



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

p 202/872-5500
f 202/872-5501

December 10, 2010

VIA EMAIL

The Honorable Gary Locke
Secretary of Commerce
US Department of Commerce
1401 Constitution Ave. NW
Washington, DC 20230

Re: Inquiry on Copyright Policy, Creativity, and Innovation in the
Internet Economy (75 Fed. Reg. 61,419)

Dear Secretary Locke:

The Business Software Alliance (BSA)¹ appreciates this opportunity to provide comments regarding the Department of Commerce's Internet Policy Task Force review of the relationship between the availability and protection of online copyrighted works and innovation in the Internet economy.

The member companies of the Business Software Alliance all rely on comprehensive and enforceable intellectual property laws. Copyrights, as well as patents and trademarks are indispensable to the continuing development of the software industry. Copyright law plays an especially important role in promoting innovation in the many software tools that make the Internet work. We see copyright law as not only fully compatible with the further evolution and health of the Internet, but

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

indispensable. Every element of the many building blocks of the Internet is subject to intellectual property law. As an example, now-emerging software-based cloud solutions, which the Obama Administration has embraced as a way to improve citizen access and cut technology costs, all rely on copyright law.

In analyzing the many submissions provided in response to this NOI, we urge the Department to keep in mind three facts: intellectual property laws promote innovation and a healthy software industry; such laws are fully compatible with both existing innovations and emerging software-based solutions such as cloud computing; and, while the threats of piracy are real and important to address, the focus of government efforts should be on improving the ability to reach the bad acts of individuals determined to derive an unfair benefit from exploiting the property of others. The focus should not be on so-called "intermediaries" or other companies engaged in the job-creating business of delivering technology solutions or promoting e-commerce. The Department should reject recommendations seeking changes to law which would dampen the evolution of the Internet and multipurpose technologies which are indispensable to our economic recovery and long-term sustained job creation and economic growth.

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 responses to the specific questions posed in the Notice of Inquiry.

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 critical contributor of jobs and economic growth. The US software and related services industry directly employs 1.7 million people. 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 use, reproduction or distribution of copyrighted software without the consent of the software developer. Software theft is by far the largest form of copyright piracy in dollar terms. 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 copies for their own internal usage without authorization or in excess of what is permitted under their licenses. We commonly refer to this activity as “organizational end-user piracy.”⁵ While the economic impact of Internet piracy on the software industry is smaller than that of organizational end-user piracy, it is also a serious and growing problem.

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. More recent US economic figures 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).

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

Organizational end-user piracy

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 software intended for educational institutions 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 majority of the economic harm that our industry experiences from software theft.

Most often, organizational end-user piracy is undertaken willfully, with management fully aware and supportive of the conduct. In some 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.

Internet piracy

The Internet is an indispensable part of global communication and commerce. It has opened opportunities for faster, more efficient and more cost-effective distribution of information, products and services across the globe. It has also enabled 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 delivered over the Internet, but also comprise a key component of the Internet infrastructure.

In addition to creating significant social and economic opportunities, in some cases the borderless and anonymous character of the Internet makes it an ideal forum for persons determined to engage in illegal acts such as committing fraud, spreading malware, and engaging in piracy. The worldwide availability of the Internet also creates challenges in enforcing right 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.

Impact of Software Theft

In 2009, more than four out of every 10 copies of software in use worldwide – with a value of more than \$51 billion – was stolen.⁶ But the impact of software piracy extends far beyond the value of the software itself: Pirates also steal jobs and tax revenues.

A study conducted for BSA by IDC in 2010 affirmed earlier findings that lowering software piracy rates stimulates the entire IT sector, creating jobs and increasing economic growth and tax revenues. On a global scale, it has been found that reducing the piracy rate for PC software by 10 percentage points in four years would create \$142 billion in new economic activity worldwide, while adding nearly 500,000 new high-tech jobs and generating roughly \$32 billion in new tax revenues.⁷

Software theft further hinders job growth throughout the economy – not in the software or IT sector alone. 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

⁶ Seventh Annual BSA and IDC Global Software Piracy Study (May 2010), available online at <http://www.bsa.org/globalstudy> (hereinafter "2010 Piracy Study"). The study methodology is described on pages 14-17 of the study. The Eighth Annual BSA and IDC Global Piracy Study (covering 2010) will be published next year.

⁷ Piracy Impact Study: the Economic Benefits of Reducing Software Piracy, BSA and IDC, (October 2010), available online at <http://portal.bsa.org/piracyimpact2010/studies/piracyimpactstudy2010.pdf>. The study methodology is described on pages 10-11 of the study.

competitive advantage over an enterprise that respects the law and acquires legal software. 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.

Part II: Responses to Questions Posed in Notice of Inquiry

Category 1: Right holders: Protection and Detection Strategies for Online Infringement

What are stakeholders' experiences and what data collection has occurred related to trends in the technologies used to engage in online copyright piracy, and what is the prevalence of such piracy?

In its efforts against software piracy of all types, BSA regularly monitors the serious and growing problem of online piracy. In 2009, for example, BSA sent more than 7.3 million takedown notices worldwide to Internet service providers, related to peer-to-peer file sharing. BSA also requested the removal of almost 153,000 torrent files containing member company software from just nine BitTorrent index sites. Nearly 4 million individuals had used those files to download software worth more than \$2.2 billion.⁸

The ever-expanding and rapidly evolving Internet poses particular challenges for tracking the incidence of piracy. Even as the problem of peer-to-peer file sharing continues, BSA has noted an increasing incidence of piracy involving one-click file sharing hosts. As new technologies arise, they often allow new ways of sharing pirated products. As a consequence, the Internet is a constantly developing field where right holders must continually adapt their approaches to fighting infringement of their products.

⁸ The retail value of the software is computed by multiplying the number of downloaders by the MSRP value of the products involved.

What new studies have been conducted or are in-process to estimate the economic effects of this piracy? What assumptions are made in such studies on the substitution rates among the different forms of content?

BSA regularly commissions IDC to carry out two studies that seek to measure the effects of software theft. Annually, we release our Global Software Piracy Study, which estimates the rate of PC software piracy and commercial value of pirated software in 111 markets around the world. The most recent version of this study found that the rate of global software piracy climbed to 43 percent in 2009. The commercial value of that software theft exceeded \$50 billion.

Every other year, we release our Piracy Impact Study, which estimates the economic benefits that could be achieved in 42 countries by reducing the piracy rate by 10 percentage points over four years. The most recent version of this study found that reducing the piracy rate for PC software by 10 percentage points — 2.5 points per year for four years — would create \$142 billion in new economic activity while adding nearly 500,000 new high-tech jobs and generating roughly \$32 billion in new tax revenues by 2013.

The methodology for each of these studies is disclosed in the respective studies, which are available on BSA's website.

What technologies are currently used to detect or prevent online infringement and how effective are these technologies?

BSA uses an array of technologies to detect instances of online infringement, including search and monitoring technologies. BSA also works directly with auction sites to develop a standard for self-compliance and more streamlined infringement identification systems. In the peer-to-peer context, BSA has developed proprietary and third-party applications to identify infringements. Once infringing files have been detected, BSA generates notifications of claimed infringement that are transmitted electronically to ISPs.

In many cases BSA members use technological means to make their works more difficult to infringe, whether online or within an office. Most

recently, some BSA companies have deployed “product activation” technology to protect their works. This technology uses a unique serial number that identifies a particular copy of a computer program, and generates a number that is derived from the configuration of the computer on which the program is installed. These are combined into an “installation ID” that is transmitted to an activation server that, in turn, provides an authorization code to the software if the copy has not already been activated on another machine. Each time the software is launched the machine configuration is compared with the installation ID. If the configuration is significantly different (suggesting that the software has been installed on another computer) the software must be reauthorized.

Product activation is the most recent technological measure used by the software industry. Over the relatively brief history of our industry, we have employed a number of techniques, including copy protection, dongles (hardware locks), passwords and serial numbers. In each instance, software developers have had to balance the robustness and efficacy of the technology in preventing piracy against ease of use and customer acceptance.

The effectiveness of our efforts to reduce online piracy is, in part, dependent on the adequacy of national copyright laws and enforcement regimes in countries around the world. For example, not all countries have laws against disabling technological measures such as product activation systems. Rules regarding removal of infringing online content vary from one country to another. For BSA, those varying legal systems require similarly varying procedures to satisfy the requirements needed to provide notice to secure a takedown or otherwise limit the availability of pirated material.

In addition, battling online piracy requires a continual research and development effort in order to understand how the piracy problem takes place in a particular distribution channel, how to collect and interpret the relevant information, and how to effectively move against pirated online material.

It is sometimes asserted that, because technology has contributed to new “innovations” in piracy, technology must be deployed to solve the

problem. Certainly, technology can play a role in helping to curb piracy and industries have looked to such solutions in appropriate circumstances.

BSA members believe strongly that broad, government-imposed technology mandates should be avoided. Recently, 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.⁹ 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 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

⁹ For example, 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.

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.

What observations, if any, have been made as to patterns of online infringement as broadband Internet access has become more available?

Expanding our national broadband network is a high national priority, and BSA members believe that it is indispensable to our economic vitality. According to OECD data, the United States ranks eleventh in broadband penetration behind countries such as Korea, Canada and Iceland. The benefits of the Internet to all aspects of our lives are well documented, from education to health care, from distance learning to managing our finances. Broadband as such, like multipurpose computers, smart phones and software, is in the vast majority of cases used for legitimate and economically important purposes. As with these other technology tools, some bad actors intent on infringement use broadband to steal others' property. Broadband technology itself is no more the cause of piracy than roads are the cause of reckless driving.

As broadband capacity grows, nations should work to ensure that the right legal infrastructure exists to promote its use for education, improving public information and services, and for increasing productivity. A sound base of laws, including respect for IP in the digital and Internet environments must be part of ensuring that countries gain the full benefits of broadband.

Is litigation an effective option for preventing Internet piracy?

Civil litigation is an important option for right holders. Civil litigation permits right holders to bring their resources to bear against infringers in

ways that are more expeditious than criminal law enforcement actions permit. Civil actions are also amenable to early settlement, limiting the use of precious judicial resources. As part of a final judgment or settlement, the counterfeiters can be put under a permanent injunction prohibiting further piracy and can be required to destroy all infringing goods.

Criminal action against software pirates also is an essential element of an effective enforcement regime. Law enforcement can send the deterrent message to the public with a unique strength. Civil litigation and judgments send an important enforcement message, but the prospect of the range of criminal sanctions – including fines and jail time – sends an exponentially stronger, deterrent message to potential pirates.

BSA has a long history of working closely with law enforcement, developing leads for investigation by the Federal Bureau of Investigation or US Immigration and Customs Enforcement. BSA has also long provided support to active investigations by developing data needed by the case agent or assisting with authentication issues.

Consistent with free speech, due process, antitrust, and privacy concerns, what incentives could encourage use of detection technologies by online services providers, as well as assistance from payment service providers, to curb online copyright infringement?

The most effective incentive against the proliferation of online piracy is a limitation on remedies against ISPs that is conditioned on the ISP cooperating to remove infringing material. Current law adequately embodies this incentive in section 512 of the Digital Millennium Copyright Act (DMCA).

For infringing material that is not hosted on a service provider's system, terms of service agreements should be more effectively enforced to prevent the use of such service for illegal purposes. Rather than create new statutory obligations, the related industries should come together on a voluntary basis to reach agreements designed to encourage such solutions where circumstances warrant.

We note that there has been a great deal of discussion about the asserted need for “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 the graduated response umbrella, as a general matter such legislation would mandate, at least, that ISPs take a series of steps in response to allegations of copyright infringement, ultimately leading to sanctions against persons who are deemed repeat infringers.

We support taking action against repeat offenders in the United States and abroad. But we have learned from similar efforts in France and elsewhere that it is very challenging to find a legislative approach that effectively deters online piracy while respecting the very aspects of the law that the Department’s question rightly suggests must be accommodated 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, and managing one’s health care. 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 with two objectives: effectively deterring the illicit downloading, uploading, making available and use of content; and, ensuring that existing technologies function as design, 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.¹⁰

What challenges have the creative industries experienced in developing new business models to offer content online and, in

¹⁰ 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> (copy attached).

the process, to counteract infringing Internet downloads and streaming?

The problem with software piracy is not related to industry's online business models. Software is regularly licensed, sold and updated online in a legal manner. The software industry's business models work successfully both online and off-line. Digital piracy, however, damages both models.

Can commenters make any generalizations about the online business models that are most likely to succeed in the 21st century, as well as the technological and policy decisions that might help creators earn a return for their efforts? (Again, keeping in mind free speech, due process and privacy concerns.)

The most successful business models in the 21st century will build on the most successful business models of today. To succeed, companies will need to provide what customers want, in easy-to-use forms, and at fair prices. In the software industry, cloud computing will be a great source of innovation, offering customers the potential for tremendous increases in efficiency, cost savings, scalability and increased performance.

How can government policy or intellectual property laws promote successful, legitimate business models and discourage infringement-driven models?

The key to promoting successful, legitimate online business models and discouraging infringement-driven models is encouraging cooperation between ISPs and content owners. Done on a voluntary basis, such a cooperative effort can produce business relationships that benefit all sides. The current legal structure works reasonably well.

And, how can these policies advance these goals while respecting the myriad legitimate ways to exchange non-copyrighted information (or the fair use of copyrighted works) on the Internet?

The vast majority of information that is retrieved, used, distributed and communicated over the Internet every day does not violate any laws or policies. As we noted above, the illegal act, whether fraud, malware distribution or piracy is done by a very small number of bad actors. In the

vast majority of situations when copies are pirated, the entire copy of the work is taken and used in direct competition with the genuine product. Fair use and other doctrines that aim to preserve important public policy interests are almost never implicated in these circumstances. In those instances where a small portion of a work is taken for criticism, teaching or other worthwhile purposes, the US Copyright Act, and the case law interpreting it, provide ample guidance. That law has evolved over time to encourage creative and truly transformative uses in ways that serve our country well, providing clarity to right holders and defenses to those engaged in acts that advance the public interest.

Fair use is, by design, a defense to infringement, not a right unto itself. But it is nonetheless an essential part of the Constitutional balance underpinning U.S. copyright law. To ensure fair use remains a vibrant source for promoting creativity, we believe it is essential that the defense be available online as in physical environments and that accused infringers have a full and fair opportunity to rebut claims of infringement based on the specific facts of the circumstance where the claim of infringement arises.

Category 2: Internet Intermediaries: Safe Harbors and Responsibilities

What processes are employed by rights holders to identify infringers for purposes of sending takedown notices?

BSA's process for identifying infringers varies based on the particular avenue of infringement – peer-to-peer, online marketplace, one-click file sharing host – but the steps that lead to the sending of a takedown notice are consistent across each. First, BSA accesses the varying online venues; we collect and analyze the relevant data; and we follow that analysis with a determination of action.

For the purposes of identifying infringers, BSA takes advantage of all available technologies across the different channels of infringement. For example, in the peer-to-peer context, BSA uses both third-party and proprietary applications to identify infringements. To locate infringing torrent files, BSA uses searching algorithms, scraping technologies and even direct search of hosting sites. These efforts are further coupled with

manual reviews of the material collected in order to refine and enhance searches.

