

Overview/Business Environment

The commercial environment for BSA members is bleak. Onerous regulatory requirements and discriminatory procurement policies threaten the ability of foreign software, Internet, and other IT firms to provide products and services to the market. The US Government should engage in consultations with the Russian Government to urge Russia to meet their international trade commitments and refrain from imposing unjustified restraints on trade and investment.

Russia's intellectual property (IP) enforcement remains deficient. It is essential that the Government of Russia, as it did prior to accession to the World Trade Organization (WTO), again recognize the importance of tackling copyright infringements. Law enforcement authorities should pursue more criminal and administrative actions against enterprises using unlicensed software, strengthen administrative penalties (particularly against large-scale enterprises), and seek deterrent administrative and criminal penalties from the judicial authorities.

Market Access

Cross-Border Data Flows and Server Localization: Federal law No. 242-FZ, in force since September 2015, requires personal data processors to process personal data of Russian citizens in databases located in the territory of the Russian Federation. Any firm collecting or processing such data is obliged to inform Russian telecommunications and media regulator (i.e., Roscomnadzor) of the location of the database prior to the data collection. In case of non-compliance, the law empowers Roscomnadzor to block access to the unlawfully collected personal data and establishes a detailed procedure for blockage of the website or web page containing such personal data. The implementation of the law began in 2016 and at least one US company was impacted when its website was blocked in Russia in November. This is one of the most restrictive data localization laws in the world and, as such, it negatively impacts both foreign and domestic companies.

Federal Law No. 374-FZ, enacted in July 2016, requires telecom providers and companies that facilitate the dissemination of information through the internet, or facilitators (a term broadly defined that includes information systems and software providers), to provide Russian investigators and prosecutors access to user information and/or to any other information deemed necessary by such authorities. The law also requires companies to provide assistance decrypting information as needed, which not only raises privacy concerns but, in many instances, may not even be technically possible. In addition, the law requires telecommunications providers and facilitators to store communications metadata in Russia for three years or one year, respectively, for law enforcement access purposes. Furthermore, companies must store communications content in Russia for 6 months.

Procurement: Federal Law No. 188, dated June 29, 2015, and Regulation No. 1236, dated November 16, 2015, which entered into effect in January 2016, impose restrictions on the public procurement of foreign software. The Federal law establishes a register of Russian software and defines the criteria for software to be considered "Russian" (i.e., copyright in the software must belong to the Russian authorities, Russian citizens, or Russian legal entities that are not controlled by foreigners; software should be legal; and foreign stakeholders of a Russian software producer cannot receive more than 30 percent of the annual software licensing revenue of that Russian software producer). Federal and state authorities are required to procure Russian software subject to the exceptions established by the Russian legislation.

In addition, Resolution No. 925, adopted on September 19, 2016, grants a preference to Russian goods and services in government procurement. The resolution entered into force on January 1, 2017.

Copyright and Enforcement

Enterprise Licensing/Legalization: According to the latest BSA information, the use of unlicensed software in Russia increased to 64 percent in 2015 from 62 percent in 2013. This represents a commercial value of over $1.3 billion USD in unlicensed software.[1]

Government and SOE Licensing/Legalization: Government software legalization decreases risks to the security of IT systems and helps change public perception of the need to license software properly. To set the right example for the market for legitimate sale of software products and services, the Russian government should use legal software. The Government of Russia should also develop procedures for the acquisition of licensed software from Russian and foreign software vendors by government agencies and state-owned enterprises. The adoption of effective, transparent, and verifiable software asset management procedures (in 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.

Compliance and Enforcement: For the past several years, the number of enforcement actions by police has declined significantly. Recently, there was an acceleration of this trend and, in 2016, this was due in large part to a reduction in the number of police assigned to perform enforcement activities and in the number of adequately trained officers available to investigate IP crimes. Fundamentally, the decline in enforcement activity is attributable to a lack of political will to address IP crimes and, consequently, IP enforcement has been deprioritized. New and inexperienced police officers are now frequently in charge of IP cases and they are hesitant to work on such cases because IP crimes are viewed as a low priority by their supervisors. Reluctance on the part of law enforcement to pursue actions against large-scale infringers also further undermines enforcement efforts. Unsurprisingly, in 2016, BSA observed a decline in virtually every statistical category related to enforcement, including the number of criminal actions and investigations taken against targets suspected of using unlicensed software, the number of criminal cases brought to trial, and the number of administrative enforcement actions conducted.

Currently, administrative penalties imposed on enterprises using unlicensed software are far too low to serve as deterrents against further infringements. Because it is not uncommon for administrative fines to be less than the cost of obtaining a legitimate license, the law creates a perverse incentive for enterprises to use unlicensed software.

In the rare instance that an investigation results in the filing of a civil or criminal complaint, BSA continues to experience a number of obstacles in Russian courts. Russian judicial practices and procedures should be clarified to establish guidelines regarding: (a) the quantum of evidence necessary to establish a defendant's criminal intent; (b) the methodology for determining the value of infringing copies; (c) the evidence necessary to obtain provisional measures; (d) the implementation of provisional measures; and (e) the use of post-raid materials as evidence.

Additionally, Russian courts are increasingly challenging the validity of powers of attorney (POAs) issued by BSA members. When POAs are notarized in the United States, the notary attests only to the identity of the signatory. The notary does not attest to the signing powers/authority of the signatory. Russian courts are unfamiliar with notaries attesting to this one aspect only and are therefore requesting evidence that proves that the signatory of the POA was authorized to execute and bind the organization. To satisfy the Russian courts, documentation evidencing the signatories' authority, as well as evidence on the practice of notaries in the United States is required. This additional documentary requirement is proving unnecessarily burdensome for BSA members.

[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.

In a number of regions of Russia, courts do not inform right holders of court hearings on infringement-related administrative cases and pass decisions in the absence of rights holders' representatives. Such an approach leads to violations of procedural rights and the legitimate interests of software producers. BSA members do not always receive up-to-date and necessary information about administrative cases, which may cause their legal representatives to be absent from the proceedings.

Recommendation: Due to recently enacted onerous market access restrictions, persistently high levels of unlicensed software use, a lack of political will to prioritize intellectual property enforcement, ongoing challenges in the administrative and judicial systems, and onerous market access barriers, BSA recommends that Russia remain on the **Priority Watch List**.

