Software Piracy in the EU:
BSA Response to the Commission Report

April 2011

Over a decade ago, in 1999, the Business Software Alliance ("BSA") responded to the Commission’s Green Paper on Combating Counterfeiting and Piracy in the Single Market.1 The BSA’s response included more than a dozen recommendations for measures to improve Europe’s enforcement regime. That first green paper and follow-on consultations eventually led to the adoption of the Enforcement Directive 2004/48/EC (the “Directive”). By harmonising the minimum means available to fight piracy across Europe, the Directive has been of tremendous benefit to the software industry.

As the Commission recognises in its recent report, despite the Directive’s important contributions, the sheer volume and financial value of piracy in Europe remains alarming. While studies show that since 2004 software piracy levels have fallen in some Eastern European countries where the Enforcement Directive has had the most impact on local legal regimes, levels have remained roughly the same in Western Europe. In fact, Western Europe was the only region in the world in 2009 to see an increase in software piracy, with the regional piracy rate rising from 33% in 2008 to 34% the following year – the same level as in 2004. Overall, the commercial value of illegal software installed in the EU in 2009 alone amounted to nearly €8.7 billion.2

In this response to the latest Commission report, the BSA explains the monumental damage that piracy continues to cause to the software industry, as well as the harmful impact that software piracy has on European economies and consumers. We also quantify the substantial benefits – in terms of increased jobs, tax revenues and safety – that would stem from curbing software piracy. Finally, we propose potential improvements to the EU’s enforcement regime. In our 1999 paper, we also suggested measures to reduce software piracy. Although many of these proposals are reflected in the Directive, adequate deterrence remains an ongoing challenge. If the Commission elects to re-open the Directive, there are a number of
improvements, particularly to the rules on damages, that would make Europe’s enforcement regime more effective. Specifically, we recommend:

- **Damages that both adequately compensate and also deter.** The WTO TRIPS Agreement requires that remedies constitute a deterrent to future infringement. But the EU’s damages rules as an incentive to infringe. These rules must be strengthened.

- **Clarification of the rules on ex parte to ensure that civil search and seizures are achievable and affordable.** Current mechanisms in some Member States impose unduly high evidentiary burdens or are too costly for any but the largest rights holders.

- **A better balance between the important rights of data protection and intellectual property.** The software industry is strongly committed to protecting user privacy. But IP is also key to the success of the internet and the technologies it depends on. These two rights must be better reconciled; and

- **An expanded toolbox of measures to tackle internet piracy.** Internet piracy remains a substantial source of harm to the software industry. Any new measures to fight internet piracy must be subject to appropriate safeguards that protect user rights and do not hinder innovation.
The software industry has always relied heavily on copyrights and other IP to drive innovation and ensure a return on investment in R&D. Theft of this valuable IP is a significant and growing problem – undermining the industry’s ability to innovate, limiting economic growth in Europe’s economies, and threatening the safety of consumers data and security.

**Types of Software Piracy.** Put simply, software piracy is the unauthorised copying or distribution of copyrighted software. But because software comes to market via many channels, there are a number of opportunities for piracy: from counterfeit software working its way through the distribution channel to the end user, to illegal software sold on auction sites, to corporate IT departments that install more copies of a program than they are licensed to install. Some of these forms of software piracy raise challenges that are unique among the copyright industries, and require specific enforcement solutions.

- **Corporate end-user piracy.** The business software industry’s worst piracy problem traditionally has involved its ultimate users – large and small corporate, government and other enterprises – reproducing copies of software without authorisation. This can involve employees using a licensed copy to install a program on multiple computers, copying disks for installation and distribution, taking advantage of upgrade offers without having a legal copy of the version to be upgraded, or simply swapping disks in or outside the workplace. Over-using a central copy of a program via the company network is another major issue. While these types of end-user piracy typically do not involve resale or commercial distribution, they nevertheless provide financial gain to the ultimate users because of the savings they make by not paying for legitimate software licences.

Corporate end-user piracy is a substantially different problem, and is addressed in substantially different ways, from counterfeiting and other unlawful manufacture and distribution of physical products that all copyright industries face. Here, legal action must be taken against the ultimate user rather than a manufacturer or reseller. As a result, the software industry generally depends heavily on civil remedies to take action against otherwise respectable companies. Determining damages in civil infringement suits against such corporate users presents special problems.