The continuing evolution of piracy also requires ongoing research and development to understand how distribution of pirated material takes place and how to collect and interpret new information in order to effectively pursue takedown notices.

Are Internet intermediaries' responses to takedown notices sufficiently timely to limit the damage caused by infringement?

In the case of digital piracy, a timely response to a takedown notice is important. The amount of time it takes to copy a pirated product using BitTorrent feeds or from a one-click file host is very short, and each available link represents thousands of potential thefts. The longer that a pirated product is available online, the more likely the product can be found and used or stolen. Unfortunately, the time it takes for intermediaries to take action in response to a takedown notice varies widely. Sharing best practices in this area would be useful to promote efficient processes.

What are stakeholders' experiences with online copyright infringement by users who change URLs, ISPs, locations, and/or equipment to avoid detection?

Digital pirates frequently change URLs or ISPs to avoid detection. In fact, BSA has known web sites that provide pirated material to switch ISPs through different companies and countries, in some cases even cycling back and ending up at the same ISP they had earlier used. Individuals and organizations also often gravitate toward countries that lack a legal framework to support the enforcement of takedown notices.

What challenges exist to the identification of such systematic infringers?

Right holders typically do not know the true identities of Internet users and website owners. This is information that is generally held by ISPs. The DMCA (section 512(h)) provides a mechanism by which right holders can obtain this information from ISPs, but at least one court has held that the mechanism is available only with respect to people who are using ISPs

to host infringing material. In the case of material that is not hosted by an ISP (e.g., material on a subscriber's own computer that is made available through a P2P network), a right holder must commence a lawsuit before a subpoena can issue requiring the ISP to identify the alleged infringer.

Identifying domain name registrants presents other challenges. In theory, right holders can identify domain name registrants using a WHOIS lookup, but WHOIS data are notoriously incomplete, particularly when the domain is registered through a proxy.

Finally, with respect to repeat or systematic infringers, it is not apparent that ISPs retain the records that would be needed to do an effective job of tracking them.

What are stakeholders' experiences with Section 512(i) on the establishment of policies by online service providers to inform subscribers of service termination for repeat infringement?

In order to take advantage of the limits on liability in the DMCA, Section 512(i) requires service providers to adopt, reasonably implement, and inform customers of, "a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

What other collaborative approaches should stakeholders consider? How can government best encourage collaborative approaches within the private sector?

BSA believes that a voluntary, industry-led approach will provide the most effective solutions to the shortcomings in the current system. New law or policies would neither effectively address the problems at hand nor allow for the necessary rapid evolution of technology and business practices needed to respond to digital piracy.

Category 3: Internet Users: Consumers of Online Works and User-Generated Content

What initiatives have been undertaken to improve the general awareness of Internet users about online copyright infringement

and the availability of legitimate sources to access online copyrighted works?

BSA issues reports and other advisories designed to increase public awareness of the dangers of online copyright infringement. "Online Software Scams: A Threat to Your Security" was released in October 2008, and "Software Piracy on the Internet: A Threat to Your Security" was released in October 2009.¹¹ BSA also issues media advisories highlighting legal developments and enforcement actions by the Department of Justice against entities that use the Internet to distribute pirated software.

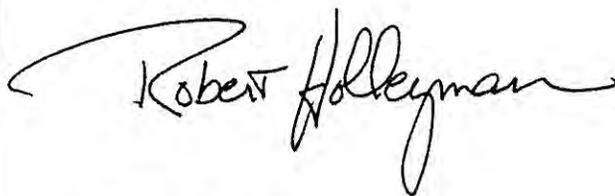
In addition, BSA has dedicated a section of its website to "Faces of Internet Piracy,"¹² which tells the stories of individuals engaged in and harmed by software piracy.

What are stakeholders' experiences in foreign countries and on university campuses in reducing online copyright infringement?

Based on the network capacity and security issues connected with piracy, universities have been responsive in efforts to reduce online copyright infringement.

In the international arena, BSA increasingly sees infringers moving to countries with ineffective IP enforcement systems and no legal framework to support the enforcement of takedown notices.

Sincerely,

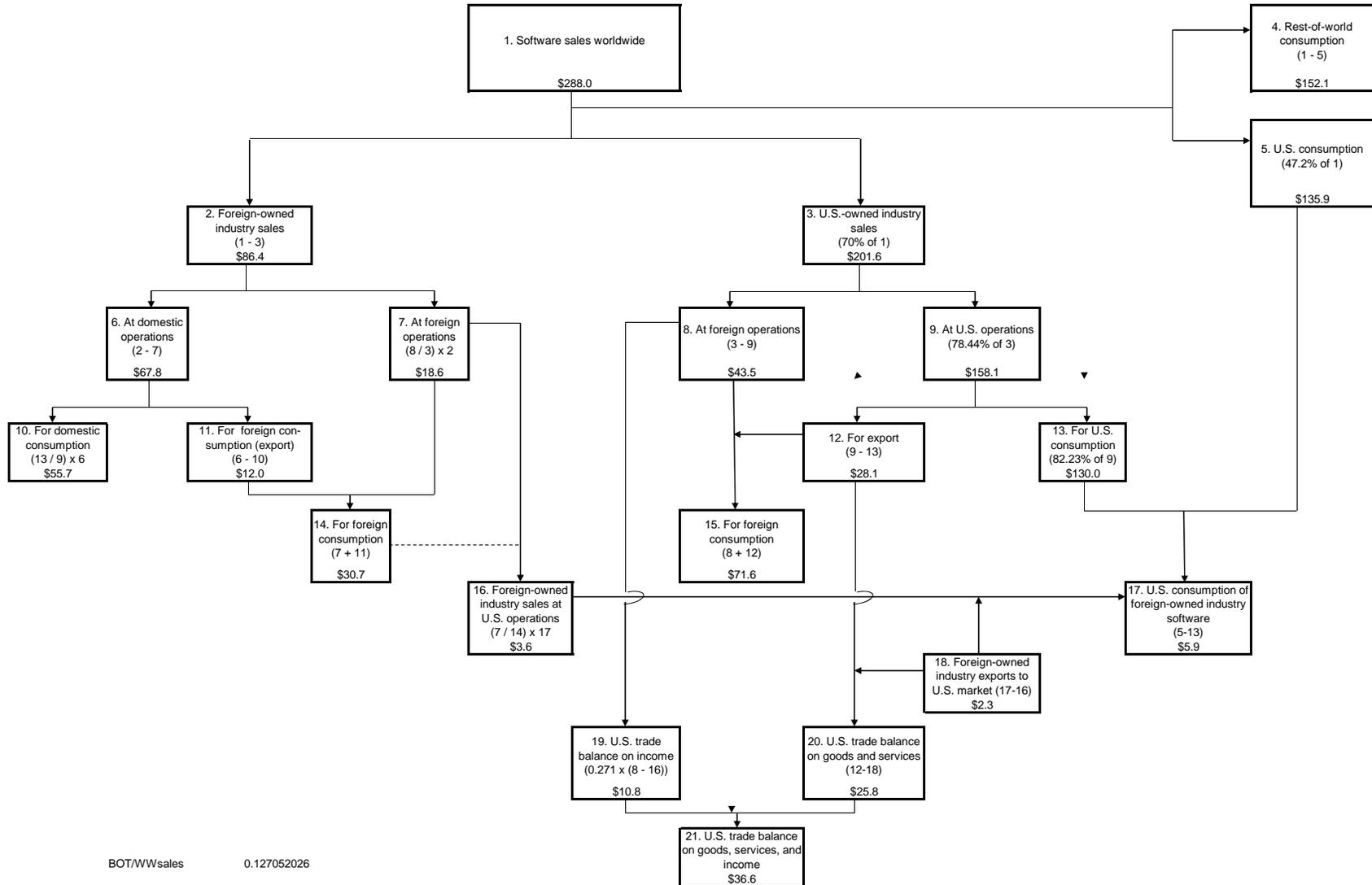


Robert W. Holleyman, II
President and CEO

¹¹ Copies of each report are attached to this document.

¹² The related material can be found at www.bsa.org/faces.

Derivation of the Contribution of the U.S.-Owned Software Industry to the U.S. Balance of Trade on Goods, Services, and Income in 2009 (US\$billion)



BOT/WWsales 0.127052026

Note: Trade balance on income is 27.1 percent of sales at foreign operations.

Sources: Nathan Associates Inc. Software sales worldwide and U.S. consumption share were reported by IDC. U.S.-owned industry share of worldwide sales was reported by the Software and Information Industry Association (SIAA).



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.



A REPORT BY THE
BUSINESS SOFTWARE ALLIANCE
OCTOBER 2008



Online Software Scams: A Threat To Your Security





Contents

- Introduction 3
- The Many Forms of Software Internet Piracy..... 5
- The Risks to Consumers..... 7
- A Closer Look at Auction Site Piracy 9
- Investigations of P2P, Website, and Auction Site Piracy..... 12
- Enforcement Action 13
- BSA Partnerships and Educational Outreach..... 16
- Auction Sites Must Do More to Protect Consumers 18
- What Consumers Can Do to Protect Themselves..... 19
- How to Report Suspected Piracy and Fraud..... 20
- Conclusion 21

Charts and Illustrations

- Software Piracy Sites Also Spread Malware 8
- Top Ten Software Publishers with Products Available on eBay..... 9
- eBay: Test Purchases of Software..... 10
- Number of Online Auction Sites Removed due to BSA Requests..... 11
- Top Ten Countries for Auction Site Piracy Takedowns, 1st Half 2008..... 11





Introduction

An employee of Wagner Resource Group of McLean, Virginia, decided to use his office computer to download music and video files from the Internet using the popular LimeWire peer-to-peer program. Unfortunately, LimeWire is one of many such programs used to exchange pirated copies of music, video, and software, and those often-tainted files can then help cyber criminals accomplish even further misdeeds. In this case, the Wagner employee's action set off a terrible chain reaction, opening up the firm's computers to outsiders and exposing the names, dates of birth, and Social Security numbers of about 2,000 of the firm's clients, including US Supreme Court Justice Stephen Breyer. The company hired by Wagner to help contain the data breach said it found more than a dozen LimeWire users in places as far away as Sri Lanka and Colombia had downloaded the list of personal data from the Wagner network. "This may explain why two weeks ago I got a \$9,000 cell phone bill from AT&T," said one of the firm's clients.¹

A consumer in Texas bought a software product online for a deeply discounted price. But when he

received the CD in the mail, he immediately realized there was a problem. "To get the serial number to activate the product, I had to use the keygen.exe software included on the disk," he said. The consumer did some research online and discovered that the keygen.exe application is used to generate CD keys or serial numbers required for software installation or activation. Keygens are available on the Internet and are often packaged with software for distribution by piracy groups. The use of keygens to activate software without purchasing a genuine code is illegal.²

On any given day, nearly 1.5 billion people around the world—one in four human beings—may go online to communicate with friends, family, and business associates; shop for a great deal; do research for school; or seek out entertainment. The global number of Internet users grew by more than 300% from 2000 to 2008.³

However, there is a darker side to the Internet when it comes to online scams that snare consumers

ALTHOUGH CONSUMERS MAY THINK THEY ARE GETTING A GREAT DEAL WHEN THEY BUY SOFTWARE FROM UNFAMILIAR SOURCES ONLINE, IT IS MORE LIKELY THEY WILL RECEIVE A SUBSTANDARD PRODUCT WITH HIDDEN CYBER SECURITY THREATS THAT MAY EXPOSE THEM TO IDENTITY THEFT AND THE LOSS OF THOUSANDS OF DOLLARS.

attracted by low-priced deals. One of the most widespread online scams involves stolen or unlicensed software programs, i.e., pirated software, offered at discounted prices. Although consumers may think they are getting a great deal, it is more likely they will receive a substandard product with hidden cyber security threats that may expose them to identity theft and the loss of thousands of dollars. As described below, software piracy is conducted via numerous channels in the online world; however, piracy on online auction sites such as eBay is challenging.

Pirated software can also enmesh the unwitting consumer in further criminal activity, as the consumers' computer is effectively converted into a "robot" and exploited remotely by the cyber criminal. Cyber crime is increasingly perpetrated by organized crime syndicates located around the world. "Cyber crime today isn't about computer geeks just having fun at other people's expense," says Rob Clyde, vice president for technology at Symantec. "It's real criminals making real money off of real victims. And it gets more serious by the day."⁴

The widespread theft and distribution of bogus software is also evidence that the value of intellectual property (IP) is under attack around the world. Far too many people are careless in how they handle software and computers, instead of respecting the value and effort that went into them or the dangers of abusing them. Some people behave

as though the copying and theft of IP is a victimless crime or that the creators of works such as software, music, films, and books can be stolen from without consequences. People who would not dream of shoplifting a music CD or a package of software from a store will go online to seek out copies of plainly illegal software.

Worldwide, more than one-third of all software installed on personal computers is obtained illegally, with foregone revenues to the software industry totaling nearly \$48 billion, monies that could have been invested in new jobs and next-generation solutions to society's needs. The ripple effects also include tax revenues not paid to support community services such as police protection and new schools. A 2008 study found that reducing software piracy in the United States alone by just 10 percentage points over the next four years could generate more than 32,000 new jobs, \$41 billion in economic growth, and \$7 billion in tax revenues above current projections.⁵

The Business Software Alliance (BSA) has spent more than twenty years defending the value of intellectual property and pursuing software pirates. Over the past decade, this mission has expanded to include cracking down on those who offer illegal software via peer-to-peer (P2P) networks, auction sites, and other kinds of Internet-based channels. The following report describes the scope and nature of the Internet piracy problem, as well as steps that are needed to reduce it, with a special emphasis on auction site scams.

The Many Forms of Software Internet Piracy

Before the rise of the Internet, unauthorized copying of software generally required the physical exchange of disks or other hard media through the mail or on the streets. But as high-speed Internet connections have spread around the world, software piracy has moved from the streets to the Internet.

Generally, Internet piracy refers to the use of the Internet to:

- Provide access to downloadable copies of pirated software;
- Advertise and market pirated software that is delivered through the mail; or
- Offer and transmit codes or other technologies to circumvent anti-copying security features.

The process can be as roundabout as any other illegal activity. Buyers may be directed to one website to select and pay for a software program, and then receive instructions to go to another website to download the product. This circuitous process makes the pirate less vulnerable to detection.

Internet-based software scams can occur through numerous channels:

AUCTION SITES: Online auction sites are among the most popular destinations on the web, with millions of people logging on to buy and sell a vast array of products. The best known auction sites are eBay, UBid, Mercadolibre in Latin America, Taobao in China, and QXL in Europe. Yahoo! operates heavily

used sites in Hong Kong and Taiwan. While many legitimate products are sold on auction sites they are also subject to abuse, especially when it comes to software sales (see more details below).

