ABOUT ANTI-PIRACY
WHAT IS PIRACY?
ANTI-PIRACY FAQ
ANTI-PIRACY NEWS
PARTICIPATING COMPANIES
CONTACT US
RESOURCES
REPORT PIRACY
EDUCATIONAL MATERIALS
LICENSING SEMINARS
AUDIT SOFTWARE
SOFTWARE RESELLERS
OTHER INFORMATION SOURCES
PROGRAMS
CORPORATE ANTI-PIRACY
INTERNET ANTI-PIRACY

What is Piracy?

SOFTWARE PIRACY BY TOPIC:

- Dimensions of the Piracy Problem
- Consequences of Software Piracy
- Types of Software Piracy
- Shareware & Freeware
- Internet Piracy
- Real-life Examples of Piracy

Download PDF version of this information

CONTENT PIRACY BY TOPIC:

- The Content Infringement Problem
- Content Compliance and Fair Use
- Content Compliance and the First Sale Doctrine
- Types of Content Infringements
- Types of License Violations
- Consequences of Content Infringement
- Corporate Liability
- Remedies for Infringements
- Third-Party Content/License Compliance
- SIIA's Educational Courses and Materials

Download PDF version of this information

What is Software Piracy: The Piracy Problem

Introduction

Over the past several years, advances in computer software have brought us time-saving business programs, educational software that teaches basic skills and sophisticated subjects, graphics programs that have revolutionized the design industry, Internet applications that help connect us with other computer users, and an increasingly complex variety of computer games to entertain us. As the software industry grows, everyone stands to benefit.

Compared to literature, music and movies, computer software is a relatively new form of intellectual property. Nevertheless, software is protected under the very same laws that govern music, literature, movies and other copyrighted content. Copying software illegally is not any different than illegally copying any of these forms of intellectual property -- and the punishments for doing so are equally harsh.

All software comes with a license agreement that specifically states the terms and conditions under which the software may be legally used. Licenses vary from program to program and may authorize as few as one computer or individual to use the software or as many as several hundred network users to share the application across the system. It is important to read and understand the license accompanying the application to ensure that you have enough legal copies of the software for your organization's needs. Making additional copies, or loading the software onto more than one machine, may violate copyright law and be considered piracy.

Unfortunately, there are many people who, either ignorantly or deliberately, engage in software piracy. Whenever you use a piece of software that is unlicensed, you are depriving software companies of their earnings. More importantly, you are depriving the creative teams who have developed the software (e.g., programmers, writers, graphic artists) of compensation for the thousands of hours they have spent working on a particular program.

In a very real sense, software piracy adversely affects the world economy by diverting money that stimulates further product development. Piracy particularly affects the United States, which currently provides approximately 80 percent of the world's software.

» top

The Dimensions of the Piracy Problem

On average, the software industry loses about US$11 to US$12 billion in revenue to software piracy

annually. Of the billions of dollars lost to piracy, a little less than half comes from Asia, where China and Indonesia are the biggest offenders. Piracy is also a big problem in Western Europe, where piracy losses annually range from $2.5 and $3 billion dollars. Piracy rates are quite high in Latin America and in Central Europe, but their software markets are so much smaller that the dollar losses are considerably lower.

About $2 billion in piracy loses come from North America. The piracy rate in the United States has been relatively constant at about 25% over the past few years, which is the lowest rate of any country. This means that one in every four copies of business application software is used illegally. The large dollar amount in losses is attributable more to the fact that there are so many computers and computer users in the United States than to a high piracy rate when compared with the rest of the world.

SIIA works with the U.S government, foreign governments and international organizations around the world to protect intellectual property in international markets. As an example, the Special 301 provision of the Omnibus Trade and Competitiveness Act of 1988 authorizes the U.S. Trade Representative (USTR) to prepare lists of countries that do not provide effective protection of intellectual property rights or deny fair and equitable market access to U.S. firms relying on intellectual property protection. The lists inform the administration about countries considered priority targets for future trade negotiations or possible trade sanctions.

There is no evidence that software piracy will be eliminated anytime in the foreseeable future. SIIA acknowledges that many countries have made efforts to improve intellectual property protection for computer software. However, the high rates of software piracy and dramatic losses to U.S. software developers demonstrate that much remains to be done. There is evidence that continuing education and enforcement efforts can - and do - make a difference. In the United States, for example, the level of piracy has been reduced from 48 percent in 1989 to 25 percent in 2002.

We have learned that reducing software piracy rates requires the combined efforts of policy-makers, software developers and publishers, businesses, journalists and concerned individuals. As long as software piracy exists, there will be fewer jobs, less research and development, increased costs and lower standards of living.

» top

Consequences of Software Piracy

The losses suffered through software piracy directly affect the profitability of the software industry. Because of the money lost to pirates, publishers have fewer resources to devote to research and development of new products, have less revenue to justify lowering software prices and are forced to pass these costs on to their customers. Consequently, software publishers, developers, and vendors are taking serious actions to protect their revenues.

Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, your organization forfeits some practical benefits as well. Those who use pirate software:

- Increase the chances that the software will not function correctly or will fail completely;
- Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
- Have no warranty to protect themselves;
- Increase their risk of exposure to a debilitating virus that can destroy valuable data;
- May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
- Are subject to significant fines for copyright infringement; and
- Risk potential negative publicity and public and private embarrassment.

It is also worth noting that the use of pirated software also drives up the costs for legitimate users - which gives legitimate users all the more reason to help SIIA fight piracy by reporting to us those companies that are not "playing by the rules."