- **Hard-disk loading.** Another problem particular to the software industry occurs when manufacturers of PCs (“original equipment manufacturers” or
“OEMs”) or resellers of personal computers load illegal copies of software onto the hard disks to make the purchase of the machines more attractive. Again, this increases the profits of the hard-disk loader without any added costs as they make no royalty payment to the software copyright holder, which allows them to undercut legitimate dealers.

Preventing hard-disk loading also presents unique challenges. Proof of copying relies on evidence gathered during a test purchase of a PC, or in a raid on a PC or hard-disk warehouse. And again, surprise searches are an important tool. But proving a definitive number of illegal copies can be difficult, especially if software is copied only when a customer orders a computer or if the reseller keeps poor records.

Like other rights holders, the software industry also suffers significant harm from piracy over the internet and from counterfeiting:

- **Internet Piracy.** The vast majority of individuals and businesses use software, computers and the internet for entirely legitimate personal, educational and commercial reasons. But while the internet vastly increases opportunities to communicate, learn and do business, it also creates new opportunities to steal software. Software was the first copyrighted content to be digitised, and as a result the software industry has **fought internet piracy far longer than any other sector.** Indeed, BSA has for many years operated an extensive, global internet anti-piracy program, which involves sending high volumes of takedown notices in conjunction with civil litigation, law enforcement liaison and support, and extensive public awareness campaigns.

  Internet piracy covers several different types of online activity. Increasingly, one-click file host services (sometimes referred to as “cyberlockers”) are being misused, allowing links to illegal copies of software to be widely distributed via forums and links sites. Unauthorised distribution of copyrighted software via BitTorrent/P2P networks also remains a considerable problem, as does software being made available for free download or in exchange for uploaded programs on dedicated pirate sites. In addition, large volumes of counterfeit, out-of-channel, infringing copyright software continues to be widely offered on internet auction sites.

- **Counterfeiting.** In the case of packaged software, it is common to find counterfeit copies of CDs incorporating the software programs, as well as related packaging, manuals, licence agreements, labels, registration cards and security features. Counterfeiting is a serious problem for the software industry, as advances in technology have enabled a growing number and variety of commercial enterprises to manufacture and distribute counterfeit
software on a massive scale. Because the risks of being caught are relatively low, and penalties are far less than for engaging in other illegal activities, the software industry is seeing a resurgence of this activity.
BSA has, for well over a decade, collected information and studied global trends in business-software piracy, including in the EU. Over the past seven years, these studies have been conducted in conjunction with IDC, the IT industry’s leading global market research and forecasting firm, using the same methodology and standard, reliable data sets. What these statistics show is that despite all of the efforts to date to combat piracy, over a third of software programs in use within the EU are illegal copies. This average piracy rate of 35% translates to €8.7 billion in value had the pirated software been sold in the market.

**Analysis of EU Piracy Rates Since the Enforcement Directive was Adopted.**

Overall software piracy rates in Europe have remained largely flat since the Enforcement Directive was adopted in 2004.

The software piracy rate across the EU is 35%.
- USA 20%, Japan 21%, and Australia 25%.

It has dropped 1% in five years.
- Japan dropped 7 points, Australia 6.

Six out of the top 20 countries by losses are in the EU.

Direct losses to the software industry in the EU have averaged over $12bn annually over the last five years.

Losses in the EU are nearly 50% greater than in the US and over 60% greater than those in China.

<table>
<thead>
<tr>
<th>HIGHEST COMMERCIAL VALUE OF PIRATED SOFTWARE 2009</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RANK</strong></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
</tbody>
</table>
Notably, there are significant geographical variations. Approximately 64% of the software programs used in Central and Eastern Europe are unauthorised copies compared to 34% in Western Europe, and the software piracy “league table” shows some marked variations among EU Member States: at 27% the UK has the lowest overall software piracy rate (although this still represents unlicensed software with a commercial value of £1 billion), while Bulgaria and Romania have the highest rates (67% and 65% respectively). BSA has found that such variations are partially due to specific deficiencies in national enforcement regimes, which infringers exploit to avoid detection or prosecution.

3. SOFTWARE PIRACY IMPACTS THE BROADER EUROPEAN ECONOMY

Piracy Reduction Means Tax Revenues and Jobs. The economic impact of software piracy extends far beyond the confines of the software industry. Estimates contained in a 2010 study by the BSA and IDC suggest that software theft has cost Member States billions of euros in lost tax revenues as well as hundreds of thousands of lost jobs.⁴ Piracy also slows the growth of the software industry overall, threatening to decrease productivity, capability and competitiveness in virtually all areas of economic activity.