UKRAINE

Due to the continued lack of software copyright protection, lack of implementation of state government plans, weak enforcement, and continued dramatically high levels of unlicensed software use in both the public sector and by enterprises, BSA recommends Ukraine remain on the Priority Watch List.

Overview/Business Environment

The economic situation in the country remains severe; the expected GDP growth for 2016 will be insignificant, and inflation is high, meaning the prospects for further positive development are very uncertain. Furthermore, the risk of the slump in the local currency exchange rate remains high as reforms announced by the government are stalled, resulting in difficulties in cooperation with the International Monetary Fund, which has in turn postponed the issuance of the next credit tranche.

The new Law on Public Procurement implemented in August 2016 has been successful in making public procurement more transparent; however, the way the law is structured still allows for situations where the government procures counterfeit software via public tenders because there are no procedures in place to ensure that when a reseller wins a tender it will sell a genuine product. As a result, the software industry, the state's budget, and users have been negatively affected. IT companies have also been negatively impacted by the difficult economic situation in Ukraine and borne losses due to lack of improvement of intellectual property rights (IPR) protection.

Copyright and Enforcement

According to BSA's most recent Global Software Survey, the estimated rate for unlicensed software use in Ukraine in 2015 was 82 percent, representing a commercial value of $ 129 million USD.[1]

Government Legalization: In 2016, the Government of Ukraine continued to fail to address the high level of unlicensed software use by government agencies and funds were not allocated for software legalization in the public sector.

In 2016, the Ministry of Economic Development and Trade (MEDT) avoided participation in any legalization discussions, so no procedures were adopted to ensure a comprehensive and permanent shift in policies leading to government use of licensed software. Rare previous discussions on this matter have cased completely and no government representative or agency has been given authority to take action in this regard.

Statutory and Regulatory Provisions:
The Ukraine Government's planned intellectual property rights (IPR) reforms announced in 2015 was not implemented completely, and no new legislation was adopted since that time. In August 2016, the Cabinet of Ministers of Ukraine passed a decree closing the State IP Services agency (SIPS). SIPS' functions were split between MEDT and a new trademark and patent office, which was created in June 2016, but is not yet operational. This instability practically paralyzed the work that was formally the responsibility of SIPS. In 2016, no noticeable IPR protection initiative was implemented and no practical support to right holders was provided either by SIPS or by any other agency. In 2016, SIPS published its official report analyzing of IPR court practices, in which it was sympathetic to the users of unlicensed software noting that they should not be criminally prosecuted. [2]

Draft law No. 4629 developed by MEDT with the input of some interested stakeholders (including the software industry), which would address online copyright infringement and implement a notice 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] http://sips.gov.ua/ua/sud-pr-rozgliadu

takedown system, was re-submitted to the Ukrainian Parliament in May 2016. Is still unclear when its first reading will take place.

Compliance and Enforcement: In 2016, the number of IPR enforcement actions conducted by the Ukrainian police was insignificant, making the 2016 scenario even worse than the poor 2015 one. BSA members reported only seven criminal raids against commercial end-user companies suspected of unlicensed software use, and 11 criminal raids conducted against resellers suspected of distributing unlicensed software. These figures are much lower than the 38 criminal raids initiated against end-user companies and the 27 raids against resellers in 2015.

Ongoing reforms affecting the police and removal of IPR protection from the top-priorities of the Ministry of Internal Affairs resulted in a lack of *ex-officio* cases related to copyright/trademark infringements, so right holders are not able to rely on law enforcement agencies' assistance to enforce the IPR laws in Ukraine.

In September 2016, after a roundtable on "combating piracy" was held, the main office of the National Police declared a special operation called "Pirates" involving regional divisions. This operation, however, only let to a few administrative proceedings and did not produce any noticeable enforcement results, as it focused on small targets and lasted only one month.

In 2016, the special Cybersecurity Police Department started its operations with hundreds of newly trained officers and specific IPR online enforcement responsibilities. In the last few months, this agency's efforts resulted in several successful actions, including shutting down popular torrent tracker servers that were located in Ukraine and, in cooperation with Europol and police from 30 other countries, it also stopped activities by the Avalanche bot network that was infecting more than 500,000 computers daily.

Notwithstanding such positive police results, the overall previous negative enforcement trends remained the same in 2016: police raids continued to focus only on small targets, and police refused to target any large wrongdoers; most criminal cases initiated against IPR infringers are not concluded and very few resulted in criminal judgments; several criminal complaints filed by BSA members have been pending for years with no prospect of being transferred to court; courts often refused to issue search/seizure warrants for police, which effectively stopped any further investigation. Civil claims filed by right holders within criminal proceedings (as is provided by the law), are often rejected by courts, forcing right holders to initiate separate, costly civil proceedings, which often are not concluded. It is unclear if the application of civil *ex parte* searches would be effective under current law. Therefore, right holders have no effective legal tools to secure evidence and pursue actions against infringers.

Recommendation: Due to the continued lack of software copyright protection, lack of implementation of state government plans, weak enforcement, and continued dramatically high level of use of unlicensed software in both the public sector and by enterprises, BSA recommends 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, as well as a number of increasingly troubling information technology (IT) regulatory measures, BSA recommends that Vietnam be placed on the Priority Watch List.

Overview/Business Environment

Over the last several years, Vietnam has enacted, implemented or proposed measures for regulating the information technology (IT) sector 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 and government procurement that 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 use remains very high, both in the private and public sectors.

Market Access

Vietnam has enacted, implemented, or proposed a number of draft laws or regulations that will likely impose restrictions on the cross-border transfer of data or require server localization in Vietnam. 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 enter the market; overly broad definitions of personal information; and overly broad provisions requiring "cooperation with the Government" regarding access to data and 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 went into effect.[1] The decree imposes onerous requirements on server localization and restrictions to cross-border data flows that will undermine the ability of BSA members to provide digital services in Vietnam. Specifically, Article 4.2.f of Circular No. 9, which implements certain provisions of Decree No. 72, requires general news website operators, social network service providers, search engines, and online applications to have at least one server system in Vietnam to allow for inspection, storage, and provision of information at the request of competent authorities.[2] In early 2015, the Government of Vietnam proposed to further elaborate these requirements in a Draft Circular. The Draft Circular also mandates 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.

