

1150 18th Street, NW
Suite 700
Washington, DC 20036

p. 202/872.5500

f. 202/872.5501

March 24, 2010

BY EMAIL: intellectualproperty@omb.eop.gov

The Honorable Victoria Espinel
United States Intellectual Property Enforcement Coordinator
Office of Management and Budget
Executive Office of the President

Re: Request for Written Submissions
Concerning Joint Strategic Plan
75 FR 8137

Dear Ms. Espinel:

The Business Software Alliance (BSA)¹ appreciates this opportunity to provide comments concerning the Joint Strategic Plan required pursuant to the Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub L. No. 110-403 (Oct. 13, 2008). BSA is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce.

This submission is divided into two parts. Part I describes the role of the software industry in the US economy, the nature of software theft and estimates as to its scope. Part II provides specific recommendations for the Joint Strategic Plan.

¹ BSA (www.bsa.org) members include Adobe, Altium, Apple, Autodesk, AVEVA, AVG, Bentley Systems, CA, Cadence, Cisco Systems, CNC/Mastercam, Corel, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, Kaspersky Lab, McAfee, Microsoft, Minitab, Parametric Technology Corporation, Progress, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

Part I: The Software Industry in the US Economy and the Harm of Software Theft

A. The Role of the Software Industry in the US Economy

The software industry has long been a driver of jobs and economic growth. In 2007, 1.7 million people were directly employed in the US software and related services industry. These jobs paid 195 per cent of the US national average per capita income (\$85,600 vs. \$43,900). The industry contributed more than \$261 billion to US GDP (almost 2 percent) and generated a commensurate amount in sales, income, payroll and corporate taxes to federal, state and local governments.² These contributions have been growing much faster than the economy as a whole each year since 2003.³ The software industry also generated a \$36 billion surplus for the US balance of trade in 2008.⁴

In addition to BSA member companies, the software industry includes thousands of distributors, re-sellers, developers and others that build and rely on our success. Jobs in these enterprises, which often are small and medium-sized businesses, also are at risk because of software theft. The attached document provides additional details of the role of the software industry in the domestic and global economies.

B. The Nature and Scope of Software Theft

“Software theft” generally refers to the reproduction or distribution of copyrighted software without the consent of the copyright owner. Software theft is by far the largest form of copyright piracy in dollar terms. Theft of software can take a number of forms, including a significant volume of convincing counterfeits, but BSA focuses principally

² OECD STAN Database, available online at <http://stats.oecd.org/Index.aspx?DatasetCode=STAN08BIS&lang=en>. “Software and related services” are those businesses that fall under code 72 in the ISIC rev. 3 industry classification. US economic figures for 2008 and 2009 are not yet available from this source.

³ Id.

⁴ Nathan Associates, Worldwide Packaged Software Sales and the U.S. Trade Balance for All and Selected Industries, Including the U.S.-Owned Software Industry, 1997-2008 (unpublished research performed for BSA) (copy attached).

on two specific types: organizational end-user piracy and Internet piracy. Of these two, organizational end-user piracy is by far the most economically damaging.

Organizational end-user piracy

The business software industry's most harmful piracy problem involves its primary users – large and small corporate, government and other enterprises – that pirate our members' products by making additional copies of software for their own internal usage without authorization. We commonly refer to this activity as "organizational end-user piracy."⁵

Organizational end-user piracy occurs in many different ways. For example, a corporate entity may purchase one licensed copy of software, but install the program on more computers than the license permits, or may obtain multiple licenses, but in numbers insufficient to cover the entity's installations. Other forms of end-user piracy include copying disks for installation and distribution, in violation of license terms; taking advantage of upgrade offers without having a legal copy of the version to be upgraded; acquiring and using in a commercial setting academic or other restricted or non-retail software without a license for commercial use; and swapping disks in or outside the workplace. Another common form of end-user piracy is client-server overuse – when too many employees on a network have access to or are using a central copy of a program at the same time, whether over a local area network (LAN) or via the Internet. In all its various forms, organizational end-user piracy causes the vast majority of the economic harm that our industry experiences from software theft.

In many cases, organizational end-user piracy is attributable to negligence and poor asset management practices. Enterprises can also be victimized by unscrupulous computer manufacturers and dealers who install copies of software onto the internal hard drive of the personal computers they sell without authorization from the copyright holder. In some cases, however, organizational end-user piracy is undertaken

⁵ Organizational end-user piracy is also sometimes referred to as "enterprise end-user piracy" or "corporate end-user piracy."

willfully, with management fully aware and supportive of the conduct. In the latter case, the infringers are potentially subject to criminal penalties under US law and, in accordance with Article 61 of the WTO Agreement on Trade-Related Aspects of Intellectual Property (TRIPS), under the laws of most US trading partners.

Internet piracy

The Internet is an indispensable part of global communication and commerce. It has opened up opportunities for faster, more efficient and more cost-effective distribution of information, products and services across the globe. It has also opened up new forms of social interaction that render geography largely irrelevant. As technology innovators, BSA's members are at the forefront of these developments. Software and software functionality are not only sold and delivered over the Internet, but also comprise a key component of the Internet infrastructure.

Unfortunately, in addition to creating significant social and economic opportunities, the borderless and anonymous character of the Internet makes it an ideal forum to engage in a broad variety of unlawful conduct, including copyright piracy. The worldwide availability of the Internet also creates challenges in enforcing rights holders' intellectual property rights, allowing sellers in countries with lax protections for intellectual property, such as China, easily to reach consumers in the United States.

While the economic impact of Internet piracy on the software industry is far smaller than that of organizational end-user piracy, it is a serious and growing problem nonetheless. In the 2009, BSA sent over 7.3 million takedown notices worldwide to Internet service providers, related to Peer-to-Peer file sharing. We also requested the removal of almost 153,000 torrent files containing BSA member software from just nine of the largest BitTorrent index sites worldwide. These torrent files were

being used by nearly 4 million individuals to download software with a retail value in excess of \$2.2 billion.⁶

Impact of Software Theft

As of 2008, one in every five copies of software in use in *this* country, valued at more than \$9.1 billion, was stolen. Globally, 41 percent, or more than one out of every three copies of software in use – nearly \$53 billion worth – was stolen.⁷ The estimated loss to US vendors from piracy outside the US was \$23.7 billion.⁸ There are few industries that could endure theft of their products at this level.

Pirates steal jobs and tax revenues as well as intellectual property. A study conducted for BSA by IDC in 2008 found that lowering software piracy rates stimulates the entire IT sector, creating jobs and increasing economic growth and tax revenues. In the US, for example, the study

⁶ Torrent file data, as well as, the number of seeders, leechers, and other torrent-specific particulars, are obtained from each BitTorrent indexing site directly. The retail value of the software is computed by multiplying the number of leechers (downloaders) by the MSRP value of the products involved.

⁷ Fifth Annual BSA and IDC Global Piracy Study (2009), available online at <http://www.bsa.org/globalstudy> (hereinafter “2009 Piracy Study”). The study methodology is described on pages 12-15 of the study, and is available online as a separate document at http://global.bsa.org/idcglobalstudy2007/studies/methodology_globalstudy07.pdf. The Sixth Annual BSA and IDC Global Piracy Study (covering 2009) will be published later this spring.

⁸ IDC, 301 Filing Submission – US Software Vendor Trade Losses from Piracy (unpublished worksheet dated 2/10/2010) (hereinafter, “IDC 301 Data”). The “value of pirated software” reflected in BSA’s annual piracy study reflects losses to all vendors (US and non-US), as well as the channel (resellers and the like). For purposes of the annual IIPA Special 301 submission, each year IDC furnishes BSA with the US vendor portion of the losses for each market in our Global Piracy Study, based on preliminary data for the previous year. A subset of these data is included in the IIPA Special 301 submission and posted on the IIPA website. See, e.g., <http://www.iipa.com/rbc/2009/2009SPEC301LOSSLEVEL.pdf>. Later in the year, IDC updates these data based on the final full-year dataset that forms the basis of our annual piracy study. The IIPA website is updated to reflect the new data.

For a description of the methodology for equating the value of pirated software with losses, see 2009 Piracy Study, *supra* note 7, at 13-14. Preliminary figures for 2009 indicate that this loss increased to \$24 billion.

concluded that a 10-point reduction in software piracy over four years would deliver an additional 32,000 new jobs, \$6.7 billion in tax revenues, and \$41 billion in economic growth.⁹ Piracy reductions outside the US would yield similar economic benefits both in the countries themselves, and – since 60 cents of every dollar spent on software worldwide inures to the benefit of US-based software companies – in the US as well.¹⁰

Software theft hinders job growth throughout the economy – not just in the software or IT sector. Our industry's products play a critical role in making businesses throughout the entire economy more productive and efficient. Software theft has a broad distortive effect on competition among businesses. Specifically, a company that steals the software it uses to enhance its own productivity enjoys an unfair competitive advantage over an enterprise that pays for it. Both enterprises have roughly equal productivity benefits from the software. But only one of them is bearing the legitimate cost of those productivity gains. When this distortive effect is considered on a national and international scale, the effect on jobs is clear. Countries where most businesses steal the software that they use are competing unfairly with countries like the US, where the vast majority of businesses license their software.¹¹

In addition to the economic harms it causes, software theft exposes computer users to serious security risks. Globally, there is significant evidence to link software piracy with the frequency of malware attacks.¹² Altered binary files, and the addition of malware through hacks or the tools used to install illegal copies provide a channel for identity theft, botnet connection and the like. Websites that offer access to pirated software also frequently disseminate malware that infects visitors'

⁹ IDC, The Economic Benefits of Reducing PC Software Piracy (2008), available online at <http://www.bsa.org/idcstudy>.