- Present Economic Contribution. As the Commission recognises, the ICT sector accounts for a substantial part of EU GDP and employment, with investment in ICT estimated to have been responsible for around half of the EU’s productivity growth in recent years.⁵ Recent figures indicate the substantial contribution that the business software industry makes to the economies of the EU: in 2010, the top 100 European software vendors generated revenues of €37.242 billion and sustained over 54,000 high-value
R&D jobsvi – and this when, according to BSA estimates, more than a third of business software applications in use were illegal copies. Had levels of illegal copying been lower, there is a strong likelihood that the contributions of the software industry to the European economies would have been far greater.

- **Economic Contribution from Piracy Reduction.** Anti-piracy efforts present an opportunity to capture employment, tax revenue and other economic benefits that result from increasing the size of the software industry via reductions in illegal copying. The 2010 BSA/IDC study demonstrates that even a modest reduction in software theft would have significant multiplier effects on the economic contribution of the packaged software industry.

- **Employment Gains.** The study found that reducing software piracy rates by 10 points from the 2009 European average of 35% to 25% in 2014 would increase total employment by **61,500 new jobs**. In essence, software theft is robbing the economies of Western Europe of **over 60,000 jobs**.

- **Gains in Tax Revenues.** Reducing the levels of illegal copying will also substantially increase the fiscal contribution of the software industry to European economies. The 12 EU countries included in the BSA/IDC study stand to add more than **€33 billion in new consumer and business spending**, and **€9.8 billion in new tax revenues** by reducing piracy 10 points in four years.

- **The Faster the Rate Reduces, the Greater the Benefits.** The study also found that the economic benefits are compounded by reducing software theft at a faster rate. Reducing the software piracy rate to 25% in two years, instead of four, would boost the new spending and extra tax revenues by 37% to €45 billion and €13 billion respectively. Reducing piracy rates 10 points in two years is ambitious, but achievable in many markets – particularly the higher piracy EU markets such as France (40%), Greece (58%), Poland (54%), Spain (42%), and Italy (49%).
4. **SOFTWARE PIRACY ALSO HARMs CONSUMERS**

Although some consumers may think they are getting a great deal when they obtain pirated software, it is more likely they will receive a substandard product with hidden cyber security threats. The fact is that using illegal software puts consumers’ 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 consumers without technical support or security updates. At worst, it can cost ordinary users hundreds or thousands of euros and lost time due to identity theft and the exposure of personal information. vii

- **Malicious code.** It is common for sites that offer access to pirated software and piracy-related tools to distribute malicious code that undermine IT security and performance. Indeed, a significant percentage of counterfeit software or key generators downloaded from P2P sites contains malicious or unwanted code. In one IDC study, (“The Dangers of Counterfeit Software”), research revealed that one in four websites that offered pirated software or counterfeit activation keys attempted to install infectious computer code, like Trojan horses and key loggers, on test computers. The study found that 59% of counterfeit software or key generators downloaded from P2P sites contained malicious or unwanted code. A subsequent study by Harrison Group Inc. found that companies using unlicensed or counterfeit software were over 70% more likely to have critical computer failures lasting 24 hours or more and/or experience the loss or damage of sensitive data.

- **Criminal activity.** Pirated software can also enmesh unwitting consumers in further criminal activity. Botnets illustrate this – they are both a contributor to software piracy and one of its most alarming side effects. In the cybercrime context, cyber criminals and/or their accomplices send out “bots” (i.e., a piece of software code programmed to conduct repetitive tasks) 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.
To help consumers avoid these and other problems associated with pirated software, BSA runs educational programs and offers tips to consumers contemplating software purchases as well as guidance on how to improve cyber security.

viii
5. **The Principal Barriers to Effective Enforcement**

Although software piracy sometimes results from ignorance of law or lax software management practices, as a general rule software piracy takes place simply because it is **profitable**. A corporate end-user increases its own profitability relative to its law-abiding competitors when it uses software without purchasing a licence. Similarly, a computer reseller increases its own profits by illicitly loading software onto the computers it sells. And an internet pirate is able to obtain expensive software illegally for free with little difficulty and at little risk of being caught and penalised.

The software industry spends substantial sums each year in protecting and enforcing its rights. Because it can only prosecute a small percentage of software infringers, the industry relies heavily on the **general deterrence** value of the cases it brings. Public education and awareness activities are important, but the solution to software piracy lies principally in **deterrence**: making it more risky, embarrassing and costly to engage in piracy than to comply with the law.