BSA remains concerned about a number of elements in the Draft IT Services Decree, issued in 2014 by the Ministry of Information and Communication (MIC). This decree would seriously impact BSA members' ability to provide products and services to the market. Specifically, the draft decree appears to restrict international data transfers, impose unnecessary requirements to localize hardware (e.g., servers) in Vietnam, and require unwieldy certification requirements for IT service professionals, among other things.

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

[2] Ministry of Information and Communication's Circular No. 09/2014/TT-BTTTT: Detailing management, provision and use of information on websites and social networks (in force since October 3, 2014)

(…continued)

Procurement Discrimination: MIC issued a circular, dated February 20, 2014, establishing a preference to purchase Vietnam-made IT products and services by government agencies and other entities funded by the state budget.[3] "Vietnam-made IT products or services" are defined as products produced or services provided in Vietnam by entities, the dominating shareholders of which are Vietnamese. Government procuring entities must provide full justifications for not purchasing Vietnam-made IT products or services.

Another MIC-issued circular, which went into effect on January 20, 2015, specifies preferences for open-source software in government software purchases.[4] BSA wishes to reiterate its view that open-source solutions can and should be part of IT solutions, but purchasing decisions should be made based on the IT needs and the total life-cycle cost of competing solutions, rather than on *a priori* mandates that prefer certain licensing models or product lines over others.

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 $598 million USD.[5]

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, with 88 administrative actions against such actors in 2016.

Statutory and Regulatory Provisions: Copyright protection and enforcement in Vietnam is governed by the Intellectual Property Code (as last amended in 2009), the Criminal Code (as amended in 2009), and the Administrative Violations Decree, which took effect December 15, 2013.[6] 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 on the part of the 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.[7] 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, the National Assembly adopted the new Criminal Code, which has not entered into force yet. 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 (i.e., enterprises). 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 (~$150,000 USD) and its business operations may be suspended for up to two years.

Amendments to the Intellectual Property Code over the years have resulted in a number of improvements in the overall protection of copyright in Vietnam. BSA recommends introducing pre-established damages

[3] Ministry of Information and Communication's Circular No. 1/2014/TT-BTTTT
[4] Ministry of Information and Communication's Circular No. 20/2014/TT-BTTTT
[5] 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.
[6] 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).
[7] 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 TPMs, decryption of encrypted satellite signals, and other acts.

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. However, fines remain too low to constitute an effective deterrent against future infringements. 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. In 2016, 88 administrative enforcement actions were initiated. Unfortunately, fines issued remain very low, in the range of VND20-50 million (roughly $1,000 – $2,000 USD), which is less than 10 percent the maximum applicable fine.

While BSA received good support from government agencies in 2016 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 remains a problem in Vietnam. To BSA's knowledge, no criminal copyright infringement case has ever been brought to the courts in Vietnam due to the lack of criminal provisions for entities in the current Criminal Code.

Also, there have been relatively few civil court actions involving copyright infringement in Vietnam to date. Complicated procedures, delays, and a lack of predictability in the outcome contribute to this problem. Despite this, BSA brought two cases to civil court in 2015 and hopes that over time, civil remedies will be available to supplement administrative, and eventually, criminal enforcement.

Technical Assistance and Education: Between March 27-April 30, 2016, BSA and the Inter Ministerial Intellectual Property Rights Protection Task Force organized an Intellectual Property Day campaign, where both educational and enforcement campaigns were conducted.

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, as well as a number of increasingly troubling IT regulatory measures, BSA recommends that Vietnam be placed on the **Priority Watch List**.

Watch List

BRAZIL

Due to an increasingly 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 new 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. 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. Brazil's current challenging political and economic situation — including high inflation rates and budget cuts — may affect initiatives to promote IP, such as enforcement efforts.

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 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 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.

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. On August 9, 2016, the new Secretary of Information Technology for the Ministry of Planning announced that the Federal government will revoke Decree 8135. A new decree was expected to be published by the end of2016, but is still pending. BSA urges the new decree and implementing regulations allow Federal agencies to procure innovative IT products and services, including cloud computing, and avoid restrictive data localization policies.

Government Procurement Preferences: CERTICs (Certification of National Technology Software and Related Services) is the certification component of the TI Maior Industrial Plan, conferring public procurement preferences to software developed in Brazil. CERTICs has not been recently applied, but the policy has also not been rescinded. Annex I of Decree 8186/14 (January 17, 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 apps and programs. Currently, 28 companies hold the certifications for 30 software packages. Only one non-Brazilian company (Accenture) has certified an individual product.

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.

Open Source Preference: Proposed legislation (PL 2269/1999) would require the obligatory use of open-source software by government entities and state-owned enterprises. The legislation had been stalled for some time, but it was resubmitted at the beginning of the 2016 congressional session with a new favorable report and a sponsor interested in forwarding the issue. The bill has not progressed so far. BSA has consistently argued that procurement decisions should be based on choosing the best products and services available to meet the specific requirements without preferences or mandates based on particular technologies or licensing models, taking into account the entire life-cycle cost of a product or service and not just the upfront fees or royalties.

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 $1.7 billion USD 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.

Compliance and Enforcement: BSA concentrates most of its efforts on bringing civil judicial actions against enterprises that are using unlicensed or under-licensed software. BSA's enforcement campaign is based on an out-of-court cease-and-desist letter procedure aimed at legalizing the use of business software. BSA escalates to filing civil lawsuits against specific companies when it becomes clear that they will not agree to comply with software licenses. 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.

BSA's efforts in Brazil also include a comprehensive risk awareness communication campaign called "Pensando Bem" ("Think Again"). This campaign is conducted exclusively online and is a collaboration with

[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.

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 increasingly 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. Brazilian courts continue to require extremely high fees for forensic experts who conduct searches and seizures and analyze the results. Further, the requirement that companies headquartered abroad must pay bonds to guarantee eventual damages during the civil procedures has proven unreasonable at times. BSA has paid bonds as high as $25,000 USD.

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 a new leadership that 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 follows up on initial steps to expand its work beyond its traditional focus of counterfeiting and piracy of physical goods.

Recommendation: Due to an increasingly 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**.

GREECE

Due to persistent and growing high levels of unlicensed software use in public and private sectors, insufficient 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 improvements to the legal framework and proper implementation in order 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 $189 million USD in unlicensed software.[1] The effects of this trend are fewer job opportunities and decreased revenues for local software and information technology (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 which would include a provision entitled "Sanctions against Copyright Infringements over the Internet" has been under consideration for two years, but it is still awaiting Parliament approval. The proposed amendment would provide rights holders with an expedited process to obtain an order requiring the removal of infringing content or the disablement of access to the violating content. As currently written, the provision would not apply when end users download or stream infringing materials, or exchange infringing files through peer to peer networks.BSA urges the Government of Greece to continue working to pass legislation that properly balances the interests of copyright holders, users, and Internet service providers (ISPs).