¹⁰ IDC 301 Data, supra note 8.

¹¹ BSA is currently working with a team of economists to develop a methodology for quantifying this economic effect.

¹² See, e.g., Harrison Group, Impact of Unlicensed Software on Mid-Market Companies (September 2008), available online at <http://download.microsoft.com/download/D/C/5/DC503630-3EDD-455D-B155-4FCCA6FCCEA3/TCO%20Global%20Final%20Whitepaper.pdf>.

computers.¹³ All of these means of obtaining illicit software threaten consumer privacy and expose consumers to a range of economic harms. Moreover, those who use pirated, unlicensed software are typically unable to access or download essential patches and critical updates that ensure their systems remain as secure as possible. This makes them more susceptible to attack over the long term.

Part II: Recommendations

It is imperative that the US government establish a specific action plan to attack the problem of software theft. Software theft is qualitatively different from other forms of copyright infringement, and the harms caused by software theft – to the economy, to job creation, and to security and privacy – are greater and affect a much broader cross-section of the economy. Development of the Joint Strategic Plan provides a perfect opportunity for establishing such a plan, and BSA is pleased to offer the following specific elements to include.

A. Secure the Procurement Supply Chain

In virtually every country, the government is the single largest consumer of software. The US is no exception. Ensuring that governments in the US and around the world use only legal copies of software has been a goal of our industry and the US government for more than a decade.¹⁴ Under Executive Order 13103 of September 30, 1998, federal agencies in the US must take steps to ensure that they use only legal copies of software. US Free Trade Agreements with a number of countries included government legalization requirements.¹⁵ Getting governments to legalize their software use serves a dual purpose: first, it decreases piracy directly by ensuring that one of the biggest software users in the

¹³ Software Piracy on the Internet: A Threat to Your Security (2009) (BSA White Paper), available online at <http://global.bsa.org/internetreport2009/>.

¹⁴ See Okinawa Charter of 2000, reaffirmed by the G8 at Aquila in 2009, during which the IP Experts Group also produced the G8 Guidelines for Governments Use of Software in Compliance with Intellectual Property Rights.

¹⁵ See, e.g., US-Australia Free Trade Agreement Art. 17.4.9; US-Bahrain Free Trade Agreement Art. 14.4.9; CAFTA-DR Art. 15.5.9; US-Chile Free Trade Agreement Art 17.7.4.

market is legal; and second, it sets an important example for the private sector to emulate. It also contributes to the ability of governments to limit their exposure to malware and other threats to privacy and security. For this reason, governments should take steps to assess the risk of being supplied with counterfeits when procuring software, as they do with other procurements.¹⁶

In the US, the federal government can have a profound effect on reducing software theft, not only through its direct procurement of software, but also by leveraging its role as a procurer of other goods and services. The principle established by EO 13103 can be extended by executive order to require that federal contractors also use only legal copies of software. Firms that seek to sell goods and services to the US government should certify that their use of software is in compliance with the Copyright Act and relevant license agreements, and that they have controls in place to ensure that this is the case. By extending the executive order in this way, the Administration would establish a standard for other governments to follow.

B. Engage with Trading Partners

Cooperation with Trading Partners

Cooperation with our trading partners is essential. Ideally, foreign governments should be willing partners with the US government and with industry in combating IP theft. Many countries have domestic IP industries that suffer proportionally greater harm than international industry players from high piracy rates in their markets. Many others have aspirations to develop such industries to help their economies “move up the value chain.”

BSA has enjoyed enforcement success in a number of markets due to strong cooperation with local authorities. For example, under a 2002 commitment made to USTR by the government of South Korea, police

¹⁶ See Department of Commerce, Defense Industrial Base Assessment: Counterfeit Electronics (January 2010), available online at http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

and prosecutors conduct a high volume of criminal raids each month against corporate end user piracy based on right holder complaints. After the raids, most infringers agree to pay damages for past infringements and to legalize their software use going forward, thus turning former software pirates into legitimate customers. Korea's software piracy rate has fallen from 48% in 2003 to 43% in 2009. This is well below the region's median rate of 67%. In the Russian Federation, the Ministry of Education worked with domestic and international software companies in 2007-2008 to legalize software use in each of the approximately 65,000 public schools in Russia. This contributed to a decline in the software piracy rate from 80% to 68% in Russia between 2006 and 2008, and to growth in jobs and taxes related to the technology sector.¹⁷ In Colombia, the tax authority, DIAN, has recovered \$87 million in additional sales taxes in the year 2008-2009 by focusing on growing legal software use and has now set a target for reducing software piracy by 16%.

By comparison, piracy rates in China have remained high, and China's government has yet to fully comply with commitments made in the bilateral Joint Commission on Commerce and Trade. China is a market with real challenges – challenges that act as significant barriers to trade. Progress in reducing the PC software piracy rate in China has essentially stalled in the last three years following a 10 point reduction in the preceding three year period. Meanwhile, the PC market has grown to be the second biggest in the world and is on course to become the biggest in the next few years. With an industry average 80% PC software piracy rate, this translates into enormous losses to the software industry. Preliminary IDC data indicates that losses in 2009 increased \$900 million from 2008 to a total of \$7.6 billion.¹⁸ Individual BSA company losses and experiences suggest that this is a very conservative estimate.

The Chinese government has made a series of high-level commitments, including bilateral commitments through the US-China Joint Commission

¹⁷ IDC, Does Lowering PC Software Piracy Actually Create Benefits for Countries? (March 2009) (copy attached).

¹⁸ IDC 301 Data, supra note 8.

on Commerce and Trade (JCCT), on reducing software piracy, and on government and enterprise legalization, but these commitments are not tied to benchmarks and have not resulted in measurable and sustainable progress.

In addition, resources devoted to administrative enforcement are completely inadequate and the deterrent value of administrative enforcement is spotty at best at the local level. Criminal remedies are not available against enterprise end-user piracy.

Given the scope of enterprise end-user piracy in China, SOEs and other major businesses, it is highly unlikely the piracy rate will drop substantially until these large organizations believe there is a credible risk in continuing to use unlicensed software.¹⁹

Abuse of intellectual property rights takes other forms as well in China. In recent years, the Chinese government has adopted a series of industrial policies aimed at promoting the development of key sectors in the Chinese economy. These policies pose serious market access barriers for US suppliers and appear designed to compel the transfer of foreign IP to China. They represent another dimension of China's broader pattern of misuse of – and lack of respect for – foreign intellectual property.

The chief recent example of China's discriminatory industrial policies focused on intellectual property is China's National Indigenous Innovation Products (NIIP) program, which imposes highly discriminatory conditions on the use of foreign intellectual property in the Chinese market. Under this program, government procurement of software and other high-technology goods is restricted to accredited products. Products that contain foreign IP – or IP whose use and development are not "totally independent" of foreign entities, or trademarks that were not originally registered in China – are ineligible for accreditation. This policy effectively excludes foreign IP from the government procurement market for software. It also extends to projects funded with "fiscal funds," and thus arguably to SOEs that draw public financing.

¹⁹ BSA is working with its member companies to develop a number of additional initiatives relating to China and would like to make a supplemental submission in the near future.

While the NIIP program is the most recent example of China's discriminatory industrial policies on IPRs, there are many others. For instance, in late 2009, the Standardization Administration of China issued draft provisions on the treatment of patents in national standards that, if adopted, would likely have the effect of expropriating US technologies that were implemented in Chinese national standards by barring US companies from licensing such technologies in China on reasonable and non-discriminatory terms. Likewise, recent amendments to China's Patent Law have expanded the scope of compulsory licensing of patents in ways that are inconsistent in several respects with the WTO TRIPS Agreement.

With these facts in mind, we have some initial recommendations on international initiatives.

First, working with countries to establish requirements for the use of legal software by all governments and their contractors would have an immediate positive impact. As discussed above, government policies have a substantial effect in shaping local markets, and establishing requirements for legal use by contractors and governments would have a profound positive effect on deterring corporate and institutional end-user piracy.