» top

Types of Software Piracy

Many computer users have found themselves caught in the piracy trap, unaware they were doing anything illegal. To avoid such unpleasant surprises, it may be helpful to know the ten basic ways one can

intentionally or unintentionally pirate software:

1. Softlifting
Softlifting occurs when a person purchases a single licensed copy of a software program and loads it on several machines, in violation of the terms of the license agreement. Typical examples of softlifting include, "sharing" software with friends and co-workers and installing software on home/laptop computers if not allowed to do so by the license. In the corporate environment, softlifting is the most prevalent type of software piracy - and perhaps, the easiest to catch.

2. Unrestricted Client Access
Unrestricted client access piracy occurs when a copy of a software program is copied onto an organization's servers and the organization's network "clients" are allowed to freely access the software in violation of the terms of the license agreement. This is a violation when the organization has a "single instance" license that permits installation of the software onto a single computer, rather than a client-server license that allows concurrent server-based network access to the software. A violation also occurs when the organization has a client-server license, the organization is not enforcing user restrictions outlined in the lciense. For instance, when the license places a restriction on the number of concurrent users that are allowed access to that program and the organization is not enforcing that number. Unrestricted client access piracy is similar to softlifting, in that it results in more employees having access to a particular program than is permitted under the license for that software. Unlike softlifting though, unrestricted client access piracy occurs when the software is loaded onto a company's server - not on individual machines - and clients are permitted to access the server-based software application through the organization's network.

3. Hard-disk Loading
Hard-disk loading occurs when an individual or company sells computers preloaded with illegal copies of software. Often this is done by the vendor as an incentive to buy certain hardware. If you buy or rent computers with preloaded software, your purchase documentation and contract with the vendor must specify which software is preloaded and that these are legal, licensed copies. If it does not and the vendor is unwilling to supply you with the proper documentation, do not deal with that vendor. SIIA offers assistance in finding qualified vendors through our Certified Software Reseller Program

4. OEM Piracy/Unbundling
Some software, known as OEM (original equipment manufacturer) software, is only legally sold with specified hardware. When these programs are copied and sold separately from the hardware, this is a violation of the distribution contract between the vendor and the software publisher. Similarly, the term "unbundling" refers to the act of selling software separately that is legally sold only when bundled with another package. Software programs that are marked "not for resale" are often bundled applications.

5. Commercial Use of Noncommercial Software
Using educational or other commercial-use-restricted software in violation of the software license is a form of software piracy. Software companies will often market special non-commercial software aimed at a particular audience. For example, many software companies sell educational versions of their software to public schools, universities and other educational institutions. The price of this software is often greatly reduced by the publisher in recognition of the educational nature of the institutions. Acquiring and using noncommercial software hurts not only the software publisher, but also the institution that was the intended recipient of the software.

6. Counterfeiting
Counterfeiting is the duplication and sale of unauthorized copies of software in such a manner as to try to pass off the illegal copy as if it were a legitimate copy produced or authorized by the legal publisher. Much of the software offered for bargain sale at non-trade computer shows is counterfeit software. SIIA estimates that at least 50% of the software sales that take place at computer shows throughout the United States involve counterfeit software.

7. CD-R Piracy
CD-R piracy is the illegal copying of software using CD-R recording technology. This form of piracy occurs when a person obtains a copy of a software program and makes a copy or copies and re-distributes them to friends or for re-sale. Although there is some overlap between CD-R piracy and counterfeiting, with CD-R piracy there may be no attempt to try to pass off the illegal copy as a legitimate copy - it may have hand-written labels and no documentation at all. With CD recording equipment becoming relatively inexpensive, the software industry is being plagued by this new form of end-user piracy. Just a few years ago, so-called "compilation CDs" (illegal CD-ROMs containing many different software applications) were

selling for $400-$500. With CD-R's becoming more available, the price has dropped to $20 -- making illegal software available to a greater number of people.

8. Internet Piracy
Internet piracy is the uploading of commercial software (i.e., software that is not freeware or public domain) on to the Internet for anyone to copy or copying commercial software from any of these services. Internet piracy also includes making available or offering for sale pirated software over the Internet. Examples of this include the offering of software through an auction site, IM, IRC or a warez site. Incidences of Internet piracy have risen exponentially over the last few years. Internet piracy is discussed in greater detail below.

9. Manufacturing Plant Sale of Overruns and 'Scraps'
Software publishers routinely authorize CD manufacturing plants to produce copies of their software onto CD-ROM so that they can distribute these CD-ROMs to their authorized vendors for resale to the public. Plant piracy occurs when the plant produces more copies of the software than it was authorized to make, and then resells these unauthorized overruns. Piracy also occurs when the plant is ordered by the publisher to destroy any CDs not distributed to its vendors, but the plant, in violation of these orders, resells those CDs that were intended to be scrapped. While most plants appear to be compliant, and there are compliance procedures in place, there have been several instances of these forms of piracy.

10. Renting

Renting software for temporary use, like you would a movie, was made illegal in the United States by the Software Rental Amendments Act of 1990 and in Canada by a 1993 amendment to the Copyright Act. As a result, rental of software is rare.

The ten types of piracy identified above are not mutually exclusive. There is often overlap between one type of piracy and another. For instance, SIIA has come across numerous instances of OEM counterfeiting. This occurs when OEM software is unbundled in order to be re-sold, and not only does the pirate sell the OEM software, but he also makes numerous illegal copies of the OEM software and sells them as counterfeits.

» top

Shareware and Freeware

Many users become understandably confused between shareware, freeware and public domain software. These are all ways of marketing software, and have nothing to do with the actual type of software being distributed.

Shareware is "copyrighted software which is distributed for the purposes of testing and review, subject to the condition that payment to the copyright owner is required after a person who has secured a copy decides to use the software." This definition is contained in Copyright Rules & Regulations, 37 CFR 201.26. (Shareware is also sometimes referred to as try-before-you-buy software.)

Freeware is software that is distributed in a way that allows individuals and non-profit organizations to use the software at no charge. The software usually comes with a license agreement that prohibits the software from being sold, rented, or otherwise distributed in a for-profit manner.