PEER-TO-PEER (P2P): Peer-to-peer technology connects individual computer users to each other directly, without a central point of management. To access a P2P network, users download and install a P2P client application. Millions of individuals have P2P programs installed on their computers, enabling them to search for files on each other's computers and download the files they want, including software, music, movies, and television programs. Popular P2P networks include BitTorrent, eDonkey, Gnutella, and FastTrack. P2P applications include BitTorrent, eMule, Kazaa, BearShare, and Limewire. In Europe, the Middle East, and Australia, P2P traffic consumes anywhere between 49% and 89% of all Internet traffic in the day. At night, it can spike up to an astonishing 95%.⁶

OTHER WEBSITES: Some Internet software scams are conducted via websites that offer advertising, such as Craigslist, Google, and Yahoo!. iOffer.com describes itself as an online "trading community" without auctions or listing fees. Other scams occur via file-hosting sites such as RapidShare, where users can upload their content, receive a web link for it, and then provide that link to others via direct e-mails or ads on other websites. Finding and stopping software piracy on such websites is becoming more difficult as the number of Internet domain names and websites

PEER-TO-PEER (P2P) TECHNOLOGY IS WIDELY USED FOR PIRACY OF INTELLECTUAL PROPERTY. IN SOME PARTS OF THE WORLD, P2P TRAFFIC CONSUMES BETWEEN 49% AND 89% OF ALL INTERNET TRAFFIC DURING THE DAY, AND UP TO 95% AT NIGHT.

based overseas proliferates. Some Internet observers have proposed allowing domain name registrars to block information about who controls the sites, which would make it more difficult to protect consumers from fraud.

BOTNETS: Botnets illustrate how the worlds of software piracy and cyber crime are merging. They are both a contributor to software piracy and one of its most alarming side effects. In simple terms, “bot” is short for robot, a piece of software code programmed to conduct repetitive tasks. In the cyber crime context, cyber criminals and/or their accomplices (“bot herders”) send out “bots” through various techniques, including e-mail spam and malicious code (“malware”) added to pirated software. The bots and malware infect ordinary consumers’ computers, which then become remotely controlled “zombies.” The compromised “zombie” computers can then be tied together in a “botnet”

and exploited remotely by the cyber criminals to carry out a variety of illegal activities, including hosting files used for additional piracy. According to the FBI, more than 1 million computers have become ensnared in botnets.⁷ “And the owners often have no idea that it’s happening,” says Dave Marcus, security research and communications manager with McAfee Avert Labs.

OLDER FORMS OF INTERNET PIRACY: Several older forms of Internet-based piracy are still seen but have been largely supplanted by the more efficient techniques described above. These techniques include Internet Relay Chat (IRC), which are locations on the Internet for real-time, multi-user, interactive conversations; File Transfer Protocol (FTP), a standard computer language that allows disparate computers to exchange and store files quickly and easily; and newsgroups, established Internet discussion groups that operate like a public e-mail inbox.

The Risks to Consumers

Internet commerce is essentially unrestricted, self-regulated, and anonymous. Consumers should proceed with caution when purchasing and using software from unknown vendors online. Using illegal software can put one's personal information, reputation, and financial security at risk. At the very least, it can lead to software incompatibility and viruses, drive up maintenance costs, and leave users without technical support and security updates. At worst, it can cost ordinary consumers hundreds or thousands of dollars and lost time due to identity theft and the exposure of personal information.

“WHEN SOMEONE CAME TO OUR SITE, THEY WOULD MAKE THEIR PURCHASES ONLINE, WITH EITHER A CREDIT CARD OR A DEBIT CARD, WHICH MEANS THAT NOW, THE PERSON YOU ARE BUYING PIRATED SOFTWARE FROM HAS YOUR CREDIT CARD OR DEBIT INFORMATION.”

— **DANNY FERRER**, A CONVICTED SOFTWARE PIRATE WHO IS CURRENTLY SERVING A SIX-YEAR JAIL SENTENCE.

The statistics on risks to consumers are ominous. According to a survey conducted by Forrester Research on behalf of BSA, one in five U.S. consumers who purchased software online in 2006 experienced problems. Of those who had problems:

- 53% received software that was not what they had ordered;
- 36% reported that the software did not work;
- 14% immediately realized the software was pirated; and
- 12% never received the product.⁸

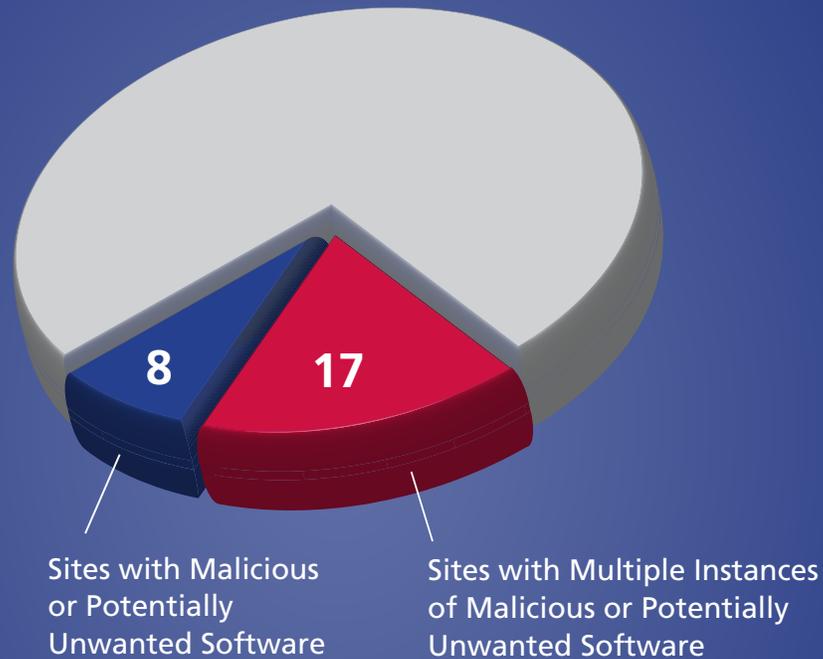
The risks to consumers also include:

- Not receiving upgrades, technical support, manuals or documentation;
- Receiving an incomplete, altered, or trial version of the software;
- Allowing criminals access to sensitive personal and financial information; and
- Infecting the consumer's computer with viruses or tools for remote-controlled cyber crime.

A 2006 report by the IDC research firm revealed that 25% of websites offering access to pirated software and piracy-related tools were distributing malicious code that could undermine IT security and performance. In some cases, the websites exploited vulnerabilities in the users' computers to install the unwanted software automatically.⁹

SOFTWARE PIRACY WEBSITES* ALSO SPREAD MALWARE

SAMPLE OF 98 UNIQUE WEBSITES



* SITES OFFER ACCESS TO PIRATED SOFTWARE AND PIRACY-RELATED TOOLS.
SOURCE: IDC STUDY, RISKS OF OBTAINING AND USING PIRATED SOFTWARE, 2006

A Closer Look at Auction Site Piracy

Of the various types of Internet-based piracy, auction site piracy is the most devious because it involves actual sales of software to consumers, as opposed to the other types of piracy that distribute free copies of software to people experienced enough to navigate P2P programs and other esoteric Internet channels.

No software titles are exempt from the threat of auction site piracy. A search of popular auction sites for the best-selling titles produces thousands of results, many with "Buy It Now" options.

While no one has quantified the scope of auction site piracy with a high degree of confidence, estimates have pegged the problem in the range of 50% to 90%. For example, in one 2005 study involving test purchases of more than 115 copies of software purchased from eBay, 39% were counterfeit and 12% came with additional software components that were counterfeit or genuine software that had been tampered with. This data indicated that there was a less than one-in-two chance of buying genuine, licensed software from eBay that had not been tampered with.¹⁰

Some auction sites provide limited safeguards such as tips for consumers, comments on sellers posted by other site users, and/or Spoof website protection, which is a toolbar that helps alert users when they are on fraudulent sites. But generally speaking, auction site owners disclaim responsibility for the legitimacy of any products sold or transactions made on their sites.

TOP TEN SOFTWARE PUBLISHERS* WITH MOST PRODUCTS AVAILABLE ON eBay

1. Microsoft
2. Adobe
3. Apple
4. Corel
5. Symantec
6. McAfee
7. Borland
8. Autodesk
9. Solidworks
10. CNC



*AS OF JULY 31, 2008. BSA MEMBERS ONLY.

In the absence of any action by the auction sites themselves to stop software piracy, it is safe to assume the practice will spread as more people around the world go online every day and learn how to buy and sell items on the growing number of auction sites. In short, auction site piracy is unlikely to disappear altogether and is more likely to resemble the carnival "Whack-a-mole" game, disappearing here and reappearing there as software pirates work to evade watchful eyes.

CASE STUDY: eBay

As the world's leading online marketplace, eBay has an interest in ensuring that its online trading platform is trusted. In 2007, eBay had approximately eighty-four million active users worldwide, who traded more than \$60 billion worth of goods. Unfortunately, the site is subject to abuse, as noted by *The New York Times*, which called eBay "the center of a new universe of counterfeit with virtually no policing."¹

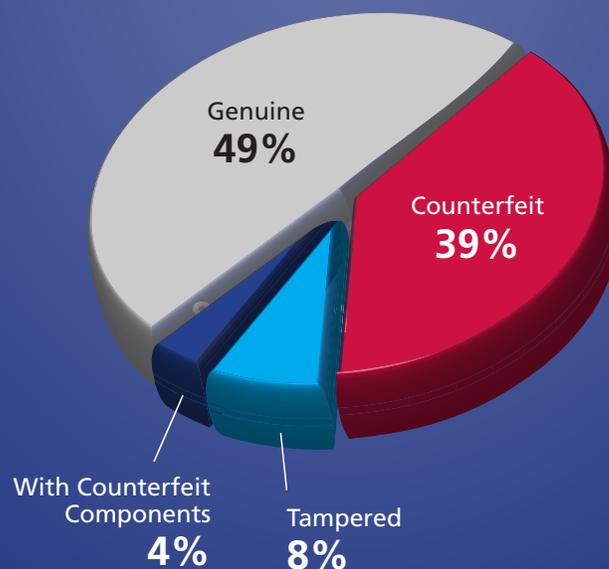
BSA has worked with eBay to fight software piracy for approximately ten years, and eBay has taken a number of steps to combat piracy. For example, eBay prohibits the sale of Original Equipment Manufacturer (OEM) or "bundled" copies of software—software obtained as part of the purchase

of a new computer—unless the seller provides it along with the original computer hardware. But eBay does not actually police the listings on its site, and it disclaims any responsibility for doing so.

In another step, eBay created the Verified Rights Owner (VeRO) Program, giving intellectual property owners an avenue for reporting eBay listings that infringe upon their rights. Based upon information provided by rights holders, eBay investigates instances of possible piracy and may remove listings that violate VeRO policies. However, the system still leaves the primary burden of monitoring listings on the rights holders. It is not designed to protect consumers—and its benefits to consumers are limited.

1. "Seeing Fakes, Angry Traders Confront eBay," Katie Hafner, *New York Times*, January 29, 2006.

eBAY: TEST PURCHASES OF SOFTWARE SAMPLE OF 115



SOURCE: MICROSOFT LEGAL AND COMPLIANCE TEAM, 2006, CITED IN "THE RISKS OF OBTAINING AND USING PIRATED SOFTWARE," IDC, OCTOBER 2006. TAMPERED INCLUDES BOTH GENUINE SOFTWARE WITH COUNTERFEIT COMPONENTS AND GENUINE SOFTWARE THAT HAS BEEN TAMPERED WITH.

CASE STUDY: **iOffer**

iOffer was launched in 2001 as an alternative to eBay and other highly competitive auction sites. Unfortunately, it has not been immune to the activities of software pirates, and it also disclaims responsibility for the legitimacy of online transactions conducted on its platform.

In response to concerns about piracy, iOffer established C.O.P.S., the Counter Online Piracy System, which allows verified copyright owners to remove and/or disable access to items that may infringe upon their copyright.

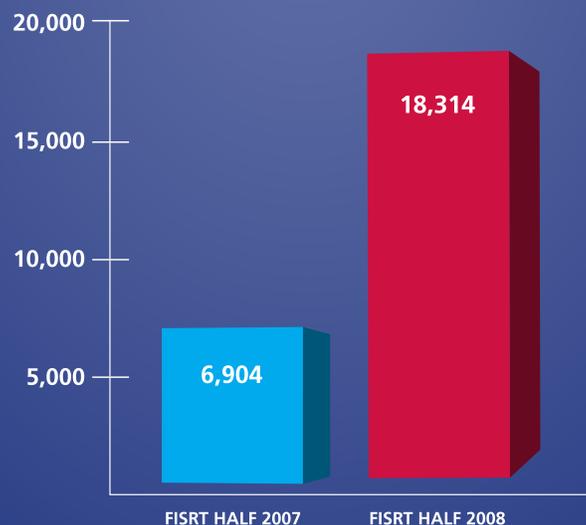
BSA has recently added iOffer to the list of websites that it monitors for illegitimate software transactions and possible takedown notices.

TOP TEN COUNTRIES FOR AUCTION SITE PIRACY TAKEDOWN REQUESTS, FIRST HALF OF 2008



SOURCE: BUSINESS SOFTWARE ALLIANCE

NUMBER OF ONLINE SOFTWARE AUCTIONS REMOVED DUE TO BSA REQUESTS



BSA has expanded its ability to request takedowns of suspicious online software auctions. Removals jumped 265% from 2007 to 2008.

SOURCE: BSA DATA

Investigations of P2P, Website, and Auction Site Piracy

The software industry has worked to combat Internet-based software scams for more than a decade. The centerpiece of BSA's efforts is the Online Auction Tracking System (OATS), a proprietary tool that monitors auction sites and BitTorrent networks (described above) on a continuous basis, while another tool monitors other P2P activity. These systems identify thousands of cases of suspicious activity each day in countries where scanning is permitted by law. BSA then analyzes each case to determine whether it merits further action.

Once BSA has identified offerings of illegal software via various websites and P2P networks, it may issue "takedown" notices to the Internet Service Providers (ISPs), asking them to remove the pirated software. In the first half of 2007, BSA sent 471,694 non-BitTorrent takedown notices to ISPs. In the first half of 2008, BSA stepped up its efforts and issued 782,832 such takedown notices.

In 2007, BSA launched an in-house Internet "crawler" to strike further up the BitTorrent supply chain, in addition to the notices sent at the "demand" level

where permitted by law. In the first half of 2008, BSA issued more than 48,000 notices related to BitTorrent files that were being used by 633,000 people to download BSA member software worth an estimated \$525 million.

When BSA finds suspicious software being offered on auction sites, it issues takedown requests to the auction site providers to remove those listings. In 2007, BSA requested that auction site providers shut down more than 13,800 online auctions that were offering more than 50,500 individual software products with a total retail value of more than \$13.3 million. Nearly two-thirds of the auctions shut down were on US auction sites. During the first half of 2008, BSA has expanded this effort, and requested auction site providers to shut down 18,314 auctions offering 45,000 products worth a combined \$22 million.

As the chart on page 11 indicates, the number of auctions removed in the first half of 2008 increased by nearly three-fold compared to the same period in 2007, reflecting BSA's increased efforts to block auction site piracy.

Enforcement Action

When necessary and appropriate, BSA files civil lawsuits to try and stop Internet-based piracy, and sometimes it refers cases to the US Justice Department (DOJ) for criminal prosecution. Such cases may bring about very serious consequences. Federally prosecuted copyright infringement cases can result in fines of up to \$250,000, and in some cases, jail time.