Second, the US should encourage trading partners to adopt good software asset management (SAM) practices to ensure that commitments to legalize government (and, where appropriate, SOE) software use are properly implemented. SAM is a business process that enterprises can adopt to optimize the purchase, installation, utilization, maintenance, and replacement of software, including ensuring the use of legal software. BSA has worked with central and local governments in a number of countries on programs to implement SAM in their own operations and on joint-campaigns to promote the value of SAM to local businesses. The US government should encourage more of our trading partners to participate in similar public-private cooperation to implement SAM.

Third, the US should move ahead as expeditiously as possible to conclude a meaningful Anti-Counterfeiting Trade Agreement (ACTA). Gaining the commitment of key, like-minded trading partners to obligations

consistent with the strong substantive and enforcement provisions currently reflected in US law and practice is itself valuable. Moreover, the potential for ACTA to provide a mechanism for further cooperation among governments in enforcement efforts recognizes the global nature of many sophisticated piracy and counterfeiting operations.

Fourth, with respect to organized criminal counterfeiting of business software we urge continued and expanded cooperation between US and foreign law enforcement and customs authorities to intercept and shut down the illicit counterfeit software trade both domestically and overseas. This should include focus on importation of counterfeit software for resale on domestic Internet sites. As discussed below, it is imperative that the government invest sufficient criminal and Internet enforcement resources to make such cooperation possible and successful.

Special 301, Trade Agreements and Other Trade Tools

Not all of our trading partners are willing (at least initially) to be cooperative on issues relating to IPR enforcement. For these uncooperative trading partners, cooperation must be preceded by persuasion. The US government has at its disposal a number of trade tools to assist in this process.

Special 301: The Special 301 process is one of the oldest of these trade tools, but it still remains important. A great deal of its value derives from (a) the way that it brings together the relevant federal agencies on an annual basis to focus attention in a systematic way on issues of IPR protection and enforcement, and (b) the increased bilateral engagement with US trading partners that results. This engagement could be made more effective by developing concrete action plans for trading partners that are named to the Priority Watch List. Having specific benchmarks would assist all parties to understand the nature of US concerns and to assess progress in addressing them. USTR already employs action plans with trading partners as part of the Special 301 process. Our proposal is that the practice be formalized for all Priority Watch List countries.

The US government should also consider ways to update the Special 301 criteria. The fact that many countries have piracy rates in excess of 75

percent year after year is intolerable. Persistent excessive piracy rates should be a factor making determinations under the Special 301 laws.

Existing Trade Agreements: Apart from those provisions that are directly related to IPR protection, there are other provisions of trade agreements that could potentially be brought to bear against countries that tolerate high levels of IP theft. For example, as we discussed above, software theft distorts competition and confers an unfair advantage on companies that break the law. A government that tolerates theft of software by companies operating within its borders is effectively subsidizing the goods and services that those companies produce and export.

New Trade Disciplines: We urge the establishment of new international regimes to address the unfair trade practices that result from governments' tolerance of software theft. The trade distortions and job losses that arise from software theft should be subject to specific rules under international trade laws. Thus, the US government should undertake a comprehensive assessment of all available avenues under domestic and international law to address circumstances where excessively high rates of software theft create unfair competitive advantages for goods and services ultimately sold in the United States. In addition, the US government should examine whether countries are living up to the goals of the WTO or are engaging in activities that impair trade.

Development Engagements: US trading partners need to understand the key role IP investments play in promoting growth in their own domestic economies, not merely as a *quid pro quo* for US market access for their non-IP based businesses. The US has a shared interest with other IP-based economies in providing assistance to commerce and related ministries in promoting understanding of the role of IP rights in fostering development, attracting foreign direct investment, and promoting technology transfer.

Capacity Building and Technical Assistance: Whether providing training to law enforcement or assistance in development-related activities mentioned above, coordination within the US government and between the US and other governments and international organizations, such as the World Intellectual Property Organization (WIPO), stands to increase

the value of these trainings. Where possible, and in particular for priority countries, comprehensive needs assessments should be carried out that can then form the basis for multi-year plans of assistance coordinated among governments and international organizations.

Improvements to Enforcement Regimes Abroad

In its engagement with US trading partners the US government should seek improvements in enforcement regimes, as needed, to ensure that our trading partners have the legal tools needed to reduce corporate end-user piracy of software. Specifically, the US government should, at a minimum seek to ensure that each of our trading partners has the following elements in place:

- **Criminal Liability for Corporate End User Piracy.** Article 61 of the WTO TRIPS Agreement requires all WTO members to have criminal penalties available at least in the case of willful copyright piracy on a commercial scale. Corporate end-user piracy has long been recognized to be one form of commercial scale piracy. When carried out willfully it should be subject to criminal sanctions. The US government should continue in its efforts to ensure that all of our trading partners make corporate end-user piracy subject to criminal sanctions. Laws that are not supported by effective enforcement regimes do little to deter piracy.²⁰
- **Pre-established (Statutory) Damages.** Statutory damages are an essential tool in civil litigation against end-user piracy, where poor or nonexistent recordkeeping by the infringer often makes it difficult to assess the full extent of actual damages. Statutory damages also serve as a deterrent, since they make it much more certain that infringers will face significant economic consequences as a result of their actions. Although US law has long provided for statutory damages, this provision is lacking in the laws of many of our trading partners. Establishing this remedy in the

²⁰ BSA's "Blueprint for Reducing Software Piracy" includes additional recommendations for government initiatives to promote compliance and encourage the use of licensed software. 2009 Piracy Study, supra note 7, at 21.

laws of our trading partners is a key goal of the business software industry.

C. Increase Resources for IP Law Enforcement

Software companies support active programs to reduce software theft in the US and abroad. BSA, for example, carries out enforcement actions on behalf of its members in the US and approximately 80 countries outside the US. But industry cannot meet this challenge alone. In cases involving organized counterfeiting of our products, or distribution on the Internet, the investigatory resources of the FBI and the deterrent value of criminal sanctions are needed.

Congress recognized the importance of providing law enforcement agencies with adequate funding by authorizing funding for three important initiatives in Title IV of the PRO-IP Act:

- \$25 million per year for grants to state and local law enforcement agencies to assist with federal enforcement of IP laws;
- \$10 million per year to assign at least 10 additional FBI agents to the Computer Crime and Intellectual Property Section (CCIPS) and to ensure that each Computer Hacking and Intellectual Property (CHIP) unit is supported by at least one FBI agent and two assistant US Attorneys; and
- \$10 million per year each to the FBI and the Justice Department's Criminal Division to hire and train law enforcement officers to investigate IP and computer crimes and to prosecute such crimes.

In communicating with the Congress during the current and future budget cycles, the Administration should, at a minimum, seek funding for these important initiatives. They should also seek to ensure that adequate funds are made available to coordinate with foreign governments in intercepting counterfeit products and running international cases. Individual agencies should also take account of these priorities in deploying any discretionary funds at their disposal.

Increased funding should also be accompanied by focused, specific targets for staffing, case volume, and case turn-around times.

D. A Note on Possible Legislative Proposals

The enactment of the PRO-IP Act in 2008 provided the federal government with a range of new tools and resources to coordinate and enhance intellectual property enforcement efforts (including the Joint Strategic Plan that is the subject of this submission). BSA supported this important legislation and looks forward to working with you and other officials in its implementation.

BSA is currently reviewing with our members potential options for legislative reforms beyond those contained in the PRO-IP Act. We will provide those recommendations to you soon.

We would like to interject a note of caution about two related proposals – “graduated response” and mandatory filtering – that have appeared in a number of countries overseas and could wend their way to our shores. Both relate to the role of Internet service providers (ISPs) and other intermediaries in addressing the very serious problem of online piracy. We do not believe the time is right to legislate on either of these subjects.

Graduated Response

We note that there has been a great deal of discussion about the asserted need for a “graduated response” or “three strikes” legislation to address some forms of Internet piracy. While proponents of these measures have been reluctant to define the full panoply of measures that could fall under this “graduated response” umbrella, as a general matter such legislation would require at least ISPs to take a series of steps in response to allegations of copyright infringement, ultimately leading to sanctions against persons who are deemed repeat infringers.

While we support taking action against repeat offenders, as we have learned from similar efforts in France and elsewhere, it has proved very challenging to find a legislative approach that effectively deters online piracy while respecting users’ rights and interests, and safeguarding the myriad legal activities that require access to the Internet. These include such increasingly indispensable activities as online banking, monitoring a

child's progress in school, managing one's health care and receiving instantaneous alerts concerning natural disasters and other threats.

BSA supports action by ISPs against repeat infringers, whether in the US or abroad. We believe that responsible action should be taken on a voluntary basis, and under the terms of service contracts between users and service providers. When it comes to government policies that require ISPs or others to impose sanctions, including potentially the suspension or termination of Internet access, it is important that appropriate safeguards – particularly due process protections – are put into place to protect subscribers. BSA members have articulated a set of key principles on graduated response (copy attached).²¹

Mandatory Filtering

Legislation in France formalizes an agreement among the motion picture industry, the recording industry, ISPs and the French government, under which French ISPs have agreed to use filtering, fingerprinting and watermarking technologies in connection with their hosting and content sharing platforms. This has led to calls for similar legislation in other jurisdictions in Europe and beyond.