Public domain software is "software which has been publicly distributed with an explicit disclaimer of copyright protection by the copyright owner." 37 CFR 201.26.

Lastly there is another category, often referred to as crippleware that is a hybrid between shareware and freeware. Crippleware allows a person to use the software for free. If the individual likes the software, he/she can then pay to receive a code that activates some "crippled" features, like the ability to print or to use advanced functions.

Both shareware and freeware are often accompanied by a license agreement that sets forth the terms and conditions of use of that product. Though shareware is commercial software, many shareware authors use electronic distribution as part of their distribution system. Loading shareware onto or downloading shareware from the Internet does not constitute piracy. However, shareware may be considered pirated if it is not registered and paid for before the expiration of the application's specified trial period.

While there is no money exchanged to obtain a copy of freeware and it can usually be downloaded without liability, freeware can still be considered to be pirated if it is used in a manner that violates an accompanying agreement. For example, if the freeware license contains a restriction on selling the freeware and someone includes the freeware on a compilation CD of freeware programs and sells the program, the freeware has been pirated because the license has been violated.

Unlike shareware or freeware, there are no copyright restrictions on a piece of public domain software. Therefore, public domain software will usually not be subject to a license agreement and the user of public domain software is generally free to use the software as they desire, with no restriction.

» top

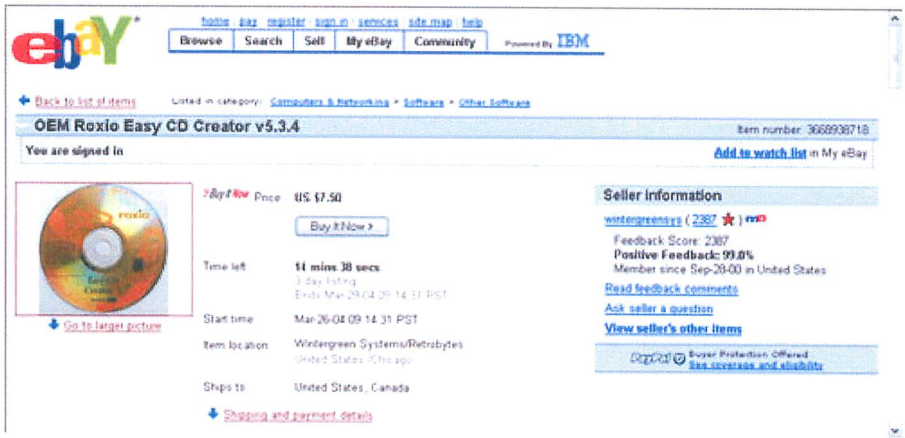
Internet Piracy

Internet piracy is the most rapidly expanding type of piracy and the most difficult form to combat. Internet piracy takes many forms:

- Auction Site Piracy;
- Bulletin Board Services & News group piracy;
- FTP Sites;
- Warez;
- Peer-to-Peer;
- Cracks/Serial Numbers sites; and
- Internet Relay Chat.

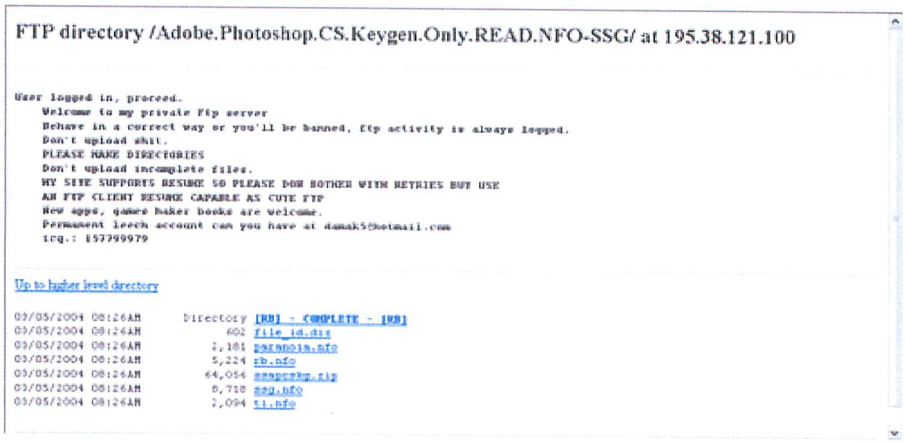
Auction site piracy occurs when the seller burns software onto CD-ROMs, offers the software for sale in an online auction. The auctioneer will often data-mine the names and e-mails of losing bidders and contact those bidders in an attempt to sell additional copies. SIIA has a good working relationship with most major auction sites and is able to remove pirate auctions shortly after their being posted.

One example of a pirate auction is provided below:

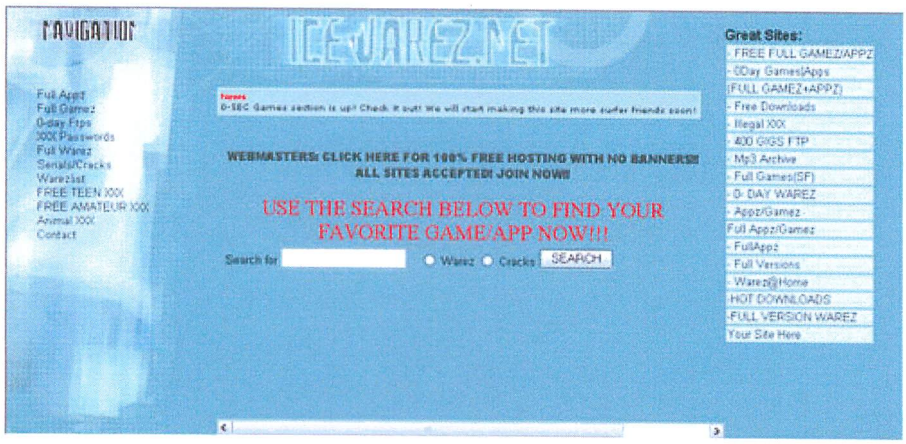


FTP allows one to upload files and download files to a site. Software pirates who transfer programs to one another commonly use FTP sites because it is efficient for transferring large files and most FTP servers support some form of anonymous login.