In our experience, the fundamental challenge to tackling piracy in Europe – offline and online – is a **lack of deterrence**. Damages and penalties for infringement are often lower than the cost of buying or using legal copies. As a result, piracy still pays throughout the EU – a concern we flagged in 1999, and which remains a problem today. The software industry faces other practical challenges in enforcing rights – including challenges in securing civil searches and taking effective action against internet pirates.

The software industry principally relies on the copyright law in the various EU Member States to enforce its rights against piracy. Accordingly, these comments focus on **copyright-based enforcement** primarily.

- **Overly complex, expensive civil ex parte procedures**

  In software piracy cases, evidence can often be deleted using a few keystrokes. For that reason, industry relies on surprise (“ex parte”) searches and seizures to secure evidence of software theft. The Directive’s ex parte provisions have dramatically improved the software industry’s ability to use civil searches; Member States that lacked civil search mechanisms have since introduced them into national law, and in most markets these mechanisms work well.

  In some markets, however, obtaining and executing ex parte search and seizure orders is prohibitively expensive – a result of the need to hire a
supervising solicitor to oversee the process, to post high bonds/securities, or to participate in multiple hearings. As a practical matter, this means that the measures are available to only the largest of right holders in the most significant of cases. In other markets, high evidentiary thresholds require applicants to all but prove infringement – contradicting the Directive’s requirement that evidence is limited to that “reasonably available” and making it all but impossible for right holders to obtain search orders. Still other courts refuse to permit the inspection and/or seizure of licensing documentation, making it difficult to ultimately prove underlicensing.

- **No protection of witness identity in civil search applications**

In order to gather the evidence necessary to obtain a civil search order, the software industry relies heavily on information from third parties. These individuals are understandably reluctant to be identified, to appear in court, or to sign sworn statements about an infringement. Unfortunately, many Member States have not implemented the Directive’s option to protect the identity of witnesses giving evidence in support of a search order; in other markets, third party (i.e., hearsay) evidence is not sufficient to obtain a search order.

- **Unduly narrow data protection rules pose obstacles to effective enforcement online**

In order to identify internet pirates, the software industry depends on evidence obtained from intermediaries under the Directive’s right of information. Some Member States only require such information to be disclosed in criminal cases, citing data protection restrictions. Law enforcement are often under-resourced and unable to take on these cases – meaning rights holders effectively have no way of identifying infringers and enforcing their rights against them. Moreover, many Member States view IP addresses themselves as personal data, even if the company processing the data cannot connect that IP address to a particular individual – and some deem IP addresses judicial data that can be processed only by government authorities. Again, these interpretations make it all but impossible for right holders to enforce their rights online.

- **Limits on the availability of injunctive relief**

Some Member States have taken the view that an intermediary must itself be liable for infringement in order for a disclosure order or injunction to issue against it. This approach – which does not appear to be consistent with EU law – serves to encourage rights holders to seek to hold intermediaries liable, a non-sensical outcome.
Non-deterrent damages

Because the software industry’s worst problem is piracy by otherwise respectable corporate end-users, the industry uses the civil system to enforce its rights rather than the criminal system. For that reason, perhaps more than any other copyright industries, the software sector relies on damages to deter infringement.

Under both the WTO TRIPS Agreement and EU law, damage awards must both compensate the rights holder and deter future infringements. But in software cases, courts in many markets calculate damages based on the licence fee that the infringer would have paid had it acquired the software lawfully. Still other courts use an assessment that based on what the software provider would have actually received (rather than full retail value) or that applies volume, status, wholesale or other discounts available to lawful users. This actually encourages end-users to pirate, and take the (low) risk of getting caught, safe in the knowledge that at worst, it will cost no more (and possibly less) than had they bought a licence.

Challenges tackling internet piracy

Online piracy poses a serious and immediate threat to software developers, as it does to other copyright-based industries. The Enforcement Directive includes a number of measures – such as the right of information and rules on injunctions – that have helped to tackle internet piracy; at the same time, the underlying liability regime in the Software, Copyright and E-Commerce Directives effectively encourages responsible behaviour by internet intermediaries and does not need reform. But it is clear that the toolbox of enforcement measures to address internet piracy could be expanded. Last year, piracy – including internet piracy – cost the software industry nearly €9 billion in the EU.