Technology has long been looked upon a potential answer to online piracy of content. The use of filtering tools to detect and block infringing content has been proposed to lawmakers as a “silver bullet” that could stop infringing uploads and downloads in their tracks. In truth, the situation is far more complex.

Filtering raises substantial questions of privacy and censorship. Too often those who advocate filtering solutions simply ignore these important private rights and focus exclusively on only one issue, namely copyright infringement. In practice, there are many simple technical means to defeat content filtering schemes. The impact of measures such as scrambling, encryption, format variations, mark and fingerprint stripping, on the effectiveness of the proposed solution should be taken

²¹ BSA's “Position on Appropriate Measures to Deter Online Piracy of Content” is available online at <http://www.bsa.org/country/Public%20Policy/intellectual-property/online-piracy-content.aspx>.

into account. It is also imperative that filtering systems allow legitimate network traffic to pass through unaffected. Technology companies are unaware of any existing technology that meets those criteria.

The development and deployment of filtering technologies entails significant costs. It has the potential to disrupt networks and degrade performance. Placing these burdens entirely on ISPs and technology companies would be unfair and inappropriate.

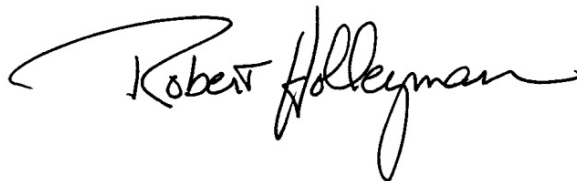
Mandated use of filtering technology is a special case of the broader issue of technology mandates. The technology industry strongly opposes government mandated use of particular technologies. The regulatory process is not well suited to the pace of technological development. To the contrary, all evidence suggests that technology develops most effectively in response to marketplace forces. Regulated mandates would freeze in place a particular technology, stifling innovation.

BSA supports the right of ISPs and right holders to enter into purely voluntary agreements that each believes is in its respective business interests to manage network traffic, including those mitigating the effects of those network users who repeatedly misuse their Internet service to infringe copyright. However, we strongly oppose the imposition of regulatory requirements on ISPs and technology providers aimed at detecting, intercepting or preventing online copyright infringements.

• • •

BSA appreciates this opportunity to provide its views on the Joint Strategic Plan.

Sincerely,

A handwritten signature in black ink that reads "Robert Holleyman". The signature is fluid and cursive, with a large, sweeping initial "R" that loops back under the first name.

Robert W. Holleyman
President and Chief Executive Officer

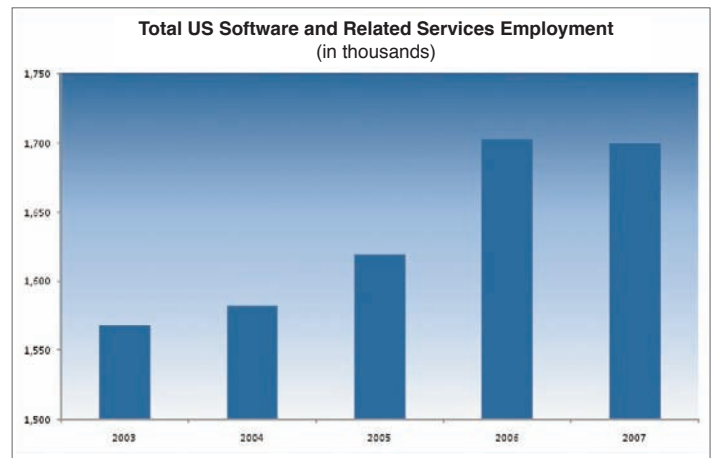
Attachment 1

Software Industry Facts and Figures

The software industry employs more than 1 million people in the US...

- **ENGINE OF EMPLOYMENT:** The software and related services sector employed 1.7 million people in the US in 2007.

[Source: OECD, STAN Database for Structural Analysis, ed. 2008]

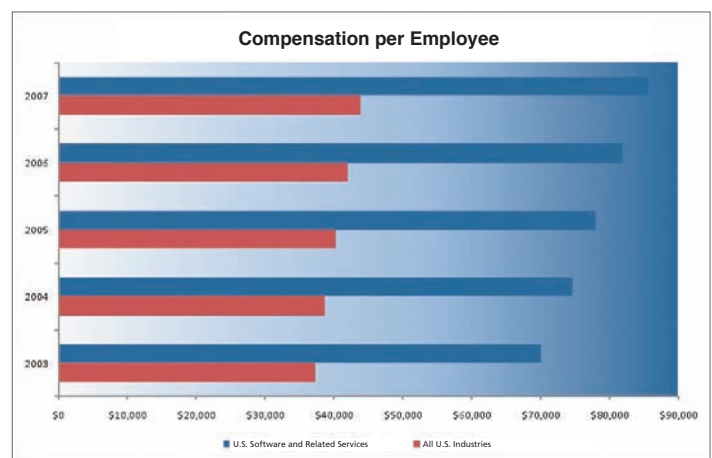


Source: OECD, STAN Database for Structural Analysis, ed. 2008

... In jobs that pay nearly twice the national average

- **GOOD, HIGH-PAYING JOBS:** On average, workers in the software and related services sector were paid \$85,600 in 2007. This is 195% of the national average.

[Source: OECD, STAN Database for Structural Analysis, ed. 2008]

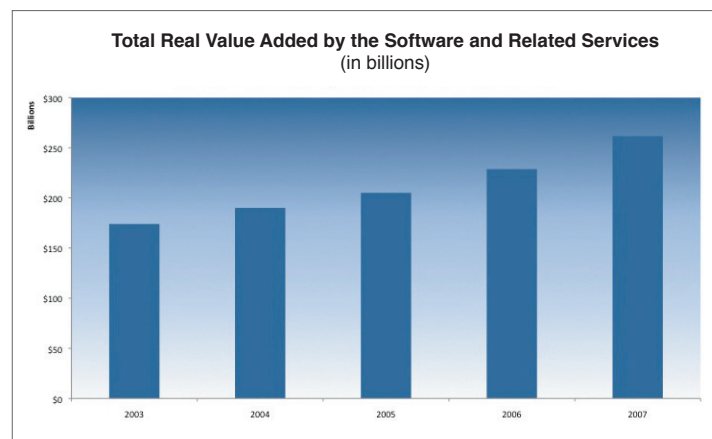


Source: OECD, STAN Database for Structural Analysis, ed. 2008

The software industry adds more than \$260 billion in value to the US economy...

- **CONTRIBUTING TO NATIONAL PROSPERITY:** The software and related services sector's real contribution to GDP exceeded \$261 billion in 2007. (This was nearly twice as large as the real value added by the entire recreational, cultural and sporting sector.)

[Source: OECD, STAN Database for Structural Analysis, ed. 2008]



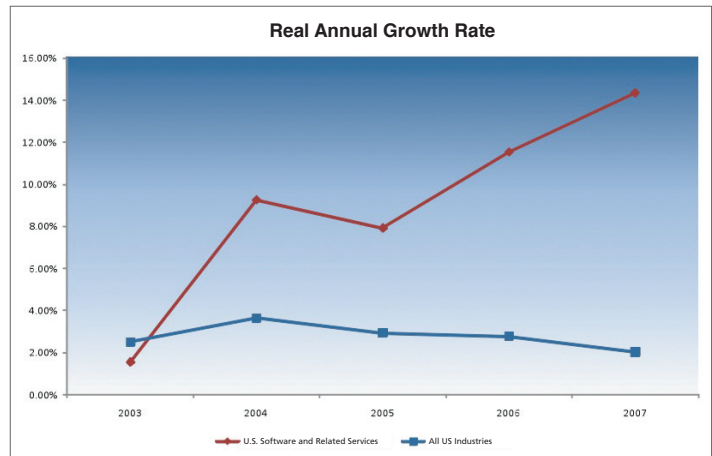
Source: OECD, STAN Database for Structural Analysis, ed. 2008

... And its contribution has historically grown much faster than the rest of the economy

• **OUTPERFORMING THE ECONOMY:**

In 2007, the software and related services sector experienced a real annual growth rate of 14%, compared with a real annual growth rate of 2% for all US industries. This sector has outpaced the rest of the economy in each year since 2003.