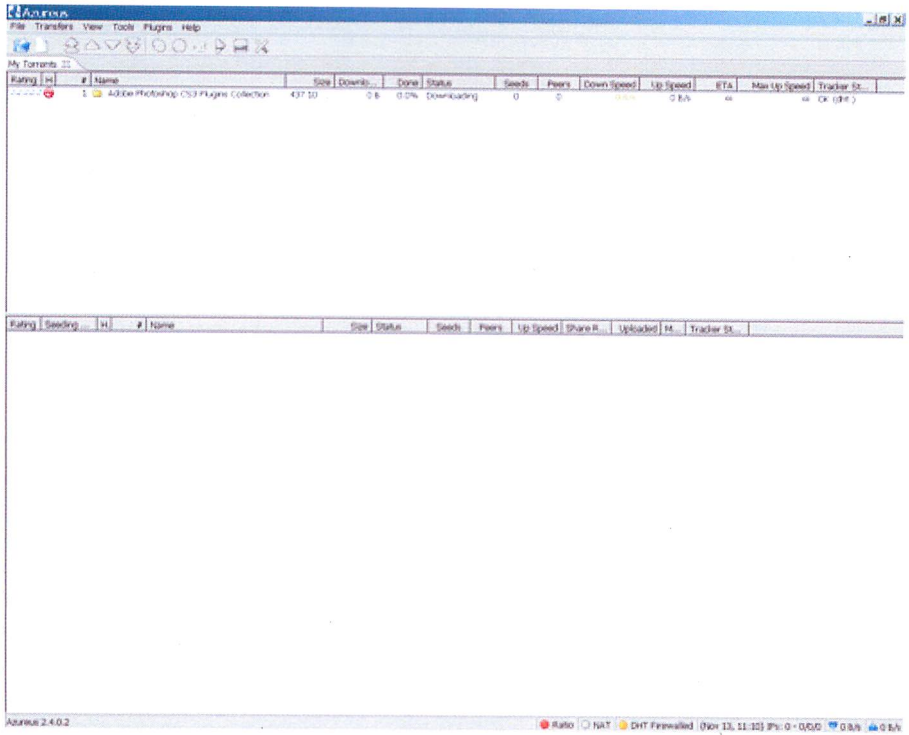
A sample FTP pirate site follows:



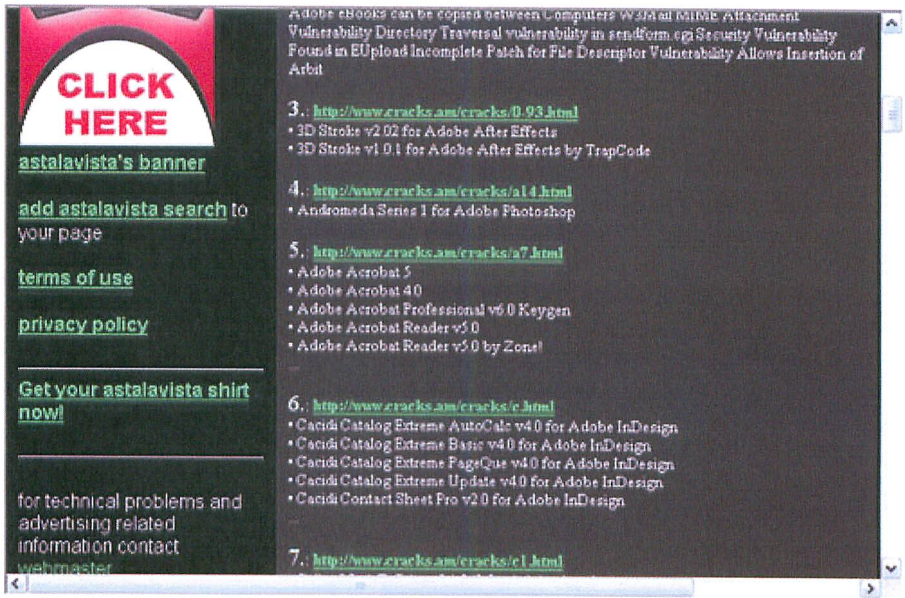
Web sites, often called Warez Sites allow the downloading of software -- generally free of charge -- from the Web.



Peer-to-Peer [P2P] technologies allow users to communicate in real-time and transfer files to each other. Because of the distributed and often anonymous nature of P2P sites, they are widely used for distribution of unauthorized software and content. P2P networks are also popular because they are basically "one stop shopping" where a user can find just about anything they are looking for - music, software, movies. Of all the forms of piracy discussed, P2P piracy is the most difficult to stop. The example below is from the P2P network Gnutella. For more information about P2P piracy, contact SIIA about obtaining a copy of its white paper on P2P piracy.



Lastly, another form of piracy that is prevalent on the Internet is the use of cracks, key-generators and patches. Cracks and patches are small files that circumvent copyright protection -- either technical access or copy restrictions -- by altering the source code. A key-gen or key generator is an application that uses the serial number or CD key-generating algorithm to create fake, yet still valid, serial numbers and CD keys. A site that provides these technologies looks like this:



» top

Taking Action Against the Pirates: Real-Life Examples of Piracy

The following examples illustrate the various scenarios under which piracy occur. These real-life stories depict how software piracy affects the industry as a whole.