Over the past decade, BSA, its member companies, and others have provided significant assistance to the Justice Department on hundreds of prosecutions of criminals who were operating for-profit and not-for-profit online software scams. Several of these cases resulted in prison sentences of between six and nine years and millions of dollars in restitution.

The following are highlights of several notable Internet piracy enforcement cases:

United States:

GEORGIA: In July 2008, a Savannah, Georgia, woman, was stopped from selling counterfeit copies of Corel software on eBay. A BSA investigation showed that she had sold more than \$212,000 worth of unlicensed software to hundreds of consumers from January to May 2008. A \$250,000 civil judgment was entered against her.

PENNSYLVANIA: Jon Crain of Coraopolis, Pennsylvania, operated nearly twenty websites distributing unlicensed copies of Adobe, McAfee, Microsoft, and Symantec software online. He was

first targeted by BSA in March 2007 as part of an international legal action against five software pirates. The other offenders were located in the United Kingdom, Austria, and Germany. In many of these cases, BSA was alerted to the illegal activity by reports or complaints from disappointed consumers who were initially attracted by low price deals. BSA sued Crain, and a civil judgment was entered that included a hefty settlement payment and a requirement to remove the unlicensed software from his website.

OREGON: In July 2008, Jeremiah Mondello, a 23-year Oregon man, was sentenced to four years in federal prison for selling more than \$1 million worth of pirated software and distributing malware via instant message networks to steal financial data from dozens of consumers. He then used the stolen bank account credentials to set up more than forty online auction accounts in the victims' names and withdraw money from their debit accounts. In addition to the prison sentence, federal investigators also seized computers and \$220,000 in cash from Mondello. The government also is entitled to seize his home and surrounding land.

CALIFORNIA: Nathan Peterson ran a Los Angeles-based, for-profit website called www.iBackups.net from which he sold illegal copies of software programs copyrighted by Adobe, Macromedia, Microsoft, Symantec, and others. An investigation conducted by the FBI, with support from BSA, determined that Peterson sold more than \$20 million worth of software and pocketed more than \$5.4 million.

The DOJ believed that Peterson was “the most prolific online commercial distributor of pirated software ever convicted in the US.” He was sentenced to a prison term of 87 months and ordered to pay \$5.4 million in restitution.

Asia Pacific:

TAIWAN: In October 2007, the Taiwanese police raided a large Internet pirate site called the XYZ Information Workshop in Kaohsiung and arrested a father and son engaged in piracy. The authorities seized 27 CD burners and more than 80,000 copies of illegal CD-Rs containing business software, games, music, and movies. The estimated retail value of the goods was more than \$30,000,000, and the pirates’ estimated daily revenue was \$3,000. BSA actively assisted the police in this case.

THAILAND: In April 2008, the Bangkok police raided the offices of www.idsoft.org, a website offering counterfeit software by mail. During the raid, the police arrested the 28-year-old pirate who had been operating the website and seized significant evidence including large quantities of supplies needed to make and mail copies of software, as well as 138 CDs containing Adobe, Autodesk, and Microsoft programs.

INDIA: BSA in 2007 carried out civil enforcement action against Hyderabad-based SM Technologies, leading to the seizure of pirated software worth approximately \$475,000.

A total of 1,843 CDs were recovered. This was the second time in three years that the same company was raided. In September 2004, BSA filed a criminal complaint against the company, leading to police raids at three locations in Hyderabad. SM Technologies was creating “compilation pirated CDs” with a range of products from Adobe, Autodesk, Microsoft, and Symantec, and selling the pirated software through multiple channels, including the Internet, resellers, and directly to end-users.

Europe, Middle East and Africa:

UKRAINE: In May 2006, a Ukrainian man, Maksym Vysochanskyy, was sentenced to 35 months in prison for his role in selling pirated copies of software from Adobe, Autodesk, Borland, and Microsoft through websites he operated and on eBay. The case was one of the first in the nation to involve an extradition in a prosecution for intellectual property offenses. Authorities from Canada, Lithuania, and Ukraine also took part in the investigation, and the Royal Thai Police collaborated in Vysochanskyy’s capture and extradition while he was on a trip there.

RUSSIA: In April 2008, the district court of Izhevsk imposed a criminal verdict on a Russian man who had created an FTP resource on his home computer to sell pirated copies of Adobe and Microsoft products worth more than \$15,000. The local police made several test purchases of software from Titov and matched them with the software on his PC.

CASE STUDY: **Danny Ferrer**

Video excerpts from an interview with Danny Ferrer can be viewed online at www.bsacybersafety.com/video.

After receiving a tip from BSA, an FBI investigation determined that from late 2002, Danny Ferrer of Lakeland, Florida, was operating for-profit websites selling illegal copies of software published by Adobe and Autodesk. Ferrer sold approximately \$20 million worth of copyrighted software products on www.BuysUSA.com at prices substantially below the suggested retail price. For example, software that had a retail value of more than \$600 was purchased by BSA from Ferrer for \$57. The software products purchased were reproduced on recordable CDs and distributed through the

mail. On the CD-R discs, Ferrer included labels that featured trademarks of the legitimate software companies and a serial number that allowed the purchaser to activate and use the product.

Ferrer made more than \$4.1 million from his operations, which was used to purchase luxury cars, airplanes, a helicopter, and boats. These items were all confiscated by the FBI, and Ferrer was sentenced in federal court to six years in prison. He also was ordered to pay more than \$4.1 million in restitution.

CASE STUDY: **The Robberson Brothers**

In early 2002, BSA began investigating Maurice A. Robberson and his brother, Thomas Robberson, after receiving complaints from software publishers. After reviewing the four reported websites, BSA made undercover purchases and determined that the software sold was pirated. BSA then referred the case to the FBI Washington Field Office, which conducted its own investigation and subsequently shut the operation down in October 2005.

The FBI investigation determined that from late 2002, the Robberson brothers sold more than \$5 million of counterfeit software products. In addition to running four for-profit websites, the Robberson brothers were also co-conspirators with Danny Ferrer in the operation of www.BuysUSA.com.

During the operation of the websites, Thomas Robberson grossed more than \$150,000 selling software with a retail value of nearly \$1 million. Maurice Robberson grossed more than \$855,000 selling software with a retail value of nearly \$5.6 million.

In March 2008, Maurice Robberson was sentenced to thirty-six months in prison, while his brother Thomas was sentenced to thirty months. Both were also ordered to undergo an additional three years of supervised release and pay restitution.

BSA Partnerships and Educational Outreach

Beyond enforcement actions, BSA also works with various organizations to gain a better understanding of Internet piracy and to educate the public about the risks of purchasing software from questionable Internet sources.

NATIONAL COMPUTER FORENSICS TRAINING ALLIANCE (NCFTA): In February 2005, BSA began a sponsorship of a dedicated cyber forensics analyst at the National Computer Forensics Training Alliance (NCFTA). The NCFTA provides a neutral collaborative venue where critical, confidential information about cyber crime—including software piracy—can be shared discreetly. It is also an environment where resources can be shared among industry, academia, and law enforcement. The partnership has provided BSA with valuable data on cyber security and software piracy.

NATIONAL INTELLECTUAL PROPERTY LAW ENFORCEMENT COORDINATION COUNCIL (NIPLECC): NIPLECC is an interagency group responsible for coordinating the United States' domestic and international intellectual property enforcement activities. Members include the director of US Patent and Trademark Office (USPTO); the Assistant Attorney General for the Criminal Division; the Undersecretary of State for Economics, Business and Agricultural Affairs; the Deputy United States Trade Representative; the Commissioner of Customs; and the Under Secretary of Commerce for International Trade. BSA is among

the industry associations that have appointed liaisons between their members and the US Commerce Department's Trade Compliance Center.

US IPR TRAINING COORDINATION GROUP: BSA works closely with the US State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) and Bureau of Economic, Energy and Business Affairs (EEB), which co-chair the Intellectual Property Rights Training Coordination Group (IPR TCG). Founded in 1998, the IPR TCG is comprised of US Government agencies and industry associations that provide education, training, and technical assistance to foreign officials and policymakers. The departments of Justice and Commerce, US Trade Representative (USTR), FBI, US Customs and Border Protection, US Patent and Trademark Office, US Agency for International Development, and Copyright Office all participate in the IPR TCG. Private sector partners include the International Intellectual Property Alliance (IIPA), US Chamber of Commerce, International Anti-Counterfeiting Coalition, and other industry organizations.

BETTER BUSINESS BUREAU: In 2003, BSA joined forces with the Council of Better Business Bureaus (CBBB) to educate consumers about the risks of purchasing software on auction sites. Together, the two organizations have reached an estimated six million consumers through outreach efforts including media tours, direct mail, television and radio advertising, and online initiatives.

“DON’T GET DUPED”: BSA’s “Don’t Get Duped” website offers consumers a forum to tell their stories about how they were duped into purchasing illegal software online. Over the past several years, nearly 400 consumers have written to BSA to share their experience. More than 150 complaints involved eBay.

For example, many consumers have complained about receiving software that was obviously pirated, oftentimes on obviously store-bought CD-Rs with handwritten titles, no registration keys, and no manuals. In one such case, a Texas consumer who paid \$155 on eBay for Adobe Photoshop CS—software that normally retails for about \$650—learned that the seller’s account was cancelled a few days later. After numerous e-mail complaints to the seller, which were not answered, he was instructed by eBay to wait ten days from the auction close and then file a complaint with PayPal. PayPal was able to contact the seller, and the man eventually received the software in the mail. But that was not the end of the story. “It was easy to tell it was pirated,” he said. “It was in a thin case with just a CD-R and only a handwritten note on the disc itself about what it was. When I opened the package and saw that it was pirated, I immediately e-mailed him requesting my money back.” The man never got his money back.

More stories about consumers who were duped are posted on BSA’s Cyber Safety website, www.bsacybersafety.com.

B4USURF: In Asia, BSA manages a cyber safety and ethics campaign (www.b4usurf.org) aimed at influencing youths aged ten to eighteen years old. The centerpiece of the initiative is a website with resources for educators, youths, and parents. For example, the site includes lesson plans and tips for teachers based on input from teachers in Singapore. Over time, BSA hopes to encourage education officials to incorporate Internet-focused ethics, security, and safety units in the curriculum of many nations. To date, the campaign has focused on Singapore, Malaysia, China, Taiwan, and the Philippines, with India, Hong Kong, and Thailand to be added later.

EDUCATIONAL VIDEO: To help individuals avoid purchasing fraudulent software online, BSA developed a brief educational video, “Software Piracy Exposed: A Dangerous Business for Buyers and Sellers.” The video educates consumers about safe online shopping while alerting potential sellers of the serious legal consequences of software piracy. The video includes interviews with Danny Ferrer, a convicted software pirate sentenced to six years in federal prison (see case study); a victim of online auction software fraud; a high-ranking Department of Justice official; a BSA spokesperson; and helpful tips on how to prevent against consumer fraud. The video is available for viewing at www.bsacybersafety.com.

The Larger Internet Crime Puzzle

Online software scams are one piece of the larger Internet crime puzzle. The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), receives Internet-related criminal complaints and refers cases to the appropriate local, state, federal, or international agency for possible investigation and prosecution.

In 2007, IC3 processed more than 219,553 complaints spanning the spectrum of Internet crime from auction site fraud, credit/debit card fraud, computer intrusions, unsolicited e-mail, and child pornography. From the submissions, IC3 referred 90,008 complaints to the appropriate law enforcement agencies. The total dollar loss from all referred cases of fraud was \$239.09 million, with a median dollar loss of \$680 per complaint. This was an increase from \$198.44 million in total reported losses in 2006.

For more information, visit www.ic3.gov.

Auction Sites Must Do More to Protect Consumers

Given the growing role of auction sites in software piracy and the especially high hurdles in identifying and fighting such piracy, BSA believes auction sites should take the following additional steps to protect consumers:

ASSUME RESPONSIBILITY: To date, auction sites have insisted that piracy on their sites is beyond their ability to police. Although the challenge is certainly broad and complicated, auction sites could do much more to protect consumers by working more closely with the software industry and others to share information and collaborate on best practices.

WARNINGS: Current warnings to sellers and buyers of software—if they exist at all—tend to be buried in hard-to-find areas of auction sites. To have a greater impact, auction sites should post warnings to vendors at the time they list their products and to consumers at the point of bidding. These could take the form of pop-up ads reiterating the risks and penalties of dealing in pirated software.

SLOW IT DOWN: Several of the auction sites offer consumers a “Buy It Now” option, short-cutting the auction process in favor of quick sales at discounted prices. However, the speed of such transactions makes it harder to monitor and catch the scammers. Recognizing that an estimated 50% to 90% of the software on their sites is illegitimate, the auction sites should eliminate the “Buy It Now” option for software sales.

What Consumers Can Do to Protect Themselves

As described throughout this report, consumers face a serious risk of identity theft, having their computers become involved in cyber crime, and many other hassles when buying software from questionable sources online. Armed with the right information, however, consumers can avoid online software piracy scams and protect their personal well-being. The following is a list of tips for consumers:

Use software updates.

Take advantage of free software updates from the original publishers, which often contain “patches” to fix security flaws that have been discovered by the publishers themselves.

Trust your instincts.

When you buy software from the original publishers, brand-name sources or other online sources, that offer security features, you are much more likely to get a safe, legitimate product than when you buy from anonymous, unprofessional sources. Also, check the online seller’s price against the estimated retail value of the software. Whether the product is being sold as new or used, if a price for software seems “too good to be true,” it probably is.

Look for a “trust mark.”

Look for a “trust mark” from a reputable organization to make sure the online retailer is reliable and has a proven track record of satisfying customers. If in doubt, conduct web searches about the website in order to determine its legitimacy. You may also check for a Better Business Bureau report at www.bbb.org.

Do your homework.

On auction sites, check the seller’s rating or feedback comments by other users. Most legitimate sellers will have responses from other users, and if they are reputable and reliable, nearly all should be positive.

Make sure it’s authentic.

Be suspicious of software products that do not include proof of authenticity such as original disks, manuals, licensing, service policies, and warranties. Beware of products that do not look genuine, such as those with handwritten labels.

Beware of back-ups.

Take care to avoid sellers offering to make “back-up” copies. This is a clear indication that the software is illegal. Also be sure to check the software version. Many people receive educational or promotional versions of software when they have been told they were purchasing a full or standard version.

Steer clear of compilations.

Be wary of compilations of software titles from different publishers on a single disk or CD. This is a sure sign that the software has been pirated and possibly altered. When buying more than one software program, be sure that each program is on a separate disk.

Get the seller’s address, if possible.

Remember that if you cannot contact the seller after making a purchase, you may have no recourse if the product turns out to be pirated. BSA receives numerous reports about sellers who became impossible to reach as soon as the payment was final.

Keep receipts.

Keep as much information as possible regarding the transaction and the seller. Print out a copy of your order with confirmation numbers and file it for your records. This information will help to build your case if the product turns out to be pirated and further action is needed with the auction site or payment facilitator site.

Understand the transaction terms.

Make sure you get a clear explanation of the merchant’s policies concerning returns and refunds, shipping costs, and security and privacy protection before you complete the transaction. Check the website’s privacy policies to understand what personal information is being requested, as well as how your information will be used and protected.

Ensure secure payment.