[Source: OECD, STAN Database for Structural Analysis, ed. 2008]

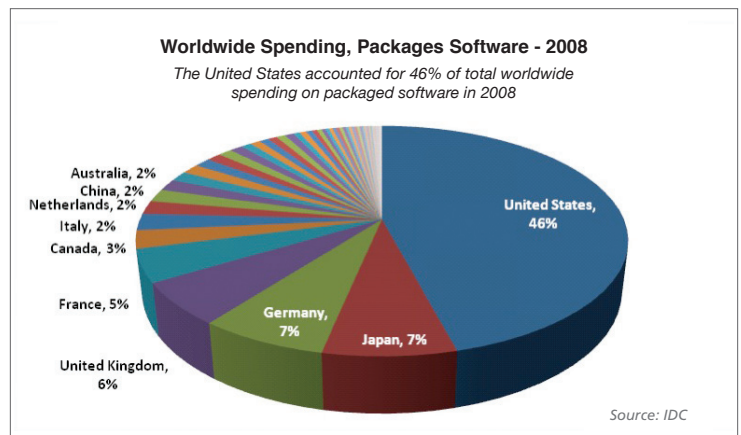


Source: OECD, STAN Database for Structural Analysis, ed. 2008

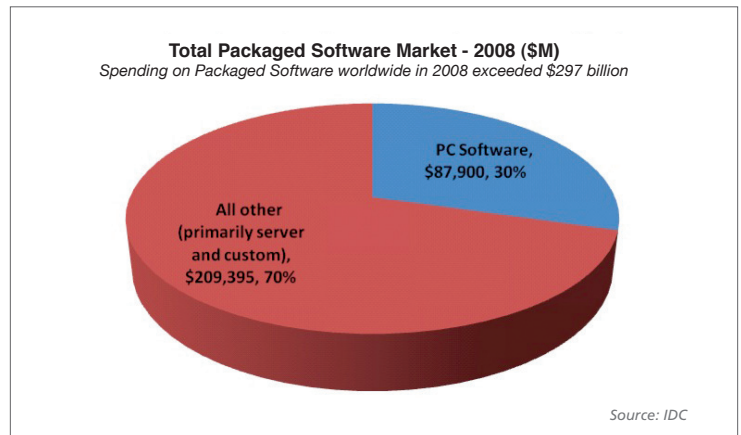
The software market is large and highly globalized...

• **TOP SOFTWARE-USING NATIONS:** In 2008, the US share of the packaged software market was \$136.6 billion, or 45.9% of the world market. Although the US is the single largest software market in the world, more than half of the world's software market lies outside the US. [Source: IDC]

• **GLOBAL MARKET SIZE:** The worldwide PC software market was \$88 billion in 2008, representing 30% of the total packaged-software market, which was \$297 billion. Packaged software includes applications (e.g., Corel Draw, or Autodesk Autocad), application development and deployment tools (e.g. Adobe ColdFusion or Embarcadero RAD Studio 2010), and system infrastructure software (e.g., Microsoft .NET Framework). PC software includes all packaged software that runs on personal computers, including operating systems (e.g., Apple OS X and Microsoft Windows), systems software such as databases (e.g., Sybase Advanced Server Enterprise 15), security packages (e.g., Symantec Norton 360 or McAfee Total Protection), and business and consumer applications (e.g., Intuit Quicken, Rosetta Stone, Corel WordPerfect or Quark QuarkXPress). [Source: IDC]



Source: IDC



Source: IDC

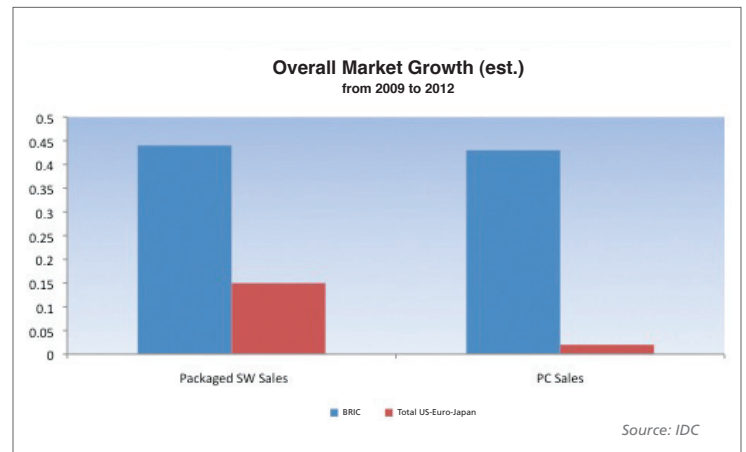
• **NUMBER OF UNITS SHIPPED:** About 3.6 billion units of software were deployed in 2008, a 20% increase over 2007. Approximately 288 million PCs were shipped, a 10% increase over 2007. [Source: IDC]

... And the fastest growth is in emerging markets

• EXPLOSIVE GROWTH FORECASTED IN "BRIC" COUNTRIES:

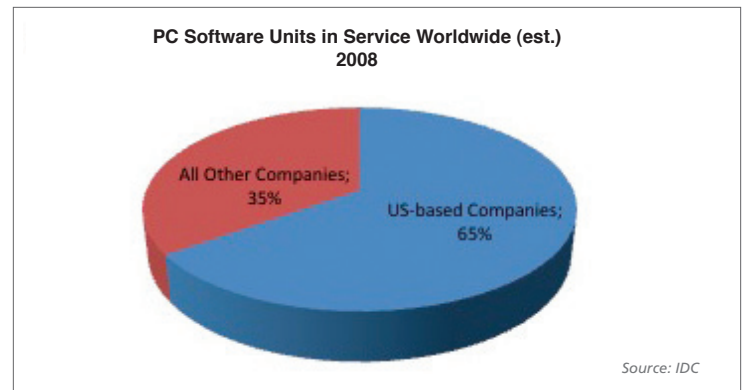
PC sales in the so-called "BRIC" markets (Brazil, Russia, India, and China) are projected to grow by 43% between 2009 and 2012 to a total of more than \$66 billion. By comparison, PC sales are projected to grow only 2% in the United States; Central, Eastern, and Western Europe; and Japan collectively in this timeframe.

Over the same period, packaged software sales in the BRIC markets are projected to rise by 44% to a total of nearly \$22 billion. By comparison, packaged-software sales are projected to grow 15% in the United States; Central, Eastern, and Western Europe; and Japan collectively in this timeframe. By 2011, the BRIC markets will account for 25% of global PC sales and 6% of packaged software sales. [Source: IDC]



US-based companies are leading the world in meeting this demand...

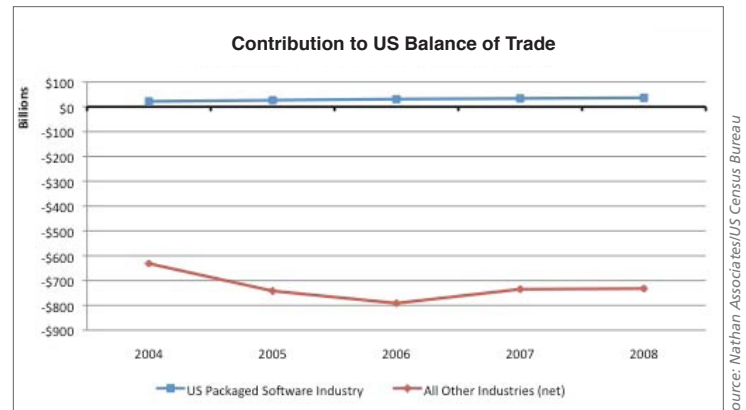
- **US LEADERSHIP IN GLOBAL MARKET:** An estimated 65% of the PC software units in service worldwide in 2008 were from US-based companies. In recent years, about 60% of global spending on PC software has been paid to US-based software companies. [Source: IDC]
- **IMPORTANCE OF OVERSEAS MARKETS:** Non-US sales represent more than 50% of revenues for most of BSA's publicly traded member companies. [Source: Business Software Alliance analysis of US SEC Forms 10-K]



... And contribute significantly to US trade performance

• A TOP CONTRIBUTOR TO US TRADE PERFORMANCE:

The US packaged-software industry contributed an estimated \$36 billion surplus to the US balance of trade in 2008. [Source: Nathan Associates]



The IT industries are leaders in innovation. . .