End User Piracy at Work and at Home

John was the head of a new division of End Corp., a small company with about 45 PCs. John was brought in to reduce expenses for the company and decided to cut corners on his software licenses. John only ever authorized the purchase of one copy of each program. His rationale was, "we bought it, and we can do what we want to do with it." John's plan seemed to work until the day that one of his employees called the software publisher for technical support for the pirated software. The publisher in turn called SIIA. End Corp., facing the possibility of a copyright infringement lawsuit, agreed to pay a fine of $70,000 for the illegal software. In addition, End Corp. was required to destroy all illegal software and re-purchase what it needed to be legal. The total cost to End Corp. for failing to comply with the copyright law was in excess of $150,000.

The unauthorized copying of personal computer software for use in the office or at home or sharing of software among friends is the most pervasive form of piracy encountered abroad and in the United States. SIIA estimates this type of piracy is responsible for more than half the total revenues lost by the industry.

Counterfeiting in Far East and Your Own Backyard

Not far from the bustling tourist areas in Hong Kong, there is a shopping center called the Golden Arcade where dozens of shops sell hundreds of CD-ROM titles for as little as US$10 each. At a quick glance, they appear legitimate. However, they are actually counterfeits.

Counterfeit software is not limited to the Far East. In the United States, some software distributors are apparently selling counterfeit software. Computer shows are also notorious for being rampant with counterfeit software. SIIA has obtained preliminary injunctions against software distributors who have sold counterfeit educational and entertainment titles through organized computer shows.

Counterfeits can be identified by close inspection of the discs, documentation (if any) and packaging. Poorly reproduced color, misplaced trademark logos, missing documentation and typographical errors are warnings the software may be counterfeit. For software publishers, the cost of counterfeiting is measured in lost sales and customer disappointment. For end users who buy counterfeits, there is a lack of technical support and documentation, the risk of viruses and the likelihood of incompatible or nonfunctioning software.

Piracy for Profit and Reputation

A college in the Midwest noticed during routine Web server maintenance that it was running at 85 percent of total capacity. Just the semester before, the server had never exceeded 25 percent. Upon investigation of the material on the site, the site operators noticed significant "warez" activity. Warez is the word commonly associated with the transfer of pirated software across the Internet. The server operators were able to determine that two students created these warez pages on the colleges server. The college made a backup of the warez site and contacted SIIA for assistance. SIIA helped the college update its policies and procedures, but more importantly, SIIA worked cooperatively with the college in pursuing the two students. In lieu of filing suit against the students, SIIA agreed to settle if they would agree to turn over their computers to SIIA, provide information as to where they received the illegal software and agree to perform community service. The college also sanctioned the students. Once the sites operated by the students were removed, the server again ran at 25 percent capacity. These two warez sites alone occupied 60 percent of the server's capacity.

Even if software pirates are not making a profit from the software, as in the example above, it is still illegal. The rules protecting software outside the Internet continue to apply in cyberspace. Copyright and other intellectual property laws protect software created, posted and traded on the Internet. Internet service providers (ISPs) or Internet access providers (IAPs) may be liable for copyright infringement if their users illegally copy or distribute software, through downloading, uploading or transmitting software files without the copyright owners' authorization and they fail to avail themselves of the "safe harbor" provisions of the Digital Millennium Copyright Act.

Web Pirates Punished in 2006

This year, judges handed down the toughest sentences for software piracy ever seen in the United States. Two major software pirates were charged with criminal copyright infringement for their involvement in the manufacture and widespread distribution of pirated software. Both were initially investigated by SIIA and later referred to the Federal Bureau of Investigation and U.S. Customs.

On August 25, 2006, Danny Ferrar, owner and operator of BuysUSA. com, a massive for-profit software piracy website, was sentenced in federal court to six years in prison. Beginning in late 2002 and continuing until its shutdown by the FBI on October 19, 2005, Ferrar and his co-conspirators had operated the www. BUYSUSA.com website, which sold pirate copies of Adobe, Autodesk and Macromedia software at prices substantially below the suggested retail price.

During the time of its operation, BUYSUSA.com illegally sold more than $4.1 million of copyrighted software, resulting in nearly $20 million in losses to the software owners. At the time of sentencing, this was the longest prison term ever handed down in a software piracy case. Ferrar was also ordered to forfeit the proceeds of his illegal conduct, pay restitution of more than $4.1 million, and perform 50 hours of community service.

The asset forfeiture included a Cessna 152; a Cessna 172RG; a Model TS-11 ISKRA aircraft; a RotorWay International helicopter; a 1992 Lamborghini; a 2005 Hummer; a 2002 Chevrolet Corvette; two 2005 Chevrolet Corvettes; a 2005 Lincoln Navigator; an IGATE G500 LE Flight Simulator; a 1984 twenty-eight foot Marinette hardtop express boat; and an ambulance - all of which Ferrar had purchased with the profits from his illegal site. Ferrar also agreed to surrender the proceeds of sales of two fire trucks that were also bought with his illegal proceeds.

Less than a month later, Ferrar's record prison term was shattered when, on September 8, 2006, Nathan Peterson, owner and operator of iBackups was sentenced to 87 months (7 years, 3 months) in prison for his crimes. Peterson had previously pled guilty to two counts of criminal copyright infringement. In addition to his prison term, Peterson was required to pay restitution of $5,402,448 and a $250,000 punitive fee.

Working on behalf of its members, SIIA first alerted the FBI of possible software piracy by Peterson in 2003 and subsequently worked with investigators and prosecutors to assure that Peterson's operation was stopped and that he was properly punished. iBackups sold pirated software over the Internet, claiming it was "backup software" - legal copies of software to be used by the software licensee for backup in case of system crashes. It is, however, illegal to resell such copies.

As SIIA has emphasized in the past, software pirates are often not just intellectual property thieves, but are involved in other illegal activities. This position was further bolstered by the fact that while on bond in this case Peterson was convicted in Los Angeles for the sale of six handguns and an illegal assault weapon to an alleged heroin dealer.