Under current law, ISPs are not allowed to disclose the Internet Protocol (IP) addresses of their users who infringe copyrights. This prohibition hinders enforcement activities. An amendment to the current law has been proposed to allow the disclosure, based on a court order, of IP addresses or other personal data such as traffic and location data, when a copyright infringement amounts to a felony. The passage of this amendment would be a positive development.

BSA also advocates for amendments to the relevant laws related to the certification of tax compliance by third-party auditors. Specifically, BSA recommends that an assessment of whether firms obliged to undergo third party audits for tax compliance are also compliant with software licenses should be included in the auditors' reports or the tax compliance certification.

[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.

Compliance and Enforcement: In 2016, the Financial and Economic Crimes Unit (SDOE) did not conduct any raids, due to ongoing restructuring of the unit and lack of resources. This lack of activity was caused in part by the transfer of some SDOE staff to the General Secretariat of Public Revenue. This deprived SDOE, the only agency with a proven positive record on the pursuit of software infringement cases in Greece, from important resources. It is critical that the Special Intellectual Property Rights and Electronic Commerce Department receives the funding and resources it needs to carry out its mission. It is also paramount that the Department recruits additional trained personnel in order to conduct more frequent inspections, building upon the good work performed in the past.

BSA and other stakeholders have conducted several training programs targeting SDOE staff.

BSA has also conducted awareness campaigns addressed to end users as well as approximately 40 raids for unlicensed software.

Inspections that were suspended in the past two years due to SDOE's reorganization should be rescheduled as soon as possible. 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 and conduct inspections, when appropriate, 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.

As soon as SDOE restarts its activity, it should increasingly focus its efforts on large scale violators. Unfortunately, SDOE in the past 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 SDOE to refocus its efforts to pursue large enterprises using unlicensed software.

BSA commends Greece for recent 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.

Recommendation: Due to persistent and growing high levels of unlicensed software use in public and private sectors, insufficient 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 2016. 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 $89 million USD 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.

Concrete progress 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 or under-licensed 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 Climate, 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. It is unclear, however, if these proposals will be considered and what the exact wording of the envisaged legislative texts will be. Consequently, to date, concrete improvement to IPR protection has not been achieved.

Statutory and Regulatory Provisions: Copyright infringement is a persistent problem in Kazakhstan. Although Kazakhstan´s IPR legislation continues to evolve, its practical efficacy remains uncertain.

The Criminal Code provides police with *ex officio* authority to commence criminal copyright cases, but the 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, has limited impact because of unclear wording in the relevant provision. The text could be interpreted to only refer 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.

[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.

Moreover, 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 do not act based on a mere raid referral, and they reject any application to initiate criminal cases or pre-trial investigation if the referral is not accompanied by evidence of the alleged offences. This continues to happen even in certain cases when the evidence of the allegedly infringing act requires direct access to computers and/or business documents; this irrefutable evidence should be actually gathered by authorities as they can get access to such computers and documents. Under such circumstances, it is practically impossible to file evidence along with the raid referral. The right holders cannot provide evidence of the infringement, which must by gathered by enforcement authorities.

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

The Kazakh legal system is not fully compliant with the requirements of Article 50 of TRIPS; under Kazakh 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, with a copy of application to the defendant (i.e., the potential violator of the right holder's IP rights). Due to this submission, the effect of "unexpectedness," which is attributable to the *inaudita altera parte* principle of TRIPS, is eliminated, since the potential violator will know that the application is 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 IP rights, Kazakhstan should amend its laws to be fully compliant with the TRIPS Agreement, especially considering Kazakhstan's WTO membership. Kazakhstan should also clarify its criminal enforcement legal framework, both in terms of offence description and applicable procedure.

Compliance and Enforcement: The law enforcement agencies responsible for IPR enforcement in Kazakhstan (the Ministry of Interior, and the Agency of State Income under the Ministry of Finance) have achieved some results related to IPR protection in the country.

However, in practice, the actions undertaken by these agencies, as well as by the Ministry of Justice, have not impacted the high level of unlicensed software use in the country. These actions have not addressed the root of the problem, which continues to be the widespread use of unlicensed software both by government organizations and commercial enterprises. 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, again, to only six in 2016.

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

Government and SOE Licensing/Legalization: The Ministry of Justice has taken a leadership role in promoting the importance of licensed software use by government agencies in order to prevent serious cybersecurity risks. However, the use of unlicensed software by government agencies remains a concern. Weaknesses in the public procurement process have also resulted in a high volume of unlicensed copies of software being acquired by government agencies.

The newly updated law on government purchases became effective on January, 1 2016. As a result, BSA remains hopeful that the government will establish and implement new provisions to regulate the acquisition and management of software by the government. The adoption of effective, transparent, and verifiable software asset management procedures, in which government agencies conduct regular internal software audits to ensure they use only licensed software, would also provide a powerful positive example to private enterprises.

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 information technology (IT) products, ongoing concerns related to government use of unlicensed software, and a decrease in software license enforcement activities, BSA recommends 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 last several years, however, the Korean Government 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 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 very concerned about the persistent under-licensing of software in a variety of government agencies, which is inconsistent with Korea's commitments to the United States under the Korea-US Free Trade Agreement (KORUS FTA). Not only does this harm the legitimate commercial interests of BSA members, but it also raises potential security risks for the government agencies engaged in such activities. Additionally, there has been a substantial decline in the number of enforcement actions undertaken and there are signs that enforcement authorities are becoming increasingly reluctant to pursue cases against enterprises suspected of using unlicensed software. This reluctance to initiate investigations threatens the progress made in reducing unlicensed software use in Korea. Furthermore, due to procedural impediments such as the lack of an effective discovery system, low damage awards, and a reluctance to issue preliminary injunctions, civil courts are not very effective in addressing software copyright infringement cases.

Market Access

The adoption of procurement preferences for domestic firms and measures imposing additional regulatory burdens, often justified by security concerns, have decreased market access for BSA members in Korea. Additional proposed measures could further impose restrictions on BSA members interested in providing Internet-based services, such as cloud-computing and data analytics services, in Korea.