- **INVESTMENT IN R&D:** BSA's publicly traded member companies spent nearly \$43 billion on R&D in 2008, equal to 7.1% of their collective revenues. Many of BSA's member companies invested double or triple that percentage of their revenues in 2008. [Source: *Business Software Alliance*]
- **PATENTS:** BSA member companies hold nearly 90,000 US patents, and several BSA members were among the top 15 US companies awarded patents in 2006 and 2007. [Source: *Business Software Alliance*]

... And provide benefits throughout the economy

- **SOLUTIONS TO BUSINESS CHALLENGES:** Software drives productivity and innovation in almost every economic sector, helping businesses of all sizes perform better in good times and bad. Some of the top 15 industry users of information technology (IT) are manufacturing, telecoms, financial services, construction, health, and utilities.
- **IT LEADS PRODUCTIVITY GROWTH:** In the United States, IT was responsible for two-thirds of total factor growth in productivity between 1995 and 2002, and virtually all of the growth in labor productivity. [Source: *Information Technology Industry Foundation*]

Top US industries Investing in IT, 2008

(In US dollars)

Banking	\$59.4 billion
Communications & Media	\$50.7 billion
Construction	\$34.2 billion
Discrete Manufacturing	\$33.7 billion
Securities and Investment Services	\$31.5 billion
Health Care	\$24.9 billion
Insurance	\$23.5 billion
Process Manufacturing	\$21.5 billion
Resource Industries	\$19.6 billion
Retail	\$19.0 billion
Professional Services	\$15.5 billion
Transportation	\$15.0 billion
Utilities	\$9.6 billion
Wholesale	\$5.7 billion
Consumer & Recreational Services	\$4.1 billion
	\$368.5 billion

Source: IDC, US Black Book Q2 2009



1150 18th Street, NW
Suite 700
Washington, DC 20036

T: +1.202.872.5500
F: +1.202.872.5501
WWW.BSA.ORG

Attachment 2

Table 1

Worldwide Packaged Software Sales and the U.S. Trade Balance for All and Selected Industries, Including the U.S.-Owned Software Industry, 1997-2008 (\$billion)

Year	Worldwide Packaged Software Sales /a	% Change	Trade Balances for U.S. Industries (+ surplus or - deficit) /b							
			United States /c	% Change	Software /d	% Change	Agriculture	Petroleum	Motor Vehicles	Finance
1997	126.4	-	-20.4	-	18.3 /e	-	-	-	-	-
1998	143.0	13.1%	-83.1	308.1%	18.8	2.8%	-	-	-	-
1999	159.7	11.7%	-172.7	107.9%	19.7	5.0%	-	-	-	-
2000	176.1	10.3%	-274.1	58.7%	19.8	0.3%	11.0	-104.8	-116.0	24.3
2001	173.1	-1.7%	-254.5	-7.2%	18.0	-9.0%	-	-	-	-
2002	177.0	2.3%	-325.7	28.0%	19.9 /f	10.6%	-	-	-	-
2003	183.1	3.4%	-387.2	18.9%	20.7	4.1%	-	-	-	-
2004	189.0 /g	3.2%	-492.1	27.1%	21.6 /h	4.2%	-	-	-	-
2005	220.0 /i	16.4%	-593.7	20.7%	26.7 /j	23.8%	6.2	-228.1	-141.9	36.8
2006	244.0	10.9%	-630.4	6.2%	31.0	16.0%	8.3	-273.6	-151.4	30.7
2007	263.5	8.0%	-840.6	33.3%	33.5	8.0%	-	-	-	-
2008	286.2 /k	8.6%	not available		36.4	8.6%	-	-	-	-

a. From various releases of IDC data.

b. Current-account balances on goods, services, and income.

c. Excludes military and government transactions. Previously reported trade balances were revised to account for additional data and revisions to the methodology employed by the Bureau of Economic Analysis (BEA). See Table 2 for all underlying data and calculations. Results are in row 47 of Table 2.

d. See Table 3 for all underlying data and calculations. Results are in row 30 of Table 3.

e. In 1999, value was originally calculated to equal \$13.0 billion. The value was recalculated in 2004 and revised upward to \$18.3 billion.

f. In June 2004, the predicted value for 2002 was revised downward from \$24.3 billion to \$19.9 billion to reflect revisions to 2002 worldwide software sales.

g. Revised downward from \$193.3 (projected by IDC in December 2003) to \$189 (estimated by IDC in November 2004). See http://news.com.com/IDC+Software+sales+to+hit+189+billion/2100-1014_3-5440877.html.

h. Revised downward in 2004 to reflect downward revision in worldwide sales.

i. Revised upward from a previous estimate of 196.9. The previous estimate was based on SIIA reported global software industry growth in 2005 of 4.2%. See www.sii.net/software/pubs/stat-03.pdf. Revised worldwide sales are from IDC.

j. Revised upward from previous Nathan Associates estimate of \$22.5 billion. Revision reflects revised worldwide sales of software and revised U.S. share of worldwide consumption.

k. IDC forecast.

SOURCES: Nathan Associates Inc. and others cited in the notes.

COMPOUND ANNUAL GROWTH RATES	
U.S. deficit	
Past five years (2003-2007)	21.4%
Past 10 years (1998-2007)	78.3%
Software industry surplus	
Past five years (2003-2007)	12.8%
Past 10 years (1998-2007)	15.6%
Worldwide software sales	
Past five years (2003-2007)	9.5%
Past 10 years (1998-2007)	16.5%

Attachment 3

DOES LOWERING PC SOFTWARE PIRACY ACTUALLY CREATE BENEFITS FOR COUNTRIES?

FOUR CASE STUDIES

March 2009

Prepared for Microsoft

INTRODUCTION

In 2002, IDC created its first study of the economic impact of lowering piracy for the Business Software Alliance. Two additional studies were conducted roughly every two years.

In these studies, IDC forecasted what would happen if piracy could be lowered 2.5% a year from the current level in terms of job creation, local revenues, and tax revenues.

The operating theory was that lowering piracy would increase sales of legitimate software, which would increase related services and channels revenues, which would, in turn support new employment. That employment would generate new taxes.

Since the first study, four countries have come close to or exceeded the theoretical drop of 10% over four years, albeit not as evenly as 2.5% a year, and not all starting in 2003. Those countries are:

- ❑ China, from 92% in 2003 to 82% in 2007
- ❑ Egypt, from 69% in 2003 to 60% in 2007
- ❑ Russia, from 87% in 2004 to 73% in 2007
- ❑ Vietnam, from 92% in 2004 to 85% in 2007

This study revisits those countries and the earlier studies to see if subsequent events have borne out the IDC predictions.

Study Methodology

Validating the original IDC study is not as easily as simply reviewing the 2002 forecasts for several reasons:

- ❑ The original studies were based on IT market forecasts at the time; actual IT market performance varied from those forecasts.
- ❑ The first two studies looked at the impact of lowering software piracy on ALL software, including PC, server, and mainframe software. The last study looked at the impact of lowering ONLY PC software.

- ❑ The piracy reductions began at different times and only in one case was exactly 10%; in no case was the actual drop in piracy as regular as 2.5% a year.

Thus, to test previous predictions on how much lowering PC software piracy by 10% over four years would actually benefit the target countries, IDC had to first recreate the forecast but for PC software, excluding server and mainframe software. We then also had to shift everything by one year to begin at 2003 and see what lowering by 2.5% in each of 2004, 2005, 2006, and 2007 would mean.

Finally, we had to decide what to do with market growth. General market growth at a steady piracy rate would also create jobs, local revenues, tax receipts etc.

Our solution was first to create a scenario was to recreate the 2002 Piracy Impact Model, adjust it to account for lowering PC software piracy only, and time shift the starting year to 2003. This would be our new predicted impact from lowering piracy. We then took the same model, input the actual piracy rate drops for the target countries, to see what the model would predict. Then we compared it to actual growth in employment, revenues, and tax receipts.

There are some important exclusions in the study:

- ❑ IT professionals in end using organizations are treated as if they are not affected by lower piracy, thus they are not counted in any employment totals.
- ❑ Local revenues are only those for software, services, and channels firms.
- ❑ The algorithms that relate lower software piracy to increased revenues in services or distribution do not assume a one-to-one ratio.

Key Findings

Across all the countries our analysis found that:

- ❑ In country job creation and local revenues vastly exceeded our forecasts for job creation and revenues created from *just* lowering PC software piracy. This difference we call “autonomous” growth. This also leads us to believe our original forecasts were conservative.
- ❑ Predicted and actual piracy benefits were often close. The variance may relate to timing of the piracy drop –dropping sooner in the cycle leads to more actualized benefits.
- ❑ The aggregate benefits from lowering PC piracy accounted for 7%-20% of total growth in employment, tax revenues, etc., depending on the country. The variance between countries can relate to a number of factors, from the IT spending mix (hardware, software, services), starting piracy rate (the higher the starting rate the more growth in the legitimate market created by a 10% drop in piracy), and IT market dynamics.
- ❑ In all countries the total software market doubled or nearly did from 2003 to 2007. Software-related employment grew by more than 50%.

In the graphics that follow, note that we are looking at job growth form 2003 to 2007 in the IT industry (we exclude IT professionals), and revenues to firms that remain in country, either local firms or the local portion for multinationals with operations in the country, and tax receipts from social taxes, VAT, and other fees.

Country Specific Findings

China

The re-forecasted Piracy Impact Model for China predicted an additional 222,000 jobs from lower PC piracy from 2003-2007. In actuality, total job growth was 786,000, of which we believe 213,000 was the result of the actual fall of the PC piracy rate.

Similar patterns are shown for in-country revenues and tax receipts. China's gains were aided by the fact that the PC piracy rate dropped early in the four year period, which gave the benefits from lower rates a chance to compound in following years.