Before you give your payment information, check that the Internet connections you are using are secure. Most Internet browsers will display a padlock icon when you are using a secure site; or you can check the website address in the address bar. If the connection is secure, the site address will be preceded by https:// instead of http://. Heed any pop-up boxes that warn you about an invalid “security certificate.”

Be cautious when dealing with software sellers in other countries.

Many cyber crime rings are based in countries abroad. Moreover, the physical distance, differences in legal systems, and other factors could complicate matters if the transaction goes awry.

Recognize and avoid e-mail spam.

Indicators that an e-mail may be unsolicited spam include senders whose names you do not recognize; typos and odd phrases in the subject line; and prices that seem too good to be true. Delete such messages without opening them, and empty your “trash” folder frequently.

How to Report Suspected Software Piracy and Fraud

Consumers have a key role to play as sentinels of possible Internet fraud. Individuals who believe they may have information about software piracy—or who have become victims of such fraud—are encouraged to file a confidential report at www.bsacybersafety.com or call **1-888-NO-PIRACY**.

Know it. Report it. Reward it.

Conclusion

Software piracy may be tempting to those who are not familiar with the risks. But far from being an innocent, victimless crime, software piracy exposes users to unacceptable levels of cyber security risk, including costly identity theft. It also undermines the value of intellectual property, which is one of the key drivers of innovation and the way millions of people earn a living.

In today's increasingly interconnected global economy, the Internet has opened incredible new frontiers for communicating, shopping, learning, and simply having fun. At the same time, the Internet's global reach, anonymity, and speed can be used for harmful purposes as well as benign ones. As long as the Internet remains a central front in the war on software piracy and related crimes, BSA will continue to raise awareness of the problem and focus considerable resources on pushing back the enemy.

For more information from BSA on online software piracy, or other important IT topics, go to www.bsa.org.

End Notes

1. "Justice Breyer Is Among Victims in Data Breach Caused by File Sharing," Brian Krebs, *The Washington Post*, July 9, 2008.
2. BSA sources.
3. Estimate as of May 31, 2008. Internet World Stats by Miniwatts Marketing Group, <http://www.internetworldstats.com/>.
4. "The Fight for Cyber Space: High Tech and Law Enforcement Experts on Defeating Today's Cyber Criminals," Business Software Alliance, 2007.
5. "2007 Global Software Piracy Study," IDC, May 2008; "2007 State Piracy Study," IDC, July 2008; "Piracy Reduction Impact Study," IDC, 2008, all available at www.bsa.org.
6. Based on a study of Internet traffic in Europe, the Middle East and Australia from August to September of 2007. "Majority of Internet bandwidth consumed by P2P services," Paul Mah, IT News Digest on Tech Republic.com, November 28, 2007, <http://blogs.techrepublic.com.com/tech-news/?p=1651>.
7. "Over 1 Million Potential Victims of Botnet Cyber Crime," FBI press release, June 13, 2007.
8. "National Survey Reveals Consumers Concerned About Safety and Security of Online Shopping," BSA press release, November 15, 2006.
9. "The Risks of Obtaining and Using Pirated Software," IDC, October 2006.
10. "The Risks of Obtaining and Using Pirated Software," IDC, October 2006.



BUSINESS SOFTWARE ALLIANCE

1150 18th Street, NW
Suite 700
Washington, DC 20036
T. +1 202 872 5500
F. +1 202 872 5501

BSA ASIA-PACIFIC

300 Beach Road
#25-08 The Concourse
Singapore 199555
T +65 6292 2072
F +65 6292 6369

BSA EUROPE-MIDDLE EAST-AFRICA

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom
T +44 [0] 20 7340 6080
F +44 [0] 20 7340 6090

WWW.BSA.ORG





A REPORT BY THE
BUSINESS SOFTWARE ALLIANCE
OCTOBER 2009

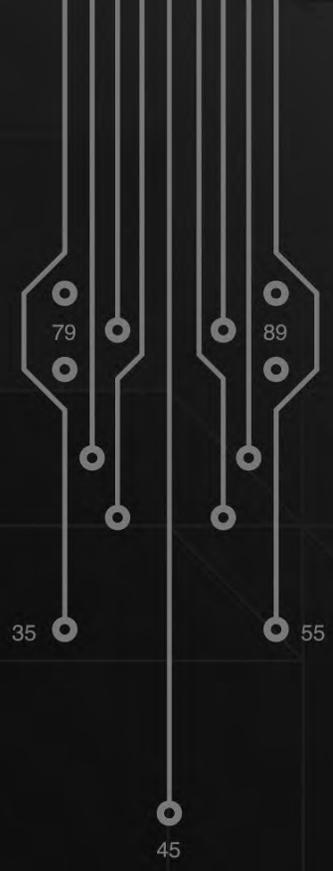
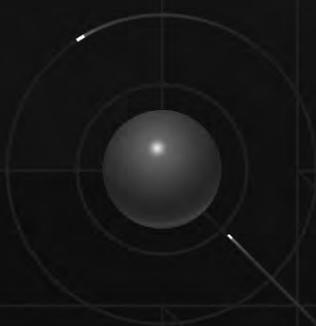


BSA®

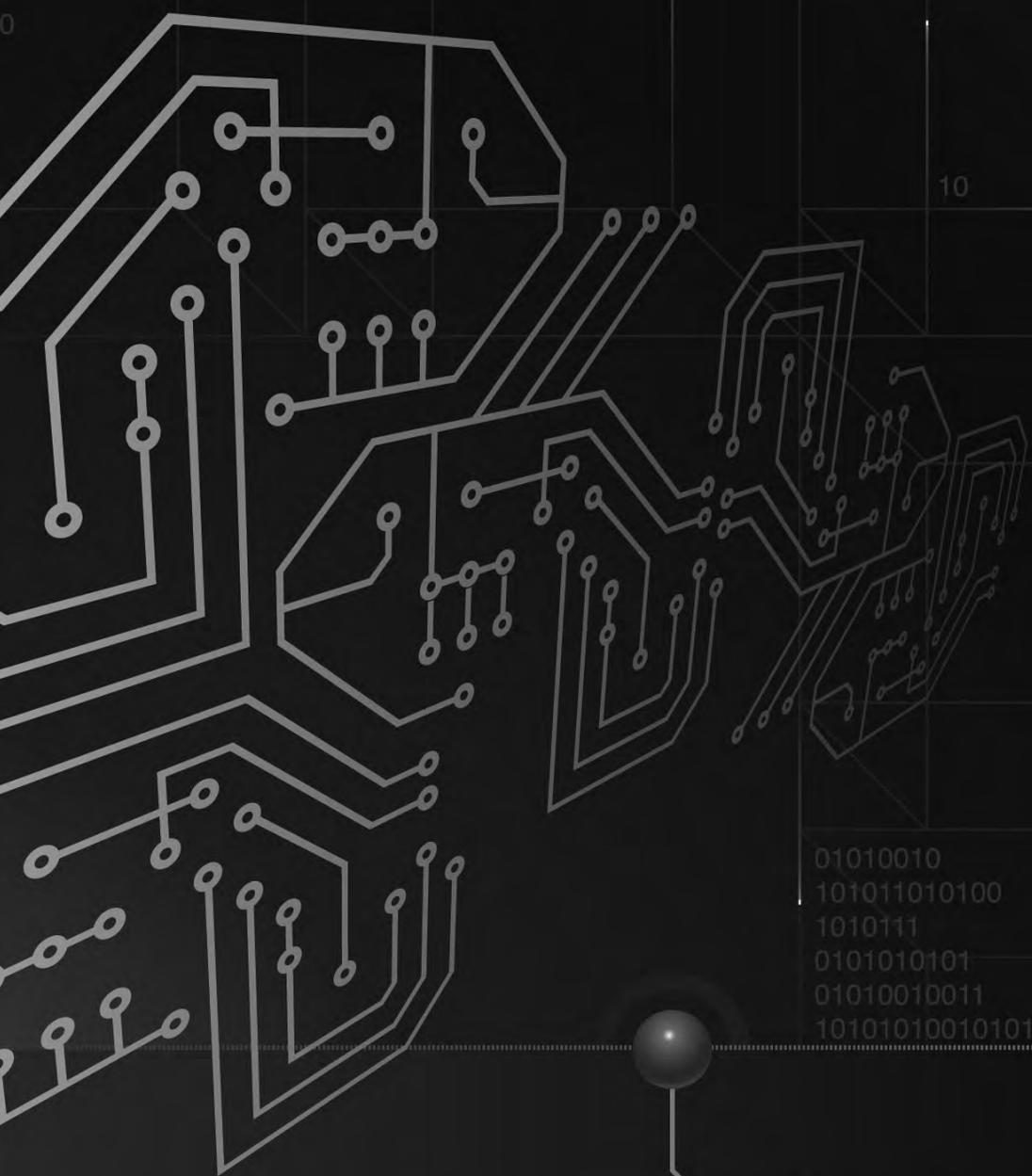
BUSINESS SOFTWARE ALLIANCE

Software Piracy on the Internet: A Threat To Your Security

100
1
11
10101
0
01001
01001
001010011
0010101
01000_



101
10101
0



10

01010010
101011010100
1010111
0101010101
01010010011
10101010010101



Contents

Foreword 5

Introduction 6

The Many Forms of Internet Software Piracy 8

The Correlation between Malware and Piracy..... 11

The Risks to Consumers 12

BSA Investigations of Internet Software Piracy..... 13

Enforcement Action 14

Enforcement Case Studies..... 16

Government Policy..... 18

BSA Partnerships and Educational Outreach 20

The Larger Internet Crime Puzzle..... 22

What Consumers Can Do to Protect Themselves 23

How to Report Suspected Piracy and Fraud 24

Conclusion..... 25

Endnotes 26

CHARTS AND ILLUSTRATIONS

Rate of Software Piracy vs. Malware Infection 10

Software Piracy Sites Also Spread Malware..... 10

Number of Online Software Auctions Removed Due to BSA Requests 13

Foreword

For the second year, the Business Software Alliance (BSA) has produced the Internet Piracy Report, an overview of the scale and serious negative impacts of online software piracy, including a retrospective look at the past year's notable enforcement actions, and a resource for those who wish to avoid the pitfalls of illegal software on the Internet. Overall, this year's report makes it clear that software piracy is as pervasive as the Internet itself, exposing users of illicit goods to a host of risks while at the same time harming the economy. Individuals who, mistakenly or otherwise, turn to auction sites and peer-to-peer networks to acquire or transfer illegal software expose themselves to everything from malware and identity theft to criminal prosecution.

Among the notable cases highlighted in this year's report is that of Tommy Rushing, recently sentenced to three years in federal prison for copyright infringement linked to four for-profit Web sites that offered pirated copies of Adobe and Macromedia software. Likewise, Timothy Dunaway was sentenced to 41 months in prison for selling counterfeit computer software through 40 different Web sites. Outside of the US, a District Court in Taiwan sentenced two individuals to six months' imprisonment for illegal duplication of software, while Hungarian authorities raided the country's largest illegal software distribution company and seized approximately 250 terabytes of illegal content stored on 43 computer servers. The largest case in the world was in China, where the government shut down and convicted the leaders of tomatolei.com, a Web site offering free downloads of massive quantities of illegal software originally published by Adobe, Autodesk, Microsoft, and Symantec.

Alongside enforcement, this year's Internet Piracy Report also highlights how BSA works proactively to educate users about the dangers of online piracy. Pirated products often fail to function properly, or worse still, they are capable of infecting users' PCs with malware that has the potential to cause serious damage. According to some reports, indiscriminate use of peer-to-peer file-sharing networks has led to the disclosure of sensitive government and personal information including FBI surveillance photos and Social Security numbers.

Consumers can often protect themselves just by using common sense and trusting their instincts. Software security updates, trust marks, and a little homework can make a big difference, too. But the best advice is simply to be aware that illegal software is all too common online, and it is best avoided.

Finally, on behalf of millions of people who work in the software industry and related fields worldwide, we at BSA say thank you to those in law enforcement and private industry who are on the front lines in the fight against Internet piracy. Every Internet user in the world ultimately depends on them to help keep the software industry — and society at large — vibrant, innovative and healthy.

ROBERT HOLLEYMAN
President and CEO
Business Software Alliance

Introduction

On any given day, nearly 1.7 billion people around the world use the Internet.¹ Software and computers have become indispensable tools in our businesses, schools, and personal lives.

However, no technology or tool is without risk, and wherever people gather, there are bound to be criminal elements on the fringe of the crowd. The Internet is no different. Almost daily it seems we hear about a new virus spreading through millions of computers; or about companies and government agencies losing sensitive data of employees, customers, and citizens; or in one recent case, about peer-to-peer (P2P) network use exposing confidential witness lists in a high-profile trial of a mafia hit man.

As complex as the technology used to create and develop the Internet is, so too is the network of online criminals and their cyber arsenal of viruses, trojans, and other forms of malware used to dupe unsuspecting consumers and even steal their identities. Internet threats are a clear and present danger to society, as the potential economic rewards for criminals are enormous and the curtain of anonymity behind which they can hide is equally heavy.

Internet threats now go far beyond e-mail spam and swindles of gullible consumers. Today, public and private organizations are dealing with massive onslaughts of malware and inappropriate content. For example, the US Federal Trade Commission (FTC) recently shut down a notorious rogue Internet service provider that was operating under various names and dedicated exclusively to recruiting, knowingly hosting, and participating in the distribution of spam, child

pornography, and other harmful electronic content including spyware, viruses, and Trojan horses. According to the FTC, the service provider even established a forum to facilitate communication between criminals.² The complexity of such nefarious organizations far transcends the stereotype of a lone individual distributing inappropriate content.

The Internet Theft Resource Center estimates that in 2008, 35 million data records were breached in the United States alone, the majority of which were neither encrypted nor protected by a password.³ This sad state of affairs shows that security practices and awareness remain low among many Internet users, making it possible for hackers to continue to prey on individuals and organizations. Even as technology providers and users work to close the obvious security holes, the “bad guys” continue to roll out new threats.⁴

What many people may not realize is the connection between Internet security threats and Internet-based software piracy. This is the second edition of a report on this subject first issued by the Business Software Alliance (BSA) in 2008. The report includes descriptions and facts about the various Internet security threats that are related to unlicensed software use; case studies from recent experience; and perhaps most importantly, additional information and steps consumers can take to be an informed and protected Internet user.

On behalf of the leadership of the global software industry, BSA has spent more than 20 years defending the value of intellectual property and pursuing software pirates. Over the past decade, this mission has expanded



to include cracking down on those who offer illegal software via P2P networks, auction sites, and other kinds of Internet-based channels.

Worldwide, roughly 41 percent of all software installed on personal computers is obtained illegally, with foregone revenues to the software industry totaling \$53 billion. These are funds that could have been invested in new jobs and next-generation solutions to society's needs. Software piracy affects more than just the software industry since for every \$1 of PC software sold, there is another \$3 to \$4 of revenues lost to local IT support and distribution services.⁵

This report also demonstrates how software piracy — far from being an innocent, victimless crime — exposes users to unacceptable levels of cyber-security risk, including the threat of costly identity theft or allowing one's computer to become a tool in further criminal activity.