Cross-Border Data Flows and Server Localization: Although the Cloud Computing Promotion Act came into force on September 28, 2015, the National Intelligence Service (NIS) maintains that many public sector entities should not use commercial cloud services without following specific NIS guidelines, including guidelines requiring internal systems to be physically or virtually separated from public-facing systems.[1] Similar guidelines and regulations requiring network separation and/or data on-shoring exist in the context of the finance [2] and healthcare [3] sectors. We remain concerned that, even after enactment of the Cloud Computing Promotion Act, significant barriers to cloud service adoption continue to exist.

Discriminatory Security Certification Requirements Applied for Foreign IT products: Since 2011, the Korean Government has imposed additional security verification requirements for international Common Criteria-certified information security products that are procured by Korean government agencies. However, no such requirement is applied to locally certified products. In 2014, the Korean Government extended similar security-conformity testing requirements to international Common Criteria-certified networking

[1] The Network Construction (Separation) Guidelines.
[2] E.g., under the Financial Services Commission's 2013 Regulation on the Supervision of Electronic Financial Activities (Supervisory Regulation).
[3] E.g. under the Medical Services Act.

products for all central government agencies. The government 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 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 KORUS FTA.

While the Korean Government 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 Korean Government, the issue remains unresolved at this time.

Procurement Preferences: The current Administration has adopted a number of policies to promote small- and medium-sized enterprises. We urge the Korean Government to avoid procurement preferences, whether based on licensing models or on the nature of the supplier. Such policies not only unfairly impact BSA members, but 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 $657 million USD in unlicensed software.[4] 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.

Government and SOE Licensing/Legalization: Government use of illegal software remains a serious problem. Frequently government agencies purchase fewer licenses than they require and use because of budgetary concerns, even though the cost of software for government may be much lower than the rates offered to private enterprises. Unfortunately, the government has resisted taking or will not sustain the necessary and effective steps to solve this problem. Effective efforts by some agencies are not replicated by other ministries and agencies where unlicensed software continues to be an issue. BSA requests that USTR open a dialogue with relevant representatives of the Korean Government to identify a mechanism to address this challenge and to ensure Korea's full compliance with its commitments under the KORUS FTA.

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

[4] 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.

unlicensed software. This force, however, has limited resources and BSA members also rely on the enforcement actions of the police.

Unfortunately, BSA has observed an alarming trend, in which the number of criminal enforcement actions undertaken by the law enforcement authorities has dropped precipitously over the last several years. Prosecutors and courts are applying overly stringent requirements for initial proof of illegal use to issue warrants. This trend is in stark contrast to the Korean Government's stated objectives of reducing the rate of unlicensed software use to less than 30 percent by 2020. BSA recommends that Korean law enforcement authorities commit to a minimum number of criminal enforcement actions not less than the average number taken between the years 2010-2012.

As criminal enforcement has become increasingly difficult, BSA members have turned to civil litigation. BSA members have found that the civil courts are not very effective in addressing software copyright infringement cases. For example, although preliminary injunctions are available, they are not often issued. It is also difficult to acquire evidence and damages awarded tend to be too low to compensate the rights holders or to deter future infringements. In 2017, Korea should amend the Civil Procedure Act, as the Supreme Court of Korea has suggested, to include effective discovery rules allowing rights holders to effectively seek civil remedies against software copyright infringement.

Recommendation: Due to challenging market access environment for software and IT products, ongoing concerns related to government use of unlicensed software, and a decrease in software license enforcement activities, BSA recommends Korea be placed on the **Watch List**.

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. The most recent information indicates that the rate of unlicensed software in Mexico is 52 percent, representing an estimated commercial value of unlicensed software of $980 million USD.[1] Illegal software is still commonly available at street markets ("carpeteros"), from online auction sites, and by download through specialized file-sharing sites. Although currently 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 (SAT) and the Mexican Institute of Industrial Property (IMPI).

Compliance and Enforcement: 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. Legal criteria are clearer and enforcement practices are more effective. Outreach campaigns launched in 2015 by 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. IMPI precautionary measures have become increasingly effective and constitute a deterrent.

Beyond IMPI raids, significant hurdles and challenges stand in the way of creating a truly effective enforcement system. Copyright certificates are still required in administrative and criminal cases. A final ruling on a typical IP infringement case brought to court after an administrative proceeding is concluded is likely to take at least 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. The recent creation of a cybercrime division within the Attorney General's Office (PGR) to focus on improving digital enforcement was a positive development in this area. This new division, staffed with five

[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.

public prosecutors, has demonstrated a high level of engagement and professionalism. However, further resources, including proper physical facilities and IT equipment, need to be dedicated to the division to allow it to properly perform its duties. Staff could also benefit from further training.

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.

Finally, 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. These requirements have a historic root, but they need to be changed drastically to adjust PGR's 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 2016, BSA conducted training programs for a wide range of individuals, from IMPI officers, PGR officers, Customs inspectors, inspectors from the Federal Consumer Protection Commission (PROFECO), judges, and magistrates, to certified public accountants, chambers and associations, police officers, entrepreneurs, students, customs agents, importers, and exporters. The program topics included IP rights, software protection, innovation, cybersecurity, ISP liability, software related tax matters, Verafirm certification, customs enforcement, licensing, administrative practices, notorious markets, rule of law, and accounting practices.
PGR has consistently held meetings with public, private, and academic sector stakeholders under the auspicies of the Interinstitutional Committee for the Protection of Copyrights and IPRs, with the participation of SAT, Customs agencies, IMPI, the Federal Police, the Cyber Police, PROFECO, the Federal Copyright Institute (INDAUTOR), and other agencies involved in the protection of IPRs, as well as chambers, associations, and other representatives of the private sector. The meetings were held to discuss the prosecution of IP crimes and infringements, the simplification of enforcement proceedings, the streamlining of expert witness procedures, the adoption of the new adversarial criminal model, the prosecution of cyber crimes, possible notice and takedown mechanisms, and the collaboration among agencies to achieve efficiencies.

Relationships with IMPI, INDAUTOR, and PGR 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 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 information technology (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, which announced that the government would begin enforcing implementation immediately for all multinational IT companies. 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.