In considering new remedies, it is important to strike a balance between effectively deterring piracy, while at the same time ensuring 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.
6. **Recommendations for Reform of the Civil Enforcement Directive**

The BSA appreciates the hard work that the Commission has done over the past few years to gather information and identify practical, balanced solutions that will help reduce piracy and counterfeiting in the EU. Many of the ideas put forward by the Commission in its report on the application of Directive 2004/48/EC would indeed be helpful. The recommendations below focus on the **five reforms** to the Enforcement Directive that the software industry believes will have the greatest impact on reducing software piracy throughout the EU. Again, these recommendations are specific to **copyright-based enforcement**.

- **Deterrent damages**

  **Recovery of the full extent of loss.** Although the Enforcement Directive instructs judicial authorities to consider “all appropriate aspects” in awarding damages, courts in some Member States equate damages with the software providers’ lost profits alone. This calculation does not reflect the full costs of enforcement – including costs of investigating and pursuing an infringement, and related legal fees (which are often reimbursed at less than 50%). This means as a practical matter that a rights holder is worse off after an infringement than before. The Directive should be more explicit in the requiring that the **full costs of enforcement**, including full recovery of expenses and attorneys’ fees, should form part of the damages calculation.

  **Pre-established or multiple damages in appropriate cases.** The Enforcement Directive’s “actual prejudice” and “lump sum” damages rules often do not serve as an adequate deterrent. In practice, under these rules a corporate infringer can make the same payment when it is caught as it would have made if it had purchased a licence in the first instance. Moreover, it can be difficult for courts to assess actual damages given that infringers rarely keep records documenting their theft. A significant number of Member States (including Austria, Belgium, Greece, Czech Republic, Lithuania, Poland, Romania and Slovenia) provide a remedy in the form of **multiple damages** to address these issues; this best practice should be incorporated into the Enforcement Directive, as an option for right holders to elect.

  **Obligation to pay damages survives acquisition of a licence.** Express language in the Enforcement Directive making clear that the purchase of a licence once an infringement has been established **does not extinguish the obligation to pay damages** would be welcomed. Under the law in some Member States, software infringers can simply acquire a licence and
successfully argue that the software provider has been “made whole” as a result and that no damages are due.

**Infringers should not retain economic benefit.** The Directive should also include measures to ensure that infringers are not able to retain any of the economic benefits of the infringement. Currently the Directive permits courts to consider the infringers profits, but does not mandate that these be awarded. As a result, in practice infringers often find themselves economically better off after an infringement than they were before the infringement. To ensure that no economic benefit of an infringement remains with the infringer, unjust enrichment in the amount of the infringer’s benefit should be available as an alternative or cumulative remedy.

**Compensation in criminal proceedings.** Judicial authorities should have the ability in criminal proceedings to assess damages and order the infringer to pay compensation. Such a mechanism would reduce costs both for right holders and for the State. It would also shorten what can otherwise be a long delay in obtaining adequate judicial relief. It would be ideal if right holders had the ability to elect to join their civil claims to criminal proceedings, as some Member States already provide.

- **Improved procedures to secure evidence of software theft**

**Affordable, obtainable and effective civil ex parte search and seizure procedures.** The Enforcement Directive requires that all measures available under the Directive not be unduly complicated or costly. In practice, this general obligation has sometimes been ignored in the context of ex parte searches. The Directive should make express that Member States may not impose expensive procedures or unduly high evidentiary thresholds as a condition of issuance of a search and seizure order. The Directive should also expressly permit the inspection and seizure of licencing information.

**Protection of witness identity in search and seizure applications.** Those reporting piracy should not be required to be named or to provide direct or affidavit evidence of infringement in order for a civil search order to issue. Hearsay evidence provided by hotline operators or qualified lawyers should be sufficient, so long as judges retain the discretion to determine whether the evidence provided is credible and reliable. At a minimum, Article 7 of the Enforcement Directive – which gives Member States the option to take measures to protect witnesses’ identity – should be made mandatory.

**Ability to access subscriber details subject to appropriate safeguards.** Rights holders must be able to process IP addresses, and service providers must be required to provide the true name and address of infringers to copyright owners in civil proceedings. Data protection and intellectual property are
both important rights and must be balanced, but one should not “trump” the other. Consumers will only be willing to utilize the full range of internet-enabled products and services if they have confidence that their personal data is safe. At the same time, data protection is not the only fundamental right that is important to the success of the ICT sector and the internet more broadly. IP is also key to driving and protecting innovation. And like privacy, the fundamental right to property, including intellectual property, is also enshrined in the Charter of Fundamental Rights.