The Many Forms of Internet Software Piracy

Before the rise of the Internet, unauthorized copying of software generally required the physical exchange of disks or other hard media through the mail or on the streets. But as technology has advanced and high-speed Internet connections have spread around the world, software piracy has moved from the streets to the Internet.

Generally, Internet software piracy refers to the use of the Internet to:

- Provide access to downloadable copies of pirated software;
- Advertise and market pirated software that is delivered through the mail; or
- Offer and transmit codes or other technologies to circumvent anti-copying security features.

The process can be as evasive as any other illegal activity. Buyers may be directed to one Web site to select and pay for a software program, and then receive instructions to go to another Web site to download the product. This circuitous process makes the pirate less vulnerable to detection.

Internet-based software scams can occur through numerous channels:

AUCTION SITES: Online auction sites are among the most popular destinations on the Web, with millions of people logging on to buy and sell a vast array of products. The most widely recognized auction sites are eBay, UBid, Mercadolibre in Latin America, Taobao and Eachnet in China, and QXL in Europe. Yahoo! operates heavily used sites in Japan, Hong Kong, Singapore, and Taiwan. While many legitimate products are sold on auction sites, the sites are also subject to abuse, especially when it comes to software sales.

PEER-TO-PEER (P2P): Peer-to-peer technology connects individual computer users to each other directly, without a central point of management. To access a P2P network, users download and install a P2P client application. Millions of individuals have P2P programs installed on their computers, enabling them to search for files on each other's computers and download the files they want, including software, music, movies, and television programs. Popular P2P protocols include BitTorrent, eDonkey, Gnutella, and FastTrack. P2P applications include eMule, Kazaa, BearShare, and Limewire. Currently, the most popular protocol worldwide is BitTorrent. BitTorrent indexing and tracker sites facilitate obtaining and sharing illegal copies of software online. In Europe, the Middle East, and Australia, P2P traffic consumes anywhere between 49 percent and 89 percent of all Internet traffic in the day. At night, it can spike up to an astonishing 95 percent.⁶

BUSINESS-TO-BUSINESS (B2B) SITES: Business-to-Business (B2B) Web sites enable bulk or large-scale distribution of products for a low price. Counterfeit software is often sold by distribution sellers on these sites.

SOCIAL NETWORKING SITES: According to Web-security firm Sophos, social networking Web sites such as Facebook, Twitter, and MySpace will soon become "the most insidious places on the Internet, where users are most likely to face cyber attacks and digital annoyances." In a recent report, the firm says security experts are becoming increasingly concerned about malicious attacks originating from social networking sites, as well as the risks of users revealing sensitive personal or corporate data online.⁷

OTHER WEB SITES: Some Internet software scams are conducted via Web sites that offer advertising, such as



According to a report in *The Washington Post*, the indiscriminate use of a P2P networks has led to the disclosure of sensitive government and personal information, including FBI surveillance photos of a suspected mafia hit man, confidential witness lists in the man's trial, Social Security numbers, names of individuals in the witness protection program, and lists of people with HIV. The information is often exposed inadvertently by people who download P2P software to share music or other files, perhaps not realizing that the software also makes the contents of their computers available to others. According to the testimony of one Internet security company executive before the US House of Representatives Oversight and Government Reform Committee, "This is not information you want to have out there."

Brian Krebs and Ellen Nakashima, "File Sharing Leaks Sensitive Federal Data, Lawmakers Are Told," *The Washington Post*, July 30, 2009

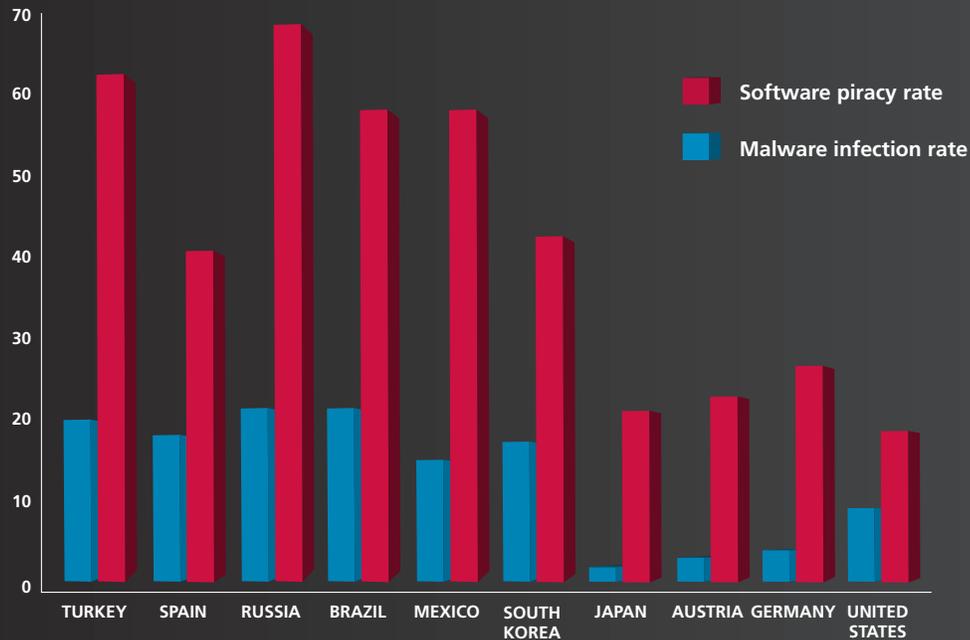
craigslist, Google, and Yahoo!. iOffer.com describes itself as an online "trading community" without auctions or listing fees. Other scams occur via "cyber lockers" or one-click file-hosting sites such as RapidShare, Megaupload, and Hotfile, where users can upload their content, receive a Web link for it, and then provide that link to others via direct e-mails or ads on other Web sites. Finding and stopping software piracy on such Web sites is becoming more difficult as the number of Internet domain names and overseas-based Web sites proliferates. Some Internet observers have proposed allowing domain name registrars to block information about who controls any given site, which would make it even more difficult to protect consumers from fraud.

BOTNETS: Botnets illustrate how the worlds of software piracy and cyber crime are merging. They are both a contributor to software piracy and one of its most alarming side effects. In simple terms, "bot" is short for robot, a piece of software code programmed to conduct repetitive tasks, while "net" is short for network. In the cyber-crime context, cyber criminals and/or their accomplices ("bot herders") send out "bots" through

various techniques, including e-mail spam and malicious code ("malware") added to pirated software. The bots and malware infect ordinary consumers' computers, which then become remotely controlled "zombies." The compromised zombie computers can then be tied together in a botnet and exploited remotely by the cyber criminals to carry out a variety of illegal activities. According to the FBI, more than 1 million computers have become ensnared in botnets.⁸ "And the owners often have no idea that it's happening," says Dave Marcus, security research and communications manager with McAfee Avert Labs.⁹

OLDER FORMS OF INTERNET PIRACY: Several older forms of Internet-based piracy are still seen but have been largely supplanted by the more efficient techniques described above. These techniques include Internet Relay Chat (IRC), which are locations on the Internet for real-time, multi-user, interactive conversations; File Transfer Protocol (FTP), a standard computer language that allows disparate computers to exchange and store files quickly and easily; and newsgroups, established Internet discussion groups that operate like a public e-mail inbox.

Rate of Software Piracy vs. Malware Infection

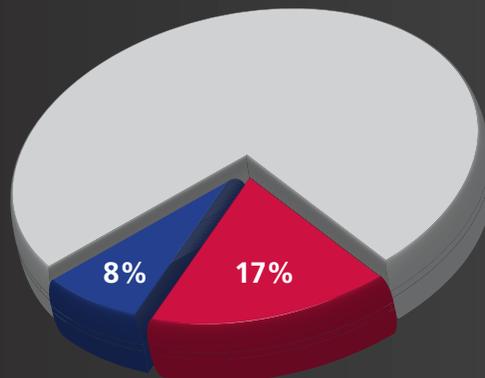


MARKETS WITH HIGH SOFTWARE PIRACY RATES OFTEN HAVE HIGH MALWARE INFECTION RATES^{12,13}

SOURCES: SIXTH ANNUAL BSA AND IDC GLOBAL PIRACY STUDY; MICROSOFT SECURITY INTELLIGENCE REPORT VOL. 6

Software Piracy Web Sites* Also Spread Malware

SAMPLE OF 98 UNIQUE WEB SITES



8% OF SITES OFFER MALICIOUS OR POTENTIALLY UNWANTED SOFTWARE

17% OF SITES HAVE MULTIPLE INSTANCES OF MALICIOUS OR POTENTIALLY UNWANTED SOFTWARE

* SITES OFFER ACCESS TO PIRATED SOFTWARE AND PIRACY-RELATED TOOLS.

SOURCE: IDC, RISKS OF OBTAINING AND USING PIRATED SOFTWARE, 2006 SOURCE: IDC STUDY, RISKS OF OBTAINING AND USING PIRATED SOFTWARE, 2006

The Correlation between Malware and Piracy



Globally, there is significant evidence to link software piracy with the frequency of malware attacks. While this correlation has not been measured with precision, the evidence from industry sources suggests that markets with high software piracy rates also have a tendency to experience high rates of malware infection (see diagram on page 10).

Security threats such as viruses, worms, trojans, and spyware are often designed to exploit vulnerabilities in common software products, forcing software developers to constantly develop patches and other fixes to keep emerging malware at bay. 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, and are therefore more susceptible to attack over the long term. Moreover, once infected, consumers are often forced to turn to experts to repair the damage done by the malware, often negating any savings from having acquired and used the products illegally.

One needs only to look at the 2008-2009 spread of the “Downadup” virus, also known as the “Conficker worm.” The sleeper virus implanted itself on at least 8 million computers worldwide, and while its exact purpose was unknown, it appeared to give hackers the ability to steal financial and personal information. Security investigators are now describing it as one of the most serious infections they have ever seen. An expert at security firm Symantec showed that the virus spread rapidly in geographic areas with the highest piracy rates,

bearing out the correlation between lax handling of software and computers, and security threats that affect millions of people.¹⁴

Another study from IDC also shows that malware and pirated software frequently co-exist on certain Web sites that offer access to pirated software and piracy-related tools (see diagram on page 10). At least a quarter of such sites were found to be rife with trojans and other security threats that are imbedded into downloaded products or distributed through other means to infect visitors’ computers.

The Risks to Consumers

Internet commerce is largely unrestricted, self-regulated, and anonymous. Consumers should proceed with caution when purchasing and using software from unknown vendors online. Using illegal software can put one's personal information, financial security, and even reputation at risk. At the very least, it can lead to software incompatibility and viruses, drive up maintenance costs, and leave users without technical support or security updates. At worst, it can cost ordinary consumers hundreds or thousands of dollars and lost time due to identity theft and the exposure of personal information.

The statistics on risks to consumers are ominous. According to a survey conducted by Forrester Research on behalf of BSA, one in five US consumers who purchased software online in 2006 experienced problems. Of those who had problems:

- 53% received software that wasn't what they ordered;
- 36% reported that the software did not work;
- 14% immediately realized the software was pirated; and
- 12% never received the product.¹⁰

The risks to consumers also include:

- Not receiving upgrades, technical support, manuals or appropriate documentation;
- Receiving an incomplete, altered, or trial version of the software;
- Allowing criminals access to sensitive personal and financial information; and
- Infecting the consumer's computer with viruses or tools for remote-controlled cyber crime.

A 2006 report by the IDC research firm revealed that 25 percent of Web sites offering access to pirated software and piracy-related tools were distributing malicious code that could undermine IT security and performance. In some cases, the Web sites exploited vulnerabilities in the users' computers to install the unwanted software automatically.¹¹



BSA Investigations of Internet Software Piracy

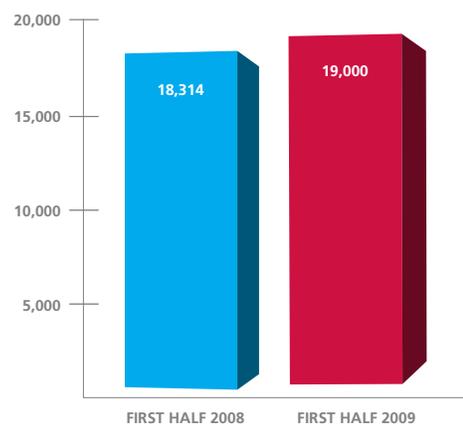
The software industry has worked to combat Internet-based software scams for more than a decade. The centerpiece of BSA's efforts is the Online Auction Tracking System (OATS), a proprietary tool that monitors auction sites and BitTorrent networks (described above) on a continuous basis, while another tool monitors other P2P activity. These systems identify thousands of cases of suspicious activity each day in countries where scanning is permitted by law. BSA then analyzes each case to determine whether it merits further action.

Once BSA has identified offerings of illegal software via various Web sites and P2P networks, it may issue "takedown" notices to the Internet Service Providers (ISPs), asking them to remove the pirated software. In the first half of 2009, BSA stepped up its efforts in this area and issued almost 2.4 million takedown notices related to P2P and BitTorrent file sharing, an increase of more than 200 percent over the same period in 2008.

In 2007, BSA launched an in-house Internet "crawler" to strike further up the BitTorrent supply chain, in addition to the notices sent at the "demand" level where permitted by law. In the first half of 2009, BSA more than doubled its impact with this tool compared to Q1 of 2008, requesting the removal of almost 103,000 torrent files from nine of the largest BitTorrent index sites worldwide. These torrent files were being used by nearly 2.9 million individuals to download software with a retail value of more than \$974 million.

When BSA finds suspicious software being offered on auction sites, it issues takedown requests to the auction site providers to remove those listings. During the first half of 2009, BSA has expanded its efforts in this area as well, requesting auction-site providers to shut down more than 19,000 auctions offering about 128,000 products worth a combined \$55 million.

Number of Online Software Auctions Removed Due to BSA Requests



BSA CONTINUES TO EXPAND ITS ABILITY TO REQUEST TAKEDOWNS OF SUSPICIOUS ONLINE SOFTWARE AUCTIONS. REMOVALS INCREASED 4% FROM 2008 TO 2009.

SOURCE: BSA DATA

Enforcement Action

When necessary and appropriate, BSA files civil lawsuits to try to stop Internet-based piracy, sometimes referring cases to the US Justice Department (DOJ) for criminal prosecution. Such cases may bring about very serious consequences. Federally prosecuted copyright infringement cases can result in fines of up to \$250,000 and, in some cases, jail time.

Over the past decade, BSA, its member companies, and outside partners have provided significant assistance to the Justice Department on hundreds of prosecutions of criminals who were operating for-profit and not-for-profit online software scams. Several of these cases resulted in prison sentences of anywhere between six and nine years, and millions of dollars in restitution.

The following are highlights of several notable Internet piracy cases.

United States

VIRGINIA: In April 2009, Gregory Fair pleaded guilty to one count of criminal copyright infringement and one count of mail fraud before the US District Court for the District of Columbia. From 2001 through 2008, Fair sold a large volume of counterfeit Adobe software on the eBay auction site using multiple user IDs. The combined retail value of this software was at least \$1 million. Fair agreed to forfeit the proceeds, including \$144,000 in cash, one BMW 525i, one Hummer H2, one Mercedes CL600 and one 1969 Pontiac GTO.