» top

The Content Infringement Problem

Introduction

Theft is an unfortunate problem that every industry confronts in some form, whether burglary, robbery, counterfeiting, shoplifting, embezzlement or others. Businesses that rely on copyright to protect their products and services - such as software companies, publishers and other information providers - are no different. Copyright is a form of property and copyright infringement is theft. "Infringement" means unauthorized use of material protected by copyright, patent or trademark law. Blatant infringement is also often referred to as "piracy".

While computers and the Internet have provided many new efficiencies and positive changes in business and in society as a whole, they have given rise to new risks and possibilities for copyright theft, particularly for the industries that create and distribute content. While "content" theoretically could refer to anything that customers read, watch, or listen to - such as films, sound recordings (i.e., music), software, electronic publications, databases - here, the term refers to published text (protected under the Copyright Act as "literary works") or information such as databases. Put another way, content is a work expressed in words, numbers or other verbal or numerical symbols, such as in newspapers, magazines, databases, industry reports, newsletters, and web pages. Because digital technology makes it so easy to make copies quickly and perfectly -- and distribute them instantaneously to large numbers of people -- it can be more tempting than ever to violate the copyright laws.

It takes just a few simple clicks of a mouse to copy and redistribute digital content. The act is so easy and such a seamless part of using the Internet (and not always illegal) that anyone who has ever used e-mail or

the Internet has undoubtedly done it. We all forward e-mails, we print out web pages and we download files from the Internet. The result is flawless copies of the original, equally flawless copies of the copies, and so on. It is this copying and distribution capability that makes digital content so easy to work with - and so difficult to protect.

While most people generally are law-abiding by nature, the copying of content has become so widespread that people who would never consider stealing a book or magazine from a store may not hesitate to use their computers to commit a similar violation -- breaking the copyright laws or breaching their license agreements with content providers. In some cases, the violation may even be inadvertent. The law, however, does not excuse inadvertent or uninformed copyright infringement, and (as will be discussed later) imposes significant consequences. The penalties are particularly severe for those who "willfully" infringe, meaning that they knew, or reasonably should have known, that they were violating the law.

Anyone who uses, copies, distributes, or displays (in whole or in part) someone else's copyrighted content without authorization may be violating the owner's copyright rights. Such violations can result in a lawsuit and money damages, and in some cases, criminal prosecution with jail time.

When someone infringes a copyright, the copyright holder effectively is deprived of income-either directly or indirectly-that could be put to use to develop new or better content. Every year the content industries lose millions - if not billions - of dollars to copyright infringement, depriving the public of new creative works, costing industry jobs and hurting the economic growth of this country. These consequences would be substantially limited if users took just a little time to understand and respect the law and the cumulative adverse effect of their actions.

» top

Content Compliance and Fair Use

"Fair use" is a limited exception that allows the use of a copyrighted work in particular circumstances without the need to pay the copyright owner or get the owner's permission. Examples of fair use might be use of a work in a limited classroom setting, in a parody, or as part of a news report or commentary. It is a fact-based concept and a court considering it will weigh various factors, including:

- **The purpose and character of the use.** Fair use is less likely to be found when the use is for commercial purposes and more likely where the use is for such purposes as scholarship or criticism. Also, fair use is less likely where the use is similar to that of the original work (e.g. when one newspaper reprints a story from another paper or magazine) and more likely to be found where the new work is highly "transformative," in the sense that a new and different work is created -for example, where a news photo is incorporated into an artistic collage.

- **The nature of the copyrighted work.** Fair use is less likely to be found when the work is highly creative, as opposed to factual, in nature.

- **The amount and substantiality of the portion used in relation to the copyrighted work as a whole.** Copying all, or most of, a work is less likely to be a fair use than taking only a small part of it. Both the amount taken and its importance to the original (e.g., whether the portion taken represents the most valuable part of the work) are considered.

- **The effect of the use upon the potential market for, or value of, the copyrighted work.** If the use in question harms a market for the copyrighted work - whether it's an actual market or a potential one - fair use is unlikely. For example, if the copyright holder generally earns revenue by licensing the use of the work, fair use will probably not apply to someone who uses the work in the same way without paying for it. It is not unusual for this factor to be given more weight by a court than the other three factors.

While fair use is one of the most frequently-discussed and recognized phrases in copyright law, it is a narrow legal concept and is often misunderstood, particularly as it applies to business uses. Assuming that an unauthorized copy is "fair use" because it is "no big deal" or "only one copy" is usually a mistake. Employees using content from third parties should consult an attorney before engaging in any unauthorized copying or distribution of copies on the belief that the actions might be fair use.

While there is no "rule of thumb" for determining with 100% certainty whether a court will find any particular copying to be "fair use," often it will be obvious that a proposed use probably will not qualify as

fair use. Such cases would include where all, or substantially all, of a work is copied in a business setting, or where the copying potentially competes with the original work (by removing the need to buy a licensed or copy of the work).

Mistakenly assuming -- or hoping -- that copying is fair use can lead to an expensive lawsuit and significant penalties against you or your company.

» top

Content Compliance and the First Sale Doctrine

If a copy of a copyrighted work is purchased, the purchaser has the right to transfer that copy under what is known as the "First Sale Doctrine." This doctrine allows the copyright owner to control the initial sale or distribution of the copy to the public, but once the particular copy is sold, the copyright owner has no right to control the subsequent resale or transfer of that copy. For example, a music CD or movie DVD can be purchased at Best Buy and then resold at a garage sale.

Significantly though, if the content is obtained through a license - as is the case for most electronic content -- the first sale doctrine does not apply because the user does not own a copy of the work, he only has access to it through the license. In those cases, the user should consult the license agreement for the content to determine whether the copy may be re-distributed. Also, the First Sale Doctrine applies only to copies that were lawfully made or obtained. If the content was a pirated copy, the purchaser does not have the right to subsequently transfer or sell that copy.