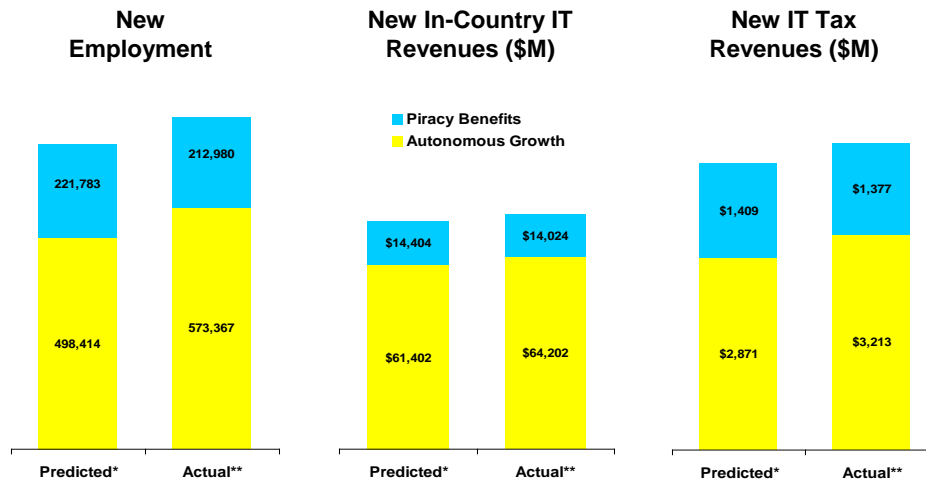
From 2003 to 2007, IDC believes China added 2 million jobs to the overall labor force, including more than 1 million in the IT professional cadre. Over time, IDC expects some of these employees to migrate to the services sector, raising growth there.

The re-forecasting exercise indicates that:

- ❑ Nearly 27% of new jobs in the IT sector can be attributed to lower PC piracy
- ❑ Nearly 18% of new in-country revenues can be attributed to lower PC piracy.

China

Benefits from Lower PC Piracy, 2003-2007



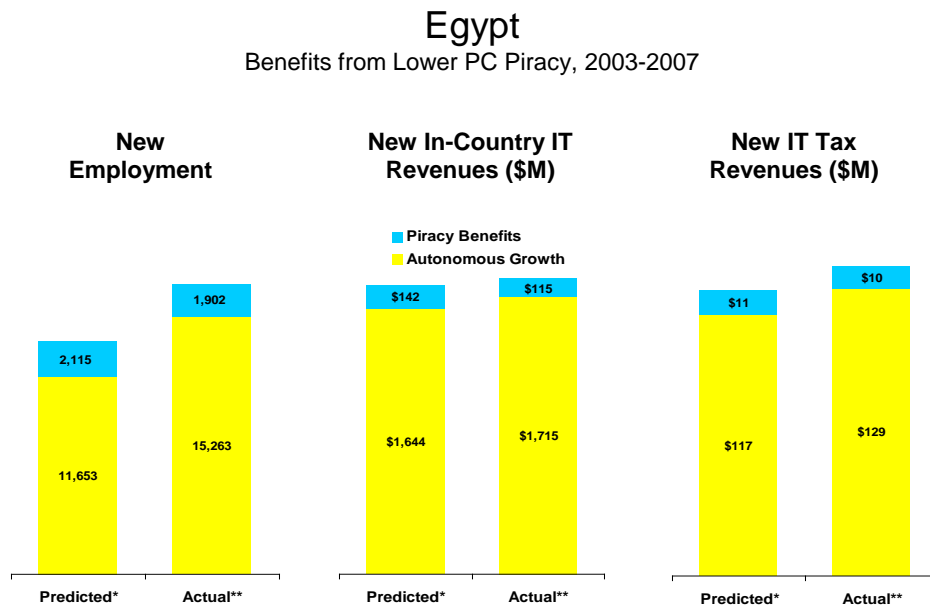
* Re-forecasted based on PC software piracy reduction and a 2.5% per year drop from 2003-2007

** Actual IDC data for 2003-2007 including the benefits from lowering PC software Piracy. All \$ values based on constant 2007 US\$

Egypt

While Egypt's market grew faster than IDC predicted in 2003 – it more than doubled between 2003 and 2007 – piracy didn't drop a full 10% in the target period, which is the reason the re-forecast overshoot actuals as a percent of total growth. The analysis shows that lower PC piracy accounted for:

- ❑ 11% of all new jobs created in the IT sector
- ❑ 6% of new in-country IT revenues
- ❑ 7% of new tax revenues



* Re-forecasted based on PC software piracy reduction and a 2.5% per year drop from 2003-2007

** Actual IDC data for 2003-2007 including the benefits from lowering PC software Piracy. All \$ values based on constant 2007 US\$

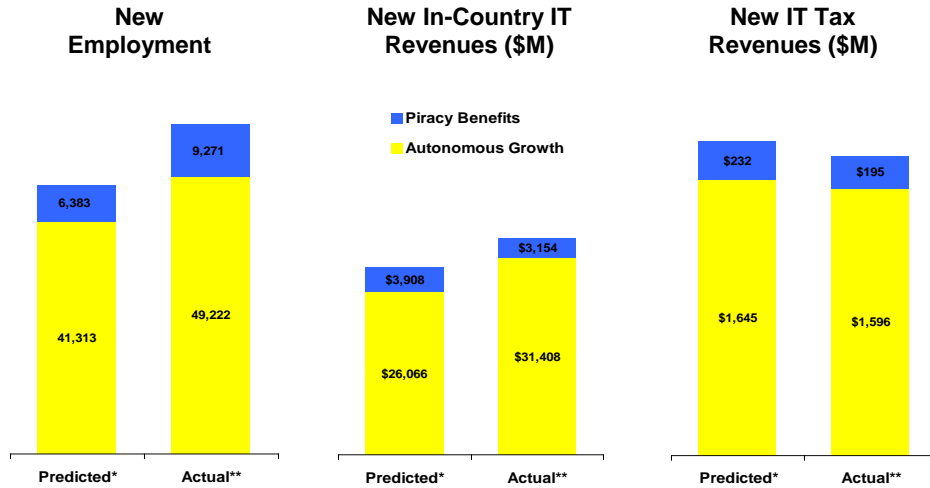
Russia

Russia nicely overshoot the 2.5% per year drop in piracy, although it wasn't done evenly. Much of the gain was in the last year – else it's actual benefit from lowering piracy would have been bigger. During that time, Russia's domestic spending grew 130%. The analysis shows that lower PC piracy account for:

- ❑ 16% of all new jobs created in the IT sector
- ❑ 9% of new in-country IT revenues
- ❑ 11% pf new tax revenues

Russia

Benefits from Lower PC Piracy, 2003-2007



* Re-forecasted based on PC software piracy reduction and a 2.5% per year drop from 2003-2007
 ** Actual IDC data for 2003-2007 including the benefits from lowering PC software Piracy. All \$ values based on constant 2007 US\$

Vietnam

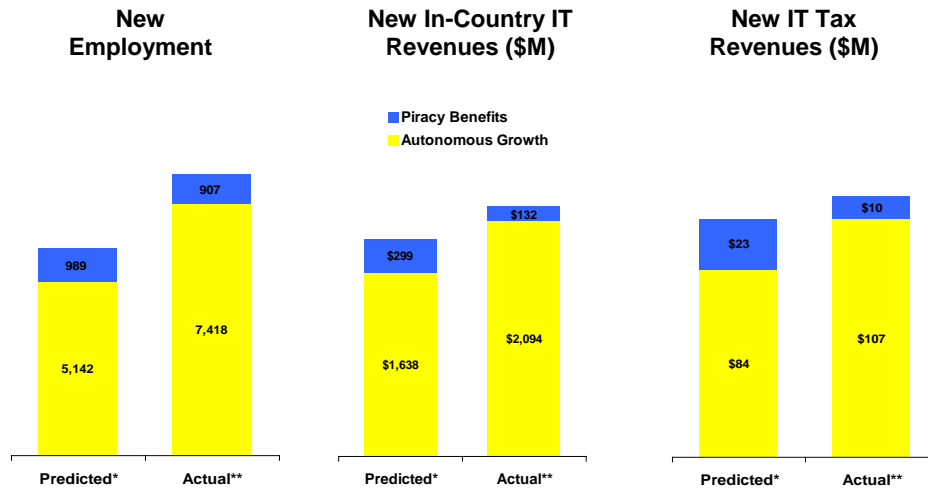
Although Vietnam's domestic IT spending grew 130% from 2003 to 2007, PC software piracy didn't drop a full 10 points, which is why the benefits from lowering PC piracy were lower than forecasted.

Nevertheless, The analysis shows that lower PC piracy account for:

- 11% of all new jobs created in the IT sector
- 6% of new in-country IT revenues
- 9% of new tax revenues

Vietnam

Benefits from Lower PC Piracy, 2003-2007



* Re-forecasted based on PC software piracy reduction and a 2.5% per year drop from 2003-2007

** Actual IDC data for 2003-2007 including the benefits from lowering PC software Piracy. All \$ values based on constant 2007 US\$

But Is This Proof?

Because the methodology of the original projection and the one showing the actuals we show here are based on a market model, one could question whether the “actuals” are, in fact actual.

Given the few data points, statistical correlations are only so useful. Testing the correlation between the piracy rate and employment in Russia from 2003-2007 we got a Pearson correlation of $-.86$, which says as the piracy rate goes down the employment rate goes up. But the significance test on the correlation just missed the cutoff ($.06$ versus a cutoff of $.05$), which means some of the correlation could be random.

So the question is, how much of the increase in jobs and revenues for our four countries from 2003 through 2007 is related to sheer market growth, how much to lower PC software piracy?

IDC’s analysis of the countries tracked in the annual BSA PC software piracy study invariably shows that countries that see their piracy rates drop over time see their software industry revenues grow to the level of countries already at the lower piracy rate.

And in this analysis, where new local revenues predicted by the model are often less than 10% of actual new local revenues – and where PCs often account for more than 50% of the value of hardware shipped – IDC believes that the projections of the “actuals” are conservative.

The Economic Benefits of Lowering PC Software Piracy

China

	2003	2004	2005	2006	2007	2003-2007 Cumulative
PC Software Piracy Rate						
Original Model	92%	90%	87%	85%	82%	
Actual	92%	90%	86%	82%	82%	
Employment						
Actual	1,648,291	1,820,116	1,959,278	2,183,481	2,434,309	786,018
Projected New Growth from Original Model*		196,176	182,531	163,916	221,783	221,783
New Growth from Actual Drop in PC Piracy		165,073	216,943	198,274	212,980	212,980
In-Country Revenues*						
Actual	\$38,569	\$45,286	\$51,331	\$61,809	\$73,978	\$78,227
Projected Growth from Original Model*		\$3,274	\$3,343	\$3,243	\$4,543	\$14,404
Growth from Actual PC Piracy Drop		\$2,695	\$3,602	\$3,598	\$4,129	\$14,024
Tax Receipts (\$M)						
Actual	\$2,516	\$2,908	\$3,245	\$3,886	\$4,614	\$4,590
Projected Growth from Original Model*		\$339	\$334	\$312	\$424	\$1,409
Growth from Actual PC Piracy Drop		\$279	\$362	\$348	\$388	\$1,377

Egypt

	2003	2004	2005	2006	2007	2003-2007 Cumulative
PC Software Piracy Rate						
Original Model	69%	66%	64%	61%	59%	
Actual	69%	65%	64%	63%	60%	
Employment						
Actual	31,813	35,348	39,275	44,012	48,979	17,166
Projected New Growth from Original Model*		417	837	1,318	2,115	2,115
New Growth from Actual Drop in PC Piracy		758	938	1,240	1,902	1,902
In-Country Revenues*						
Actual	\$957	\$1,108	\$1,276	\$1,490	\$1,783	\$1,830
Projected Growth from Original Model*		\$11	\$24	\$39	\$67	\$142
Growth from Actual PC Piracy Drop		\$16	\$21	\$30	\$48	\$115
Tax Receipts (\$M)						
Actual	\$38	\$57	\$66	\$76	\$90	\$139
Projected Growth from Original Model*		\$1	\$2	\$3	\$5	\$11
Growth from Actual PC Piracy Drop		\$1	\$2	\$2	\$4	\$10

Russia

	2003	2004	2005	2006	2007	2003-2007 Cumulative
PC Software Piracy Rate						
Original Model	87%	85%	82%	80%	77%	
Actual	87%	87%	83%	80%	73%	
Employment						
Actual	78,159	86,261	99,451	111,977	136,652	58,493
Projected New Growth from Original Model*		3,206	4,001	4,907	6,383	6,383
New Growth from Actual Drop in PC Piracy		429	3,108	4,131	9,271	9,271
In-Country Revenues*						
Actual	\$11,118	\$14,018	\$17,506	\$20,730	\$26,872	\$34,652
Projected Growth from Original Model*		\$616	\$814	\$1,054	\$1,424	\$3,908
Growth from Actual PC Piracy Drop		\$69	\$539	\$759	\$1,787	\$3,154
Tax Receipts (\$M)						
Actual	\$836	\$969	\$1,114	\$1,319	\$1,735	\$1,791
Projected Growth from Original Model*		\$37	\$48	\$62	\$85	\$232
Growth from Actual PC Piracy Drop		\$4	\$33	\$47	\$110	\$195

Vietnam

	2003	2004	2005	2006	2007	2003-2007 Cumulative
PC Software Piracy Rate						
Original Model	92%	90%	87%	85%	82%	
Actual	92%	92%	90%	88%	85%	
Employment						
Actual	10,771	11,779	13,052	15,209	19,096	8,325
Projected New Growth from Original Model*		664	710	696	989	989
New Growth from Actual Drop in PC Piracy		-49	312	513	907	907
In-Country Revenues*						
Actual	\$954	\$1,094	\$1,268	\$1,572	\$2,108	\$2,226
Projected Growth from Original Model*		\$61	\$67	\$68	\$103	\$299
Growth from Actual PC Piracy Drop		-\$4	\$23	\$39	\$73	\$132
Tax Receipts (\$M)						
Actual	\$44	\$51	\$59	\$79	\$106	\$117
Projected Growth from Original Model*		\$5	\$5	\$5	\$8	\$23
Growth from Actual PC Piracy Drop		\$0	\$2	\$3	\$6	\$10

* Includes software, services, distribution, excludes hardware

Attachment 4

Deterring Online Piracy of Content

BSA Position on Appropriate Measures to Deter Online Piracy of Content

Online piracy presents a serious and immediate threat to software developers as well as to other copyright-based industries. Too many persons now treat illicit acquisition of copyrighted works online as a routine matter, ignoring the fact that they are engaging in illegal acts. But it is important not to lose track of the fact that the vast majority of individuals and businesses use software, computers, and the Internet for a myriad of legal and legitimate personal and business reasons.

The current voluntary industry-led approach to developing technologies to address online content piracy continues to be effective and mandated use of any such technologies is not justified. Measures taken should be tailored to the content piracy issue identified and Government's role should be to ensure that legal offerings for digital content services are facilitated.

BSA members approach proposed solutions to address online content piracy with two objectives:

1. To effectively deter illicit downloading, uploading, making available and use of content, and,
2. To ensure existing technologies function as designed, that innovation and the development of new technologies and services are not obstructed, and that users' enjoyment of software, computers and the Internet is not diminished.

BSA members believe due care must be taken to ensure policies meet both considerations. We believe the following principles provide the basis for achieving this balance.

1. Some anti-piracy content identification and filtering technologies may play a useful role in deterring piracy in some limited cases, but they are not a "silver bullet" solution to piracy. Rather, addressing piracy effectively requires ongoing voluntary inter-industry efforts.
2. In appropriate circumstances, BSA supports:
 - a) Automated educational notification mechanisms for alleged online infringers and a requirement for ISPs to preserve evidence of repeated infringements such as a user's IP address to enable anti-piracy court proceedings and administrative anti-piracy procedures or appropriate enforcement actions, subject to appropriate safeguards, including those governing privacy;
 - b) The imposition of appropriate sanctions, including blocking a

user, blocking a site, and the suspension or termination of Internet service for individual repeat offenders, provided:

Such sanctions against individual repeat offenders shall be based on either:

i) Breach of contract, i.e., the terms of subscriber's contract with the service provider. (Contractual mechanisms are a helpful and efficient way of dealing with online piracy and should be encouraged and widely implemented.) or

ii) Through a decision by an administrative or judicial entity, provided such entity gives all parties an opportunity to be heard and to present evidence, and that the decision can be appealed before an impartial court. Before an order becomes final, parties shall have the opportunity to have the order stayed pending appeal to courts.

3. When developing steps to address online content piracy, the following shall also be given due consideration:

a) The voluntary development and use of anti-piracy content identification and filtering technologies should continue unimpeded: this self-regulatory approach is the effective way to address piracy. The specific technologies themselves should be developed through voluntary processes open to all affected stakeholders, and the results should be based on consensus of the participants.

b) In specific cases where anti-piracy content identification and filtering technology is used, it should be demonstrated to be robust, renewable, interoperable, free of unintended consequences for existing systems, and any other relevant criteria necessary to ensure users' experience will not be degraded and the development and deployment of new technologies will not be impeded.

c) Where it is determined that it is necessary to empower national judicial or administrative entities to require the use of anti-piracy content identification and filtering technologies, such entities shall impose the requirement as a remedy on a case-by-case basis, in view of the specific facts presented, and after all affected stakeholders have had an opportunity to assess the impact of the specific anti-piracy content identification or filter's use on their technologies, and identified issues have been comprehensively addressed.

4. BSA opposes:

a) The termination of ISP services or any other sanctions or penalties imposed on alleged infringers without due process and, at a minimum, a right of appeal to a judicial authority,

except when such penalties are imposed as a result of a breach of contract with the service provider.

b) Imposition of broad anti-piracy content identification and filtering technological requirements applicable to all Internet users, or all computers and software used to access the Internet, by legislation, administrative fiat or adjudication.