As noted above, the Buhari Administration has announced its intention to begin immediate implementation of the Guidelines, despite the concerns of US companies and the US Government. BSA member companies report that in November 2015, the Nigerian government demanded that US companies prepare and submit within 30 days a detailed "implementation plan." Starting in August 2016, the government sent letters to a number of BSA member companies requesting additional details about these "implementation plans" and information regarding how companies will meet the localization requirements detailed in the ICT 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 $232 million USD 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 two 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 $161 million USD.[1]

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

The new 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 (ORDA), which has only 10 inspectors. This change in procedure significantly impedes enforcement efforts, as the number of organized crime officers available for inspections is considerably lower. The manner in which forensics analysis is presented frequently lack 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 regarding the authorities that are allowed to conduct the inspections referred to above 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.

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

[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.

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 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 2016, 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.

Compliance and Enforcement: In 2016, Romanian law enforcement conducted 57 inspections of enterprise end-users and 14 distribution channel raids in which unlicensed BSA member software were found. There were nine convictions reported by BSA members in 2016. Moreover, out of the 71 raids in 2016, more than half were conducted at low-profile targets (i.e. those with only one PC).
This status continues and illustrates a trend triggered by the aforementioned two legislative changes (i.e. competence of conducting computer searches; competence to prosecute and judge copyright criminal cases), as a major step backwards compared to the situation 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 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 offence in the Romanian legal system.

Technical Assistance and Education: In December 2016, BSA delivered in an extensive technical training for 9 experts of the Romanian Copyright Office that can still conduct searches, according to the new Criminal Procedural Code. Despite investments in training programs by both the private sector and the US Embassy, such trainings have not yielded results yet. There is a high rate of prosecutor turnover and they fail to support search warrants requests in IP infringement cases; on the rare occasion a search is executed, the evidence collected from computer searches continues to be substandard and often useless.

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 two years - and persistently high levels of unlicensed software use by enterprises lead BSA to recommend Romania be placed on the **Watch List**.

THAILAND

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

Overview/Business Environment

Thailand's software market did not significantly improve in 2016 mainly due to the persistence of high rates of unlicensed software use by enterprises. This is exacerbated by the widespread use of unlicensed software in the public sector.

In 2015, Thailand's Securities and Exchange Commission (SEC), an independent public-sector regulatory agency, set a good example by adopting software asset management (SAM) practices based on the International Standards Organization's (ISO) SAM standards. Other government agencies and most private sector companies have not followed this important lead and do not have adequate internal controls or management systems to reduce the use of unlicensed software and enhance cybersecurity. Only two private sector companies have adopted ISO-based SAM practices in 2016. Unfortunately, the Royal Thai Government (RTG) lacks clear goals and strategies to reduce unlicensed software use by enterprises and has generally failed to set a good example to Thai businesses.

BSA is also concerned that fair and equitable market access for our members' products and services could be harmed if legislation regarding personal data protection and cybersecurity remains both vague and potentially over-prescriptive. BSA appreciates the opportunities to discuss and address concerns in these bills, particularly the Ministry of Digital Economy and Society [1] (MDES) and the Electronic Transactions Development Agency's (ETDA) willingness to discuss the draft Personal Data Protection (PDP) Bill. BSA urges the RTG to continue to conduct and enhance an open and transparent process when developing legislation, 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 .

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 information technology (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 broad powers to access confidential and sensitive information without sufficient protections to appeal or limit such access. Granting the Office of the National Cybersecurity Committee 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.

Privacy: The PDP Bill is under review by the MDES. The PDP Bill is designed to build public trust and confidence in IT products and services and to implement the APEC Privacy Framework's principles for cross-border data transfer. BSA filed comments on the draft legislation in March 2015, and subsequently held a number of meetings with the RTG to discuss the bill. In these meetings, BSA highlighted the importance of protecting personal information for fostering the trust and confidence necessary for growth of the digital economy. However, the PDP Bill still contains imprecise or unclear provisions in some cases,

[1] MDES is the new name of the Ministry of Information and Communication Technology (MICT).

and in others appears to take an overly prescriptive approach that does not adequately take into consideration the nature of the personal information in question. Such an approach is not consistent with the expected technical and commercial evolution of digital products and services and could result in undermining both the effective protection of personal information and the trust and confidence that are necessary for widespread adoption of digital products and services in the economy.

Copyright and Enforcement

BSA enjoyed good cooperation with the RTG authorities in 2016, 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 $738 million USD.[2] The rate of unlicensed software use in Thailand is well above the Asia regional average of 62 percent, demonstrating that much greater efforts must be made. Beyond enterprise use of unlicensed software, 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 may expose the RTG to unnecessary cybersecurity risks.[3] BSA urges the RTG to upgrade their networks and eliminate the use of unlicensed software to help 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 occasionally damages awarded in civil litigation are 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 costs. Preliminary injunctions are not sufficiently granted to be an effective tool. In addition, criminal cases can be effective in Thailand, but the courts should apply more deterrent penalties for convictions.

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 the adequate protection for IP rights. The agencies BSA engaged with in 2016 include the Department of Intellectual Property (DIP), the ECD, the Central Intellectual Property and International Trade Court, Thailand's SEC, the Ministry of Digital Economy and Society, and the Electronic Transactions and Development Agency. BSA filed a submission recommending SEC require listed companies to have sound SAM practices or policies to strengthen their IT governance.

Technical Assistance and Education: In 2016, BSA, DIP, and ECD jointly launched the national campaign "Safe Software, Safe Nation" to promote the use of licensed software and to explain the cybersecurity risks posed by unlicensed software. BSA continued to promote SAM practices based on the ISO standard and its efforts targeted over 2,000 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 unlicensed software in Thailand, and would bring about many benefits to the enterprises themselves, as well as 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 privacy and security-related legislation now pending that may undermine the operations of BSA members, BSA recommends Thailand be placed on the **Watch List**.

[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] The "*Unlicensed Software and Cybersecurity Threats*" report available at http://bsa.org/malware demonstrates the link between unlicensed software and malware on personal computers (PCs).

TURKEY

Based on Turkey's failure to fully implement policies to ensure that government agencies use only licensed software, and persistent high levels of unlicensed software use by enterprises, BSA recommends that Turkey remain on the Watch List.

Overview/Business Environment

With an economy that fared remarkably well over the past decade despite recessions in Europe and other parts of the world, Turkey is an important emerging market for the software industry. Despite the overall health of the economy, the software market continues to underperform due to unacceptably high levels of unlicensed software use by enterprises and public entities.