» top

Types of Content Infringements

Many people who infringe copyright may be unaware they are doing anything illegal. Some illegal practices are so widespread that most people don't even think about whether or not they are legal. Therefore, we have built a list of some of the most common ways in which content is infringed, focusing on those methods principally employed by business users.

Photocopying
Photocopiers have been around a long time (at least in comparison to the Internet), and people are accustomed to using them for all sorts of tasks, some of which may violate copyright. Remember that a copy is a copy and the exclusive right to copy belongs to the copyright holder. Even if you have legally purchased a copy of a work, that does not give you the right to make photocopies of it. Before you head to the copy room, ask yourself where your original document came from and whether you have permission from the copyright holder to make another one.

Printing
While users don't normally think of sending a file to a printer as making a copy in the same way as using a photocopier does, the same principles apply. The only difference is that in one case the original copy is printed on paper and in the other it's a digital file. Many content publishers place limits on the number of times a particular work may be printed under the usage license. Other content, such as a publicly-accessible web page, is usually safe to print. Be sure to check the limitations on the content you're working with to make sure that such a normal, mundane process as sending it to a printer does not violate someone's copyright.

Scanning
While photocopying and printing can create an unauthorized physical copy of a document, scanning can create an unauthorized digital copy. You don't have to be able to hold the copy in your hand in order to violate the author's exclusive right to copy. As with photocopying and printing, before going to the scanner you should always ask yourself whether you have the right to make a digital copy of someone else's document.

E-mail
There are various ways to infringe copyright via e-mail. Any e-mail you receive from another person is their copyrighted work, so forwarding it to someone else or printing it without the author's permission technically violates the author's exclusive rights. E-mail is a fast and easy way to distribute information and therefore is a fast and easy way to violate a copyright owner's right to distribution. This could be done by attaching a copy-even a legally obtained copy-of a file to an e-mail, or even by copying and pasting text into

the body of an e-mail. Probably all of us have infringed someone's copyright through e-mail, but one should be particularly careful in the case of proprietary information -- information that is obtained only through paid subscription. Pay particular attention to copyright notices and warnings on e-mails you receive and on any attachments you send.

Networking

A user can infringe copyright by posting content on a public or private network for others to access. If the content is offered only on a subscription basis, and is meant only for one person, then placing the content on a network has the same effect as sharing passwords because it gives access to more people than are licensed. But even more specifically, placing an item on a network for others to access can be tantamount to distribution, in violation of the exclusive right to distribution held by the copyright owner. This holds true even if the network is not a public one. Sharing the content even with your own co-workers is still a violation of copyright. Indeed, most of the content infringement that goes on in the workplace is unauthorized intra-office sharing.

File Sharing

File sharing, a category similar to, but more specific than networking, is the uploading or downloading of a content file (i.e. a Word document, a PDF file, or an e-book) onto or off of an online service where anyone can copy it. File sharing is often conducted through peer-to-peer sites, many of which specialize in music files, but include other content as well. Another place where file sharing is rampant is on FTP sites, which allow users to upload and download files to and from a site. Infringers commonly use FTP sites because they are efficient for transferring large files and most FTP servers support some form of anonymous login.

Piracy and Counterfeiting

If you make a copy of someone else's content and sell it, whether in hard copy form, on an auction website, or in any other way, you are pirating the copyright owner's rights to copy and sell the content. If the infringer tries to pass off the pirated copy as if it were a legitimate copy produced or authorized by the copyright holder, the activity is known as counterfeiting.

» top

Types of License Violations

A type of license violation is the sharing of passwords. Often, when a publisher sells subscriptions to proprietary content, it is protected by a password feature. When a user shares his password with another person who has not paid to view the content, he is at the very least violating the contract under which the password was supplied, and is possibly also violating the copyright right to distribution. Publishers depend on selling multiple subscriptions in order to pay for the content you receive. Unless your license specifically states otherwise, you should have a separate subscription-and therefore a separate password-for each person who will be accessing the content. Sharing passwords is just as wrong as sharing copies.

Publishers often include contracts with many copyright licenses that specify what the user can and cannot do with the content. Subscription agreements often not only prevent copying, but also might include other, non-copyright-related restrictions as well.

A license contract might prohibit subscribers from disclosing sensitive information contained in the copyrighted work in any way. In those cases, even if the user does not infringe the owner's copyright, the user can still be liable to the copyright owner under a breach of contract action. Such contracts put users on notice about use restrictions under the copyright license, so that the owner can use it in a potential lawsuit to establish 'willfulness', and thereby to increase the damages award.

» top

Consequences of Content Infringement

The losses suffered through content infringement directly affect the profitability of various industries. Because of the money lost to infringers, publishers and other content providers have fewer resources to devote to the research, writing and development of new works and have less revenue to justify lowering subscription prices or offering content for free.

Copyright infringement obviously hurts the copyright owners, but it's also risky business for consumers. Even setting aside the risk of litigation and civil or criminal penalties, there are common-sense business reasons to avoid infringement. Following are just a few of the practical reasons why the user benefits from obeying the copyright laws.

- Infringement drives up the cost publishers must charge to all law-abiding consumers.
- If the content you are using has been illegally copied and distributed, you will not be able to contact the copyright owner with questions or problems.
- Digital infringers increase their risk of catching a debilitating virus that can destroy valuable data.
- Infringers may find that the content is actually an outdated or incorrect version. .
- Infringers risk potential negative publicity and public and private embarrassment.

» top

Corporate Liability for Infringement of Copyrighted Content

Any organization or individual that violates any of the exclusive rights of a copyright holder, whether by copying, distributing, performing, displaying or adapting the work without authorization, is legally an infringer. Ignorance of the law will not excuse the violation -- the organization will be liable, whether they knew their acts constituted infringement or not.