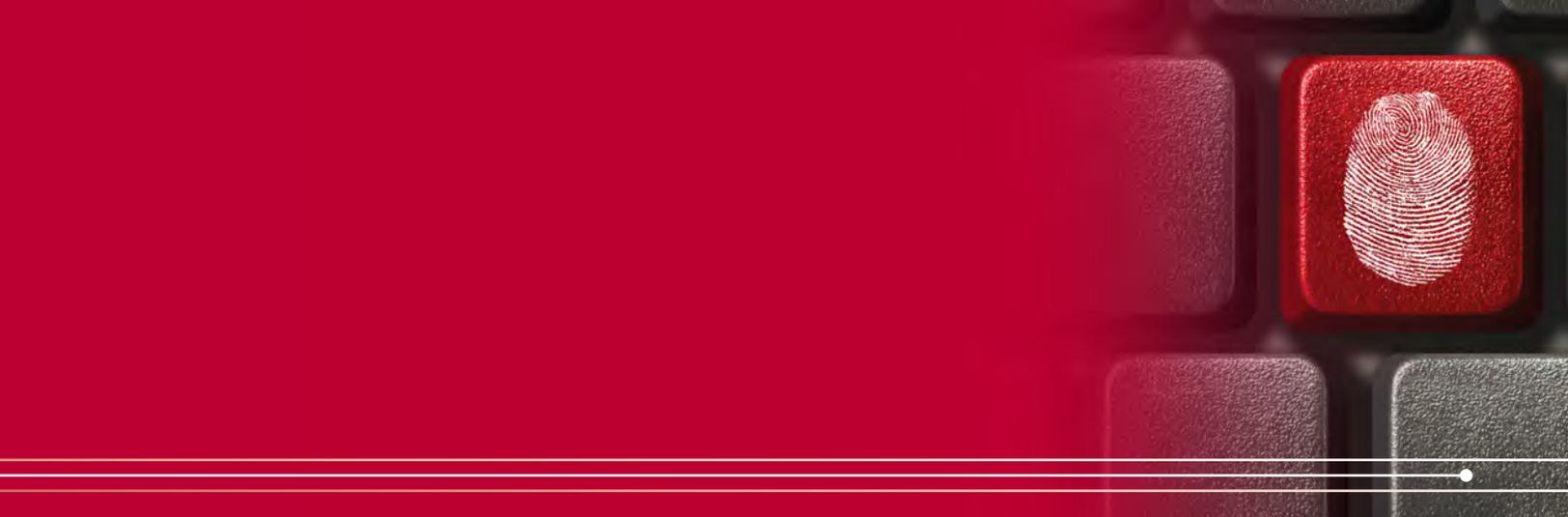
WISCONSIN: In February 2009, Kelly Garcia of Dubuque, Iowa, was sentenced in the Western District of Wisconsin to six months in prison for copyright infringement. In March 2003, Garcia advertised the sale of software products by e-mail offers, including more than 25 products of BSA member companies. After an undercover investigation conducted by BSA, the case was referred to the US DOJ. In November 2003, federal agents searched Garcia's home and discovered she had received approximately \$85,000 in proceeds from illegally selling copyright-protected software.

MISSISSIPPI: In May 2008, Mark Anderson was sentenced in the Southern District of Mississippi to 24 months of incarceration plus three years of suspended supervisory release for copyright infringement. While operating the Web site oemcdshop.com, Anderson offered unlicensed copies of more than 31 BSA member-company products. As part of his sentencing, he was ordered to pay restitution in the amount of approximately \$46,000.

Asia Pacific

JAPAN: In July 2009, BSA settled a case with an architect who was making illegal copies of Autodesk products and selling the pirated software on Yahoo! Japan's auction site. The seller agreed to pay damages and submit the full list of customers who purchased the software.

TAIWAN: In July 2009, a court in Taiwan sentenced two individuals to six months imprisonment and a criminal fine for illegal duplication of software. The Web site, XYZ Information Workshop, had been operating since 2002, providing unlicensed software products for sale over



the Internet. BSA assisted the government's Intellectual Property Rights Protection Team with the investigation. As part of a 2007 raid, approximately 80,000 copies of CD-Rs were seized in addition to two servers and 19 CD burners. The CD-Rs inspected contained 2,877 copies of BSA members' software, including products by Adobe, Altium, Apple, Autodesk, Bentley, McAfee, Microsoft, PTC, Siemens, Dassault Systemes SolidWorks, Sybase, Symantec, and The Mathworks.

Europe, Middle East and Africa

HUNGARY: In April 2009, the Hungarian National Investigation Authority against Organized Crime raided the country's largest illegal software distribution company, ColdFusion Kft (aka Spamfusion). During the raid, the authorities seized approximately 250 terabytes of illegal content stored on 43 computer servers. Internet traffic in Hungary dropped by 10 percent after the raid, illustrating the far-reaching impact of online software piracy on the Internet. BSA supported the National Investigation Office with the case starting in 2007.

UNITED KINGDOM: In September 2008, Richard Clark of Wolverhampton was stopped from selling counterfeit copies of Adobe, Corel, and Quark software from his Web site, RJ-Software. He agreed to terminate sales of the counterfeit software and pay damages for the distribution of 24 batches of fake software disks. Clark cooperated with the investigation and named a computer maker in Manchester as the source of the illegal goods.

RUSSIA: In April 2008, BSA supported Russian law enforcement with an investigation of a major warez site called ftpwelt.com. For a monthly subscription, users were able to download software programs of BSA members. The two Web site operators were brothers aged 16 and 20. Both were sentenced to prison terms.

Enforcement Case Studies

CASE STUDY: Tommy Rushing

In December 2008, US District Judge Sam Sparks in Austin, Texas, sentenced Thomas “Tommy” Rushing to three years in federal prison, three years of supervised release following jail time, and a \$10,000 fine for copyright infringement. Rushing’s 2006 Porsche Cayenne Turbo, valued at approximately \$40,000, a high-definition television, and computer equipment were also seized as part of the sentencing.

Rushing, of Wichita Falls, Texas, was a college track star at the University of Texas. Beginning in his sophomore year in January 2004, he operated four for-profit Web sites that offered pirated copies of Adobe and Macromedia software. Claiming it was “backup”

software, Rushing and his partners offered individuals the opportunity to download the software from his Web site or purchase both the download and CD. Rushing would then burn the software on a CD-R and mail it to unsuspecting customers. Between early 2006 and September 2007, Rushing and his partners sold an estimated retail value of \$2.5 million in illegal software.

BSA was responsible for providing the US Department of Justice (DOJ) with evidence that led to Rushing’s conviction.

Video excerpts from an interview with Tommy Rushing can be viewed online at www.bsa.org/faces.

CASE STUDY: Timothy Dunaway

In early 2009, Timothy Dunaway of Wichita Falls, Texas, was sentenced to 41 months in prison by US District Court Judge Reed O’Conner for selling counterfeit computer software through the Internet. Dunaway was sentenced to two years of supervised release, ordered to pay \$810,000 in restitution, and forfeit a Ferrari 348 TB and Rolex watch. From July 2004 through May 2008, Dunaway operated approximately 40 Web sites that sold a large volume of downloadable counterfeit software. He operated computer servers in Austria and Malaysia; US and foreign law enforcement agents cooperated in the investigation. Dunaway purchased advertising

for his Web site on major Internet search engines and processed more than \$800,000 through credit-card merchant accounts under his control. The software sold by Dunaway had a combined retail value of more than \$1 million.



CASE STUDY: Matthew Miller

In August 2009, BSA announced that its members won a \$210,563 judgment in the US District Court for the Northern District of California against Matthew Miller of Newark, Del., who sold illegal copies of software through an Internet auction site. Software programs published by Adobe, Autodesk, and Microsoft were at the center of the case, which stemmed from a 2008 investigation by BSA. US District Judge Susan Illston awarded the plaintiffs \$195,000 in statutory damages and an additional \$15,563 for filing costs and attorneys' fees. Miller was barred from committing future acts of copyright infringement involving Adobe, Autodesk, and Microsoft software products, and was ordered to immediately destroy any and all infringing copies of such software in

his possession or control. According to legal documents filed on behalf of BSA member companies, the defendant "admitted he had 'downloaded software, burned and copied CDs, and sold about 200 to outsiders for \$8.00 to \$12.00.'" Records in the case also describe how Miller used the popular iOffer Web site to sell unlicensed copies of BSA member software. In one particular instance, Miller was accused of offering approximately \$12,000 worth of software to an undercover investigator for just \$52, with an agreed price of \$45 after some haggling.

CASE STUDY: Tomatolei

Established in early 2004, tomatolei.com is a China-based Web site offering free downloads of illegal software originally published by Adobe, Autodesk, Microsoft, and Symantec. BSA supported Chinese law enforcement with this case, filing a complaint in June 2008 against tomatolei.com to the National Copyright Administration (NCA) and the Ministry of Public Security (MPS) on behalf of its member companies. In August of that same year, Suzhou Public Security Bureau arrested the Webmaster of tomatolei.com, impounded approximately \$266,000 belonging to the suspect, and found evidence linking him to large-scale reproduction of counterfeit CDs. Chengdu

Gongruan Network Technology Co., Ltd., which runs the tomatolei.com Web site, together with the four defendants, were convicted in August 2009 of criminal liability for copyright infringement associated with unauthorized reproduction and distribution of PC software.

The verdicts marked the end of China's largest online software piracy syndicate and a milestone in the nation's efforts to crack down on Internet piracy. It also demonstrates the joint efforts and achievements of the Chinese government, its enforcement agencies, and the international software industry in fighting large-scale Internet piracy.

Government Policy

As described throughout this report, online software piracy presents serious and immediate threats to software users, software developers and service providers, and society at large. Online piracy also has serious negative effects on other copyright-based industries such as music and motion pictures. While the vast majority of individuals and businesses use software, computers, and the Internet legally, too many people treat the illicit acquisition of copyrighted works online as a minor offense — or even as their right. The truth is, those people are breaking well-established laws, causing severe and widespread damage.

In recent years, governments in many countries have witnessed lively debates over the appropriate policy responses to counter online piracy. BSA members approach the debate with two objectives in mind:

- To effectively deter illicit downloading, uploading, providing, and using of licensed content; and
- To ensure that existing technologies function as designed; that innovation and the development of new technologies is not obstructed; and that users' enjoyment of software, computers, and the Internet is not diminished.

BSA members believe the following principles can help governments strike the right balance between these two objectives:

- 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.

The current voluntary, industry-led approach to developing anti-piracy technologies continues to be effective, and mandated use of any such technologies is not justified.

- In appropriate circumstances, BSA supports:
 - 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 appropriate enforcement actions — subject to appropriate safeguards — including those governing privacy.
 - 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 that such sanctions shall be based on either breach of contract (i.e., the terms of the subscriber's contract with the service provider), or 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 should have the opportunity to have the order stayed pending an appeal.
 - Contractual mechanisms are a helpful and efficient way of dealing with online piracy and should be encouraged and widely implemented.



- When developing steps to address online content piracy, the following should also be given due consideration:
 - The voluntary development and use of anti-piracy content identification and filtering technologies should continue unimpeded; this self-regulatory approach is an 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.
 - 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 meet any other relevant criteria necessary to ensure that users' experience will not be degraded, and the development and deployment of new technologies will not be impeded.
 - 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 impacts of such technologies, and after identified issues have been comprehensively addressed.
- BSA opposes:
 - 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.
 - 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.

BSA Partnerships and Educational Outreach

Beyond enforcement actions, BSA also works with various organizations to gain an even deeper understanding of Internet piracy and to educate the public about the risks of purchasing software from questionable Internet sources.

NATIONAL COMPUTER FORENSICS TRAINING ALLIANCE

(NCFTA): In February 2005, BSA began a sponsorship of a dedicated cyber forensics analyst at the National Computer Forensics Training Alliance (NCFTA). The NCFTA provides a neutral collaborative venue where critical, confidential information about cyber crime — including software piracy — can be shared discreetly. It is also an environment where resources can be shared among industry, academia, and law enforcement. The partnership has provided BSA with valuable data on cyber security and software piracy.

US IPR TRAINING COORDINATION GROUP (IPR TCG):

BSA works closely with the US State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) and Bureau of Economic, Energy and Business Affairs (EEB), which co-chair the Intellectual Property Rights Training Coordination Group (IPR TCG). Founded in 1998, the IPR TCG is comprised of US government agencies and industry associations that provide education, training, and technical assistance to foreign officials and policymakers. The departments of Justice and Commerce, US Trade Representative (USTR), FBI, US Customs and Border Protection, US Patent and Trademark Office, US Agency for International Development, and Copyright Office all participate in the IPR TCG. Private sector partners include the International Intellectual Property Alliance (IIPA), US Chamber of Commerce, International Anti-Counterfeiting Coalition, and other industry organizations.

SMALL BUSINESS ADMINISTRATION (SBA): In 2007, in an attempt to help American small businesses avoid the risks of software piracy, the US Small Business

Administration (SBA) and BSA partnered for a multi-year education program called "Smart About Software: Software Strategies for Small Businesses." By using the tools and tips for responsible management available at www.smartaboutsoftware.org, small businesses can learn to protect themselves from the legal and financial consequences of using unlicensed software. In March 2008, the SBA and BSA hosted a free Webinar for small businesses to discuss software license management and how it fits into a comprehensive business plan. It is estimated that the partnership will educate as many as 100,000 small businesses through the national SBA network.

BETTER BUSINESS BUREAU: In 2003, BSA joined forces with the Council of Better Business Bureaus (CBBB) to educate consumers about the risks of purchasing software on auction sites. Together, the two organizations have reached an estimated 6 million consumers through outreach efforts including media tours, direct mail, television and radio advertising, and online initiatives.

LOOKSTOOGOODTOBETRUE.COM: This Web site was developed and is maintained by a joint federal law enforcement and industry task force, including the US Postal Inspection Service and the FBI. The Web site was built with the goal of educating consumers and preventing them from being affected by Internet fraud. BSA was recently accepted as a new member of the task force and will lend its expertise and resources to the group's efforts.

"DON'T GET DUPED": All computer users should have a basic understanding of how to protect themselves from Internet dangers. The "Don't Get Duped" Web site found at www.bsacybersafety.com was created to help educate consumers on these dangers and offer them a forum through which to tell their stories about how they were duped into purchasing illegal software online. Over



the past several years, nearly 400 consumers have written to BSA to share their experience. More than 30 percent of complaints involved eBay.

For example, many consumers have complained about receiving software that was obviously pirated, oftentimes on store-bought CD-Rs with handwritten titles, no registration keys, and no manuals. In one such case, a Texas consumer who paid \$155 on eBay for Adobe Photoshop CS — software that normally retails for about \$650 — learned that the seller's account was cancelled a few days later. After numerous e-mail complaints to the seller, which were not answered, he was instructed by eBay to wait 10 days from the auction close and then file a complaint with PayPal. PayPal was able to contact the seller, and the man eventually received the software in the mail. But that was not the end of the story. "It was easy to tell it was pirated," he said. "It was in a thin case with just a CD-R and only a handwritten note on the disc itself about what it was. When I opened the package and saw that it was pirated, I immediately e-mailed him requesting my money back." The consumer never got his money back.

More stories about consumers who were duped are posted on www.bsacybersafety.com.