Copyright and Enforcement

The key concern in Turkey remains the widespread use of unlicensed software by enterprises. The most recent data indicates that the unlicensed software rate in Turkey is 58 percent, representing a commercial value of unlicensed software of $291 million USD.[1]

Government and SOE Licensing/Legalization: In 2008, the Turkish Government issued a circular that ostensibly requires all government agencies to ensure the use of properly licensed software.[2] Nearly eight years later, the Government of Turkey has yet to fully implement the circular. As a consequence, unlicensed use of software within the government and in state-owned enterprises (SOEs) remains rampant. In 2017, Turkey should allocate the budget and resources necessary to ensure that each ministry and public authority issue and adhere to similar circulars to establish reasonable software legalization procedures. The adoption of effective, transparent, and verifiable software asset management procedures (where government agencies and SOEs 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. The government should also conduct public awareness campaigns to highlight the risks associated with using unlicensed software, such as the potential exposure to security vulnerabilities, and the collateral damage to domestic innovation and the growth of the software and information technology (IT) industry.

Statutory and Regulatory Provisions: Turkey has been developing draft amendments to the Law on Intellectual and Artistic Work for the past several years. In 2015, the Government of Turkey announced plans to amend its Patent Law. BSA encourages Turkey to develop these amendments in an open and transparent consultation, in which all interested stakeholders are afforded meaningful opportunities to participate and provide input.

Compliance and Enforcement: Turkey's criminal justice system provides an effective forum for intellectual property (IP) enforcement. Law enforcement authorities maintain units specialized for IP enforcement that have served as capable partners in the fight against the distribution and use of unlicensed software. Prosecutors are willing to take on IP infringement cases. The system, however, could be further improved by encouraging judges to issue deterrent sentences and damage awards in criminal and civil cases, respectively. Although courts generally provide adequate, equitable relief (e.g., orders requiring the seizure or destruction of infringing goods), they have been reluctant to issue adequately deterrent awards and penalties to defendants in both civil and criminal cases.

Recommendation: Based on Turkey's failure to fully implement policies to ensure that government agencies use only licensed software, and persistent high levels of unlicensed software use by enterprises, BSA recommends that Turkey remain 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.

[2] *Circular on Legalization of Software Use in Public Entities*, No. 2008/17 (July 2008).

Country of Concern

SPAIN

Despite positive developments, continuing concerns regarding the unlicensed use of software by enterprises in the country lead BSA to highlight Spain as a Country of Concern.

Overview/Business Environment

The unlicensed or under-licensed use of software by enterprises and the availability of unlicensed software on the Internet continue to be the main challenges for the software industry in Spain. This is substantially the same as the previous year, although legislative changes may help to improve the business environment.

Copyright and Enforcement

Enterprises of all types, both private and state-owned, and especially small- to medium-sized enterprises (SMEs) continue to use unlicensed or under-licensed software at rates significantly higher than those observed in similar markets in Europe. According to the most recent data, the use of unlicensed software in Spain decreased slightly from 45 percent in 2013 to 44 percent in 2015. This percentage is still high and represents a commercial value of $ 913 million USD.[1]

Enterprise Licensing/Legalization: Enterprises have been slow to adopt internal controls on software in use by their organizations, contributing to high rates of unlicensed use. This lack of internal control may decrease due to the enactment of a new Criminal Code that came into force in July 2015. The new Criminal Code makes intellectual property (IP) crimes, including copying software without authorization and accessing unlicensed software, one of the offenses that triggers corporate criminal responsibility. This will make both companies and their managers criminally liable for the unlicensed copying of business software within enterprises' information technology systems. However, the publication of Instruction 8/2015 by the General Prosecutor of Spain in late 2015 could prevent the changes introduced by the new Criminal Code from being as effective as they could have been (please refer to next section for further details).

In 2016, the Government of Spain announced that a special branch within the General Prosecutor's office exclusively dedicated to the enforcement of IP rights, *Fiscalía Antipiratería*, would be created in 2017. Should it come to fruition, this positive development would help improve the enforcement of IP rights in Spain.

Statutory and Regulatory Provisions: In 2014, Spain enacted a set of reforms to the Intellectual Property Law and the Civil Procedure Law, which went into force in early 2015. Amendments to the Criminal Code went into effect on July 1, 2015, but the effectiveness of some of these amendments may be jeopardized by recent policy developments.

Revisions to the Intellectual Property Law (Law 21/2014) were adopted and published on November 5, 2014 and went into effect on January 1, 2015. Article 138 of the new law establishes indirect liability for copyright infringement for: (a) those who willingly induce others to infringe; (b) those who cooperate with the infringement, either having knowledge of the infringement or having reasonable means to know about the infringement; and (c) those with the ability to control the activity of the infringer and with direct economic interest in the results of such infringement. The indirect liability applied to these categories remains subject to the limitations on liability set forth in the Law on Information Society Services and Electronic Commerce (LSSI). Law 21/2014 also increases the powers of the Intellectual Property Commission of the Ministry of Culture to carry out actions against online infringers.

Finally, changes have been introduced to Article 256 of the Civil Procedural Law regarding civil procedures available to enforce IP rights. The changes enable copyright holders to obtain court orders to access the

[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.

identity of infringers. This information can be used as preliminary evidence prior to the formal initiation of a civil suit. Some software vendors have successfully tested this new procedure.

Amendments to the Criminal Code, which went into force on July 1, 2015, allow Spanish law enforcement authorities to pursue criminal actions against enterprises that are willfully using unlicensed software. These amendments override former instructions to prosecutors issued by the Attorney General's Office decriminalizing infringing distributions of content by peer-to-peer networks and denying that unlicensed use of software by enterprises meets the standard for criminal prosecution. The former instructions resulted in a cessation of criminal enforcement actions against illegal file sharing and eliminated the possibility of prosecuting infringing enterprises.

Unfortunately, a subsequent instruction issued by the Attorney General's Office (Instrucción 8/2015 de la Fiscalía General del Estado) in late 2015 could jeopardize the complete effectiveness of the changes implemented by the new Criminal Code. The instruction establishes that the lack of a license remains insufficient to characterize unlicensed software use as a criminal offence. This would make proving the criminal offense more difficult. Representatives of the General Prosecutor's office have informally indicated that Instruction 8/2015 would not apply to enterprise software infringement cases. However, it is still uncertain if this will be the case. It is worth noting, however, that the General Prosecutor's office has demonstrated willingness to work with the software industry in the future to enforce IP rights even before criminal lawsuits are filed.