Employers are typically responsible-legally and financially-for the misdeeds of their employees on the job, whether they are copyright infringement, discrimination or sexual harassment.

In addition, corporate officers and members of the board of directors cannot always hide behind the corporate veil. For example, an officer of an infringing corporation may be personally liable for infringement done by someone in his company if he:

- uses employees to carry out deliberate infringement;
- personally participates in the infringement;
- determines the policies that result in infringement; or
- derives a financial benefit from the infringement.

Every person who participates in an organization's copyright infringement may be "jointly and severally liable" for the actions, meaning that each defendant can be required to compensate the copyright owner for the full damages and legal fees assessed, up to the entire amount assessed. As discussed below, these costs can be substantial even for infringement that does not cause great economic loss. That liability extends far beyond the individual who may have made the original copy of the content.

» top

Remedies for Corporate Content Infringements

Because Congress has understood copyright infringement to be a significant problem that severely damages the U.S. economy, the fines and penalties under the Copyright Act are among the most severe in U.S. law. The remedies are designed to provide substantial deterrence to the infringer and others, in order to limit or prevent future copyright infringement, as well as penalize the infringer for the past conduct, and fully compensate the aggrieved copyright owner and recoup any gain reaped by the infringer.

When someone infringes another person's copyright, the Copyright Act allows the copyright owner to seek several types of damages. First, the copyright owner may elect to recover the actual amount of money he lost as a result of the infringement, along with any additional profits made by the infringer. This is known as "actual damages." Actual damages are intended to put the parties back in the financial position they would have been in had there been no infringement.

Alternatively the copyright owner may elect to recover so-called "statutory damages." To be eligible for this option, the copyrighted work must have been registered with the U.S. Copyright Office before the violation began or, in the case of a published work, within three months of publication. Statutory damages are based on the number of works that were infringed (as opposed to the number of infringing acts, or the number of copies made).

A jury is allowed to set statutory damages for each infringed work in an amount that seems just, taking

into account all of the circumstances as well as the per-work range of awards specified by the statute. If the infringement was not willful, the statutory damages must fall between $750 and $30,000 for each infringed work. If the infringement was innocent because the infringer had no reasonable way to know it was infringing, the damages can be reduced to not less than $200 per work. However, an infringement cannot be innocent when the work contains a copyright notice, as most copyrighted works do. For willful infringement, the amount may be as much as $150,000 per infringed work. Inclusion of a copyright notice on a work is often sufficient to permit a jury to find that infringement was willful.

Where a number of works are infringed by a given course of conduct (e.g., regularly making copies of periodicals or downloading files from the Internet), these penalties can quickly add up to very large liability. Infringement involving digital works and digital networks has, therefore, yielded some striking statutory damage awards. For example, in one court case, *Lowry's Reports, Inc. v. Legg Mason, Inc.*, 302 F.Supp.2d 455 (D. Md. 2004), a financial institution's practice of e-mailing and posting on its internal network each issue of a copyrighted financial newsletter resulted in the jury assessing more than 200 statutory damage awards totaling nearly $20 million.

In addition to damages, the court may order the defendant to pay the prevailing copyright owner's attorneys' fees and expenses incurred in bringing the infringement action. Prevailing defendants also may recover their attorneys' fees where the court considers it appropriate.

In addition to the monetary consequences, the content owner may also ask the court to temporarily or permanently stop the infringer from further infringement. To do so, the court will issue an injunction, which either prohibits the defendant from performing some infringing act or instructs the defendant to take some action that will undo the infringement.

» top

Managing Third-Party Content and License Compliance Within An Organization

A content management plan provides a way for management to approve and support policies that may seem restrictive, but are in the best interests of the organization. A carefully designed and implemented content management plan is crucial to establishing a copyright-friendly culture and will reduce uncertainty within an organization.

These are some of the essential steps in developing a content management plan:

- Determining where and how content is used within the organization;
- Reviewing the current content license use and compliance policy;
- Evaluating current content acquisition and management practices;
- Determining the level of management support;
- Establishing a formal organization content management plan;
- Educating and reminding users about the organization's content use policies;
- Creating an organization-wide content management team, and assigning responsibility for copyright compliance to a designated individual in each department;
- Providing the necessary budget and access so that all employees can use the publications necessary for their work;
- Establishing a company culture of compliance, including regular self-assessments and performance reviews, together with rewards and penalties for compliance and non-compliance.

These, and many other steps, are discussed in great detail in SIIA's Certified Content Rights Management (CCRM) seminars taught throughout the country. It's not possible to explain each of these steps in detail on the website, since organizations all operate differently and what works for one may not work well for another. The size of the organization and the diversity of the content it uses regularly will be factors in

determining how long it will take and how easy it will be to develop a satisfactory plan. Each organization will have to identify which components best suit the organization's goals and customize its plan accordingly.

Organizations must be proactive in identifying and abating copyright infringement risks. Once a claim has been brought, it is too late to avoid the consequences, though responsible cooperation can limit the downside.

» top

SIIA's Content Compliance Educational Courses and Materials

Education is a significant component of SIIA's content compliance efforts. SIIA's copyright and compliance education programs have been widely recognized as an effective force in combating infringement. SIIA has developed, published and distributed numerous educational videos, publications, posters and other educational materials to teach companies, students, children, educators, consumers and the public in general about the "Do's and Don'ts" of content infringement and compliance.

SIIA has heard from business professionals who want to be content compliant, but lack the tools, knowledge and guidance to "get legal." In response, SIIA created a special course, called the Certified Content Rights Manager (CCRM) Seminar. This course is designed to help teach content managers and users how to get the most out of the vast digital and paper-based content resources that are available, and still respect the rights of those who provide that content, whether it be for free or via a paid subscription.

» top