

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

The following examples illustrate the various scenarios in which piracy occurs. 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 hired to reduce expenses for the company and so he decided to cut corners on his software licenses. John would only authorize the purchase of one copy of each software 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 knew they were not licensed for multiple users so they called SIIA. End Corp., facing the possibility of a copyright infringement lawsuit, agreed to pay a fine of \$270,000 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 \$500,000.

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.

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, auction and classified ads sites are notorious for being rampant with counterfeit software. SIIA will often pursue civil litigation against those who are selling counterfeit software. For example, through its Auction Litigation Program, SIIA identifies the most egregious sellers of pirated software and content on

auction sites (eBay, Amazon, iOffer, etc.) and then sues them in federal court demanding that they cease their infringing activities and pay a steep monetary penalty.

Counterfeits can sometimes 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 non-functioning software. For more information on how to identify pirated software see SIIA's Software Buying Guides

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 college noticed significant "warez" activity. Warez is the word commonly associated with the transfer of pirated software across the Internet. The college was able to determine that two students created warez pages on its servers. 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 apply on the Internet just as they do to more traditional media. Copyright and other intellectual property laws protect software created, posted and traded on the Internet. Internet service providers (ISPs) 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

Judges routinely hand down tough sentences for software piracy. Three 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.

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. Ferrar and his co-conspirators 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 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 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.

Often software pirates are often not just intellectual property thieves, but are involved in other illegal activities. This proved true once again when, 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.

Shortly after Ferrar and Peterson were sentenced, Jeremiah Mondello, formerly a college student from the University of Oregon, was sentenced by a U.S. District Court in Oregon on charges of copyright infringement, aggravated identity theft and mail fraud. Mondello received a sentence of 48 months in federal prison, three years supervised release following jail time, and 150 hours of community service per year. Further, Mondello's personal computers and \$220,000 in cash were seized as part of the sentencing mandates. SIIA began investigating the eBay seller later discovered to be Mondello. Using data collected by SIIA's proprietary Auction Enforcement Tool, SIIA identified Mondello through his eBay seller ID and determined there were many more additional eBay identities that likely were being used by Mondello. SIIA then referred all of its case information to the DOJ's Computer Crimes and Intellectual Property Section (CCIPS) and the Department of Homeland Security's (DHS) U.S. Immigration and Customs Enforcement Cyber Crime Center -- where investigators were able to determine that Mondello was not only using a handful of falsified identities - but also created more than 40 fictitious seller IDs. He did so by recording and stealing peoples' bank account information through a keystroke logger that he distributed over the Internet. He then used that information to set up false PayPal accounts using fictitious seller names. By creating these fake seller IDs, he was able to artificially inflate his relatively high standing in the eBay marketplace, which he then used to attract sales and deliver the pirated goods.