Other shortcomings in Spain's legal framework remain. Further changes are required to allow criminal and civil actions to proceed against the manufacture and sale of devices and services that are primarily designed or marketed to facilitate the circumvention of technological protection measures (TPMs) used to prevent unauthorized access to or reproduction of software in violation of the law. Spanish courts have erroneously concluded that devices primarily designed for purposes of circumvention of TPMs are lawful when capable of some ancillary non-infringing use. While these courts arguably are improperly interpreting the law, legislative amendments could clarify the intent of the law and ensure that the provisions function as intended to effectively enable the prosecution of manufacturers and distributors of circumvention devices.

An amendment to the Criminal Code (Article 270.6 of the new Criminal Code), that includes a definition of TPM circumvention measures is a step in the right direction. The new Criminal Code considers the "manufacturing, importing into Spain, making available or possessing with commercial purposes any device conceived, produced, adapted or created to suppress or neutralize any technical device designed to protect software or any other copyrighted work" a criminal offense. This could help the courts issue more favorable interpretations, but the fact that the expression "with commercial purposes" has been included may still cause some misinterpretation by the courts.

In addition, BSA recommends further legislative amendments to the Civil Procedure Law to avoid bonds for *ex parte* inspections, to permit anonymous evidence to initiate *ex parte* inspections, and to clarify that compensation of damages must be valued at least at the full retail value of the infringed goods. Commercial Courts generally perform well, but the effectiveness of civil actions is occasionally impeded by the imposition of burdensome bonds, difficulties in obtaining the detailed evidence required to conduct *ex parte* inspections, court-imposed measures that frustrate inspections in progress, and extremely low damage awards in some cases.

Technical Assistance and Education: In March 2015, BSA and the Ministry of Industry signed a cooperation agreement through which the Spanish Government fully commits to promote awareness messages about the importance of legal software use, and the legal and technological risks created by unlawful software use. As result of this agreement, several awareness initiatives have been identified and some were implemented place in 2016. The first initiative under the scope of the agreement consisted of a letter sent jointly by the Ministry, BSA, and AMETIC (a local Spanish IT association) to nearly 19,000 companies and organizations throughout Spain, as well as a LinkedIn awareness campaign that reached 6.000 corporate accounts. Other initiatives resulting from the agreement included a seminar held in November 2016 in cooperation with CEOE (Confederación Española de Organizaciones Empresariales),

AMETIC, and INCIBE (the Spanish anti-cybercrime agency) to raise awareness about cyber risks created by the use of unlicensed software. Unfortunately, the lack of an elected national government in Spain for the majority of 2016 resulted in delays in some initiatives planned under the cooperation agreement. With the recent establishment of the new government, a dedicated ministry was created to address digital economy issues, which should be helpful in the implementation of initiatives to combat the use of unlicensed software in the future.

Recommendation: Despite positive developments, continuing concerns regarding the unlicensed use of software by enterprises in the country lead BSA to highlight Spain as a **Country of Concern**.

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 *de facto* market access barriers. While BSA members fully respect and share the EU's strong interest in protecting the privacy of EU citizens, many of these policies would block US firms from offering digital services in the EU even where they offer strong privacy protections. 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. For these reasons, 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.

Market Access

Several of the comments below relate to localization requirements, which act as barriers to data services and digital trade. Such barriers at the EU level are increasing and are of major concern to BSA members. BSA commends US government efforts on this subject globally, and strongly recommends continued focus on the specific issues listed below.

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 by US companies 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 transfer 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). 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.

Standard contractual clauses, a second major mechanism used to transfer data from Europe to the United States and other countries, is under judicial review in Ireland and the case is likely to be referred to the ECJ in 2017. The Irish Data Protection Commissioner contends that standard clauses also are not consistent 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. For example, a November 2016 French government report calls for data localization and justified its position in part with clear anti-American

economic motivation. According to the report[1]: "French and European hosting companies see data location as an opportunity to stand out from the existing, primarily US, service offering." And further, "Moreover, the USA has a substantial competitive advantage in this sector, that the enshrinement of the free data flow principle would automatically strengthen."

The US Government had sought to limit data localization measures in the now-suspended Transatlantic Trade and Investment Partnership (TTIP) and Trade in Services Agreement (TISA) negotiations. The EU refused to discuss the subject in either negotiation. In addition, the European Commission announced in late 2016 that it was abandoning plans to propose legislation restricting member states' abilities to enact data localization members.

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 would expand substantially, from telecommunications services to any electronic communications services provided with the use of a public communications network, including over-the-top services and the conveyance of machine-to-machine communications for use in the Internet of Things. It also would apply extraterritorially, where processing is conducted outside the EU in connection with services provided within the EU.

Among the onerous requirements that would be imposed on data-related businesses are: confidentiality requirements that would restrict commercial uses of metadata (such as traffic data) and content data without user consent; stricter, express consent requirements, including for the use of cookies for profiling and data analysis; creating a foreseeable conflict of law regarding the obligations to respond to data requests from EU governments. Violations of the proposed regulation's provisions would carry heavy administrative penalties at the level of the General Data Protection Regulation (see below).

General Data Protection Regulation (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 US 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. 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 turn-over.

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.

Under current EU law, 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 affirmatively allow only public interest research organizations engaged in scientific research to conduct TDM, thereby creating an implication that such activity, when performed by commercial entities, falls outside of the existing temporary copy exception. 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.

Digital Content Directive: The proposed Digital Content Directive would introduce potentially burdensome rules with respect to the supply of digital content to consumers, including software and cloud services. It might also impact business-to-business transactions. For example, the directive would impose an onerous

[1] "The Free Flow of Data in International Commercial Agreements". Executive Summary in English available at http://www.economie.gouv.fr/files/files/PDF/Executive_summary_digital_in_trade_agreements.pdf

and ill-defined requirement to return consumers' data (personal data and non-personal data) at the conclusion of a contract. Because the scope of this obligation is inadequately defined, it could require companies to return enormous volumes of proprietary data created by a company during the course of providing online services (e.g., quality assurance data, telemetric data, and cybersecurity data). Ongoing legislative consideration of the Digital Content Directive could also result in reclassification of software embedded in consumer devices as "goods," thereby exposing companies to increased liability for consequential damages.

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**.