To achieve a balance between these rights, the Enforcement Directive should ensure that rights holders can process IP addresses and can effectively use the right of information in all cases of infringement, subject to appropriate safeguards including disclosure only with a court order and an obligation to maintain the confidentiality of the information disclosed.

- **More effective injunctions**

  Injunctions available against intermediaries regardless of liability. Clarification that – consistent with EU law today – liability is not a condition for an injunction to issue against an online intermediary would be welcomed. Of course, such injunctions must be available only pursuant to a court order and after an opportunity to be heard. Injunctions against intermediaries also should not extend to the imposition of broad mandates for the use of technology filters screening all content or all users. The vast majority of traffic on the internet involves personal and commercial communications that have nothing to do with copyright infringement. Broad-based use of copyright filters to screen these communications is disproportionate and can interfere with users’ legitimate rights and reliance on the internet.

- **An expanded toolbox against internet piracy**

  Persistent and Repeat Infringers. The vast majority of individuals and businesses use software, computers, and the Internet for a myriad of legal and legitimate personal and commercial reasons. But individuals and entities also use the internet to distribute and download illegal content such as software – and often do so not just once or twice, but repeatedly and persistently. Too many people now treat illicit acquisition of copyrighted works online as a routine matter, ignoring the fact that they are engaging in illegal acts.

  Addressing this activity requires measures that (i) effectively deter illicit downloading, uploading, making available and use of content, and at the same time, (ii) 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. In adopting new measures to address internet piracy, due care must be taken to ensure policies meet both considerations.

Consistent with this view, we support effective remedies, including blocking a site and the suspension or termination of Internet service for repeat offenders. We believe that these remedies should be based on evidence and procedures that are proportionate and have sufficient due process guarantees, such as (i) through a claim for breach of contract, i.e., the terms of the contract with the service provider or domain name registry (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 a judicial entity, provided that 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 must have the opportunity to have the order stayed pending appeal to courts.

**Action against intermediaries and others in the value chain.** Infringing copies of computer programs are increasingly distributed by persons operating for-profit websites. The distinguishing feature of as such websites is that they operate for profit and the site has no demonstrable commercially significant purpose or use other than facilitating the unauthorized distribution of infringing or counterfeit goods and services. One option that the Commission may consider is a mechanism that would allow national courts, upon a case initiated by a public official, to order the termination of the operations by such sites by suspending their domain name registrations.

In addition, because these are for profit sites that often require payments through credit cards and other systems for accessing the site and generate additional revenues from advertising, the Commission should consider ways to cut off these sources of payments in appropriate cases. It is important, however, that any such cause of action include safeguards against overbreadth and abuse, such as a limitation that they be initiated solely by public officials and not by private parties, and any measure imposed on either the website or those intermediary doing business with the site should be executed upon an order from a court of law, based on reliable evidence of infringement by that particular site and subject to due process guarantees. The remedies should be narrowly tailored to address the specific adjudicated threat and be least intrusive remedy available taking into the interests of user of the Internet generally and the development of technologies and legitimate offerings.

**FOR FURTHER INFORMATION PLEASE CONTACT THOMAS BOUÉ [thomasb@bsa.org](mailto:thomasb@bsa.org) OR AT +32 (0)2 274 13 15**
These are among the findings of the seventh annual BSA/IDC Global Software Piracy Study, http://portal.bsa.org/globalpiracy2009/studies/09_Piracy_Study_Report_A4_final_111010.pdf, which tracks software piracy rates in 111 economies around the world.

These studies cover piracy of all packaged software that runs on personal computers (PCs), including desktops, laptops and ultra-portables, including netbooks. This includes operating systems, systems software such as databases and security packages, business applications and consumer applications such as games, personal finance and reference software. The studies do not include software that runs on servers or mainframes, however.

This figure is calculated using the blended average price of software in an economy, as sold in retail stores, using volume licences, and as bundled with hardware. Calculating commercial value is intended to help quantify the value of unlicensed software in the market and allows for year over year comparisons of change in the software piracy landscape. It does not mean that eliminating unlicensed software would grow the market by €8.7 billion — not every unlicensed or stolen software product would be replaced by a paid-for version. But BSA/IDC has studied the relative performance of software markets in relation to piracy rates and has found that, in general, as piracy drops the ratio of software sold to hardware sold grows.


For example, see http://www.bsa.org/~/media/297120CD90D1413FA1833C2979A1894B.ashx.