# Online Software Copyright Infringement and Criminal Enforcement

**Submitted: May 14, 2005**

Randy K. Baldwin

American University Washington College of Law

## What are Warez and Who Trades Them?

This paper will discuss infringement of software copyrights with a focus on criminal 'warez trading' of copyrighted software on the Internet. Warez are infringing electronic, digital copies of copyrighted works whose copy protection measures have been removed.[1] Warez are most often 'cracked' software programs whose digital rights management (DRM) and copy control measures have been circumvented. Once DRM controls have been disabled, warez are subsequently distributed and traded on the Internet, usually without any direct financial gain to the distributors and traders.[2] Distribution of warez usually starts as small-scale deployments from password-protected file transfer protocol (FTP) servers and encrypted and/or password-protected web sites run by warez groups. Warez are then traded on the Internet among broader groups via direct peer-to-peer (P2P) connections, and encrypted emails with warez attachments. Trading and downloading of warez is coordinated via closed, invite-only Internet Relay Chat (IRC) channels, Pretty Good Privacy (PGP) encrypted email, Instant Messaging (IM), private chat rooms, direct connect P2P networks, and messages posted to Usenet groups under pseudonyms.[3] Servers and sites hosting warez and communications means used by warez traders are designed to avoid detection and identification by law enforcement.[4] File and directory names are intentionally

---

[1] Goldman, Eric, *A Road to No Warez*: *The No Electronic Theft Act and Criminal Copyright Infringement*. 82 Or. L. Rev. 369, 370-371 (2003). [hereinafter *Road to No Warez*], available at http://ssrn.com/abstract=520122 (last visited May 9, 2005) (on file with author) (Defines warez and warez trading. Argues that the NET Act has been largely ineffective in fighting warez trading)

[2] *Road to No Warez* at 370-372 ("Like a typical warez trader, [first prosecuted warez trader] LaMacchia operated the BBS for fun and without any commercial advantage or private financial gain")

[3] Press Release, U.S. Department of Justice, *Leader of Oldest Game Piracy Group Gets 50-Month Prison Sentence* (February 10, 2004) available at http://www.usdoj.gov/criminal/cybercrime/breenSent.htm (last visited April 29, 2005) (on file with author) (Discusses warez group Razor1911's use of IRC and encrypted email for communications; *See* Press Release, U.S. Department of Justice, *Attorney General Ashcroft Announces First Criminal Enforcement Action Against Peer-To-Peer Copyright Piracy* (August 25, 2004), available at http://www.usdoj.gov/criminal/cybercrime/operation_gridlock.htm(last visited May 2, 2005) (Discusses use of Direct Connect P2P network by warez group 'The Underground Network')

[4] *Id.*

mislabeled to obfuscate the fact that warez are being stored on servers and web sites. In reaction to several successful prosecutions of warez groups, it is now extremely rare to find a warez server or site labeled as such.[5] The final stage of the warez life cycle occurs when warez leave the close-knit warez community and become widely available on public P2P networks, anonymous FTP sites that require no password for access and unencrypted, public web sites. Regardless of the distribution method and the point in the deployment life cycle, cracked software warez eliminate protections that force users to register with software vendors in order to install and/or run programs.[6]

A warez trader is someone "who copies and distributes computer software simply for self-aggrandizement - the reputation, the thrill, the 'fun' of having the latest programs or the biggest 'library' of 'warez' titles."[7] Warez traders are self-styled rebels, online Robin-Hoods, and enthusiasts who trade and distribute warez as a hobby. Warez trading is coordinated with and enabled by Internet technologies, and warez traders are a sociological group unique to the Internet.[8]

The importance of fighting warez trading and the link between warez groups and pirated software available on the Internet is undeniable. The head of the US Department of Justice's (DOJ) Computer Crime and Intellectual Property Section (CCIPS) remarked in 2003 "warez groups pose a growing and significant threat to

---

[5] There are thousands of web sites that currently **reference** or mention warez and warez groups, but they seldom, if ever offer direct links to download pirated software.

[6] Goldman, Eric, *The Challenges of Regulating Warez Trading*. Social Science Computer Review, Vol. 23, No. 24, 3 (2005), available at http://ssrn.com/abstract=652702 (last visited May 2, 2005) (on file with author) [hereinafter *Challenges of Regulating Warez*]; Steve Snyder, *Warez Groups and Enforcement: A Rational Approach* (May 2002). Available at http://www.foley.com/files/tbl_s31Publications/FileUpload137/1