B4USURF: In Asia, BSA manages a cyber safety and ethics campaign (www.b4usurf.org) aimed at influencing youths ages 10–18. The centerpiece of the initiative is a Web site with resources for educators, youths, and parents. For example, the site includes lesson plans and tips for teachers based on input from teachers in Singapore. Over time, BSA hopes to encourage education officials to incorporate Internet-focused ethics, security, and safety units in the curriculum of many nations. To date, the campaign has focused on Singapore, Malaysia, China, Taiwan, the Philippines, Hong Kong and India.

B4UCOPY: In a continuation of the BSA's efforts to educate youth and higher-education students about the potential risks they face online and the importance of respecting intellectual property, BSA introduced B4UCopy, a program designed to raise overall student awareness of copyright issues and to encourage responsible behavior online. BSA selected Young Minds Inspired (YMI), an in-school curriculum-based program creator, to assist in the design of the comprehensive program and curricula which includes lesson plans and teacher guides for grades 3 through 12. The curricula are available on two BSA Web sites created for parents/guardians and educators at www.b4ucopy.com/kids (grades 3-8) and www.b4ucopy.com/teens (grades 9-12). In conjunction with the curricula, the main Web site (www.b4ucopy.com) includes materials to educate college students about cyber safety and cyber ethics. BSA also introduced a B4UCopy video specifically targeting college students. This video includes interviews with college students and offers tips to help students be smart about piracy and using digital media. Due to the success of the North America effort, the Web site has been translated into both Spanish (www.pienseantesdecopiar.com) and Portuguese (www.penseantesdecopiar.com) for use in Latin America.

EDUCATIONAL RESOURCES: In April 2008, BSA unveiled "Faces of Internet Piracy," a revealing look at the true stories of people affected by online piracy. BSA toured the country interviewing software pirates from all walks of life, including an Austin, Texas, college track star (See "Case Study: Tommy Rushing," above); a Richmond Hills, Ga., grandmother; a Lakeland, Fla., entrepreneur; a Wichita Falls, Texas, software programmer; and a New Milford, Conn., college student. The BSA Web page (www.bsa.org/faces) features videos of the pirates telling their personal stories, along with tips for consumers on how to avoid online piracy.

The Larger Internet Crime Puzzle



Online software scams are one piece of the larger Internet crime puzzle. The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), receives Internet-related criminal complaints on an ongoing basis and refers cases to the appropriate local, state, federal, or international agency for possible investigation and prosecution.

In 2008, IC3 processed 275,284 complaints spanning the spectrum of Internet crime from auction fraud, non-delivery, and credit/debit card fraud, computer intrusions, spam/unsolicited e-mail, and child pornography. From the submissions, IC3 referred 72,940 complaints to the appropriate law enforcement agencies. The total dollar loss from all referred cases of fraud was \$264.6 million, with a median dollar loss of \$931 per complaint.

For more information, visit www.ic3.gov.



What Consumers Can Do to Protect Themselves

As described throughout this report, consumers who buy software from questionable sources online or engage with Web sites of dubious credibility face serious risk of identity theft or having their computers involved in cyber crime, among many other hassles. Armed with the right information, however, consumers can avoid online software piracy scams and protect their personal well-being and privacy. The following is a list of key tips for consumers:

TRUST YOUR INSTINCTS. When you buy software from the original publishers, brand-name sources, or other online sources that offer security features, you are much more likely to get a safe, legitimate product than when you buy from anonymous, unprofessional sources. Check the online seller's price against the estimated retail value of the software. Be wary of compilations of software titles from different publishers on a single disk or CD. This is a sure sign that the software has been pirated and possibly altered. Remember, whether the product is being sold as new or used, if a price for software seems "too good to be true," it probably is.

USE SOFTWARE SECURITY UPDATES. Take advantage of free software updates from the original publishers, which often contain "patches" to fix security flaws that have been discovered by the publishers themselves. Also, install antivirus software and make sure it is activated.

LOOK FOR A "TRUST MARK." Look for a "trust mark" from a reputable organization to make sure the online retailer is reliable and has a proven track record of satisfying customers. If in doubt, conduct Web searches about the Web site in order to determine its legitimacy. You may also check for a Better Business Bureau report at www.bbb.org.

DO YOUR HOMEWORK. Most legitimate retail sites will have sections for feedback comments by other users, so check the seller's rating and see what comments others have posted. Most legitimate sellers will have responses from other users, and if they are reputable and reliable, nearly all should be positive.

MAKE SURE IT'S AUTHENTIC. Be suspicious of software products that do not include proof of authenticity such as original disks, manuals, licensing, service policies, and warranties. Beware of products that do not look genuine, such as those with handwritten labels.

BEWARE OF BACK-UPS. Take care to avoid sellers offering to make "back-up" copies. This is a clear indication that the software is illegal. Also be sure to check the software version. Many people receive educational or promotional versions of software when they have been told they were purchasing a full or standard version.

GET THE SELLER'S ADDRESS, IF POSSIBLE. Remember that if you cannot contact the seller after making a purchase, you may have no recourse if the product turns out to be pirated. BSA receives numerous reports about sellers who became impossible to reach as soon as the payment was finalized. If the vendor is unfamiliar to you, look for an online and offline customer support contact. A legitimate transaction should involve ongoing transparency and communication between buyer and seller.

UNDERSTAND THE TRANSACTION TERMS. Make sure you get a clear explanation of the merchant's policies concerning returns and refunds, shipping costs, and security and privacy protection before you complete the transaction. Check the Web site's privacy policies to understand what personal information is being requested, as well as how your information will be used and protected.

ENSURE SECURE PAYMENT. Before you give your payment information, check that the Internet connections you are using are secure. Most Internet browsers will display a padlock icon when you are using a secure site, you can check the Web site address in the address bar. If the connection is secure, the site address will be preceded by <https://> instead of <http://>. Heed any pop-up boxes that warn you about an invalid "security certificate."



HOW TO REPORT SUSPECTED SOFTWARE PIRACY

Consumers have a key role to play as sentinels of possible Internet fraud. Individuals who believe they may have information about software piracy — or who have become victims of such fraud — are encouraged to file a confidential report at www.nopiracy.com or call 1-888-NO-PIRACY. Consumers are also able to file a confidential report at www.bsacybersafety.com.

Through BSA's "Know it, Report it, Reward it" program, individuals who provide qualified reports of software piracy are eligible to receive up to \$1 million in cash rewards.

Know it. Report it. Reward it.

Conclusion



Software piracy may be tempting to those who are not familiar with the risks. But far from being an innocent, victimless crime, software piracy exposes users to unacceptable levels of cyber-security risk, including the threat of costly identity theft. It also undermines the value of intellectual property, which is one of the key drivers of innovation and the way millions of people earn a living.

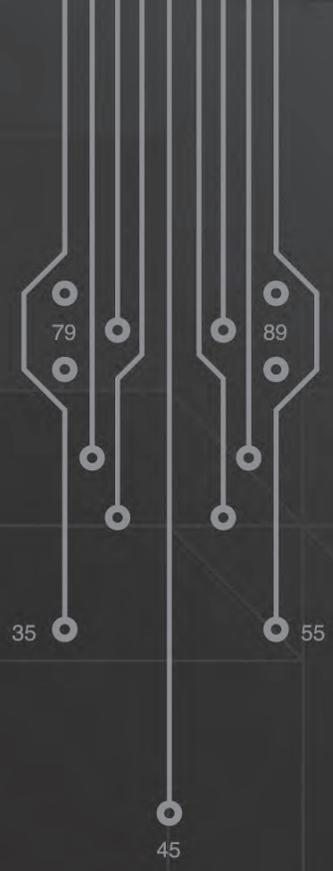
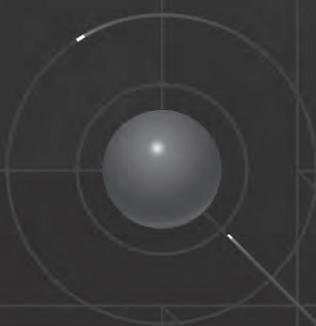
In today's increasingly interconnected global economy, the Internet has opened incredible new frontiers for communicating, shopping, learning, and simply having fun. At the same time, the Internet's global reach, anonymity, and speed can be used for harmful purposes as well as benign ones. As long as the Internet remains a central front in the war on software piracy and related crimes, BSA will continue to raise awareness of the problem and focus its resources on pushing back the enemy.

For more information from BSA on online software piracy or other important IT topics, visit www.bsa.org.

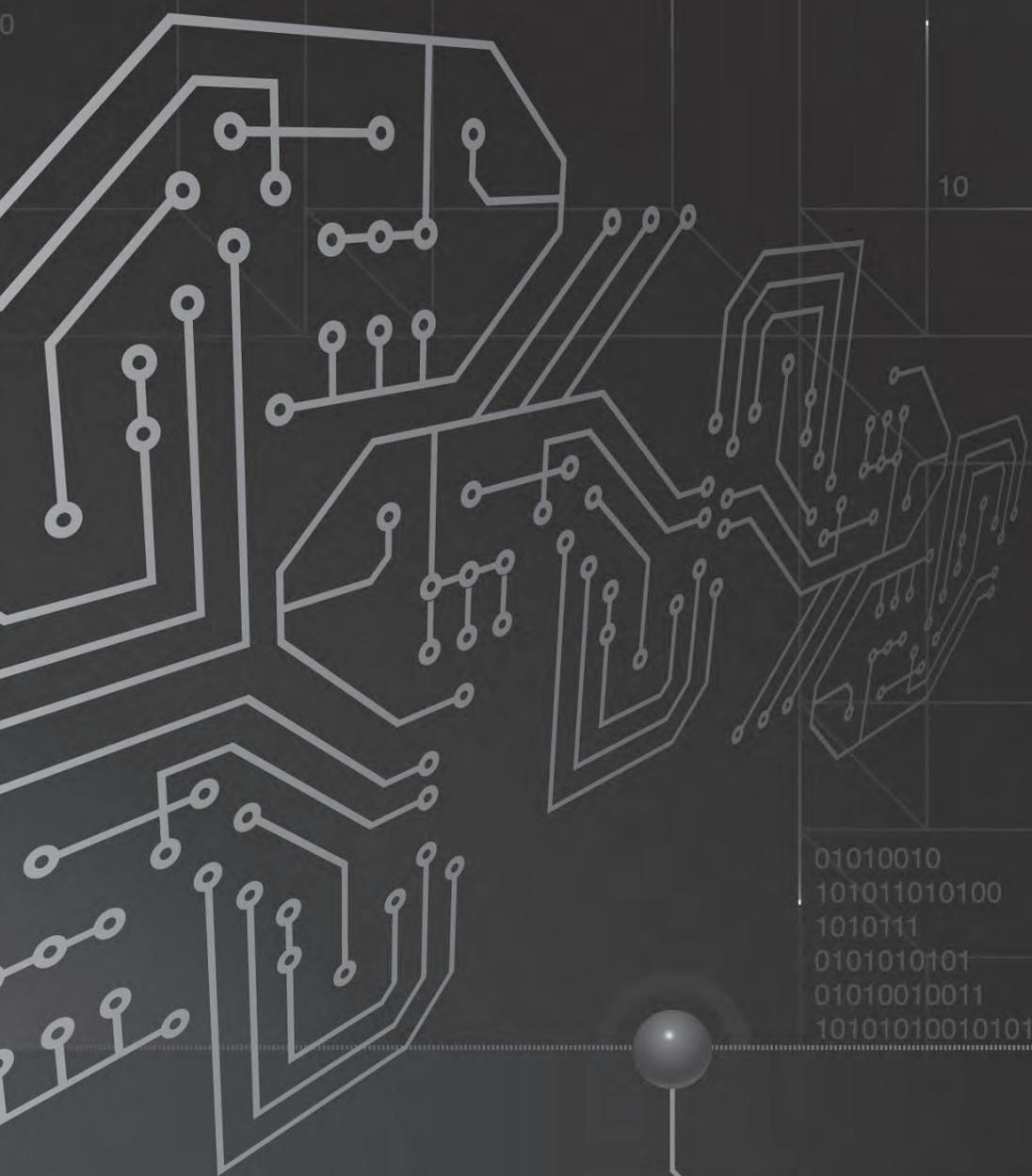
Endnotes

- 1** Miniwatts Marketing Group, Internet World Stats (Web site); 30 June 2009; <http://www.internetworldstats.com/stats.htm>
- 2** FTC Press Release; FTC Shuts Down Notorious Rogue Internet Service Provider, 3FN Service Specializes in Hosting Spam-Spewing Botnets, Phishing Web sites, Child Pornography, and Other Illegal, Malicious Web Content; FTC Press Release; 4 June 2009; <http://www.ftc.gov/opa/2009/06/3fn.shtm>
- 3** ITRC ; ITRC 2009 Consumer Awareness Survey: The Need for "Secure Payment Agent" (SPA); 23 September 2009; http://www.idtheftcenter.org/artman2/publish/lib_survey/SPA_White_Paper_printer.shtml
- 4** IT-Director.com; Ignorance is not Bliss; 19 January 2009; <http://www.it-director.com/business/security/content.php?cid=11015>
- 5** IDC; Sixth Annual BSA and IDC Global Software Piracy Study; May 2009
- 6** Paul Mah, IT News Digest on Tech Republic.com; Majority of Internet bandwidth consumed by P2P services; 28 November 2007; <http://blogs.techrepublic.com.com/tech-news/?p=1651>
- 7** Euractive.com Report; Facebook: A new battleground for cyber-crime; 27 July 2009; <http://www.euractiv.com/en/infosociety/facebook-new-battleground-cyber-crime/article-184380>
- 8** FBI Press Release; Over 1 Million Potential Victims of Botnet Cyber Crime; 13 June 2007
- 9** BSA; Online Software Scams: A Threat to your Security; October 2008; http://www.bsa.org/files/Internet_Piracy_Report.pdf
- 10** BSA Press Release; National Survey Reveals Consumers Concerned About Safety and Security of Online Shopping; 15 November 2006; <http://www.bsacybersafety.com/news/2006-concerned-online-shopping.cfm>
- 11** IDC; The Risks of Obtaining and Using Pirated Software; October 2006
- 12** Microsoft Security Intelligence Report Volume 6; April 2009; <http://www.microsoft.com/security/portal/Threat/SIR.aspx>
- 13** BSA; Sixth Annual BSA and IDC Global Piracy Study; May 2009; http://global.bsa.org/globalpiracy2008/images/GlobalStudy2008_CoverDL.jpg
- 14** Symantec Security Blog; January 2009; <http://www.symantec.com/connect/blogs/downadup-geo-location-fingerprinting-and-piracy>

100
1
11
10101
0
01001
0
01001
001010011
0010101
01000_



101
10101
0



10

01010010
101011010100
1010111
0101010101
01010010011
10101010010101





BUSINESS SOFTWARE ALLIANCE

1150 18th Street, NW
Suite 700
Washington, DC 20036
T. +1 202 872 5500
F. +1 202 872 5501
www.bsa.org

BSA ASIA-PACIFIC

300 Beach Road
#25-08 The Concourse
Singapore 199555
T +65 6292 2072
F +65 6292 6369

BSA EUROPE-MIDDLE EAST-AFRICA

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom
T +44 [0] 20 7340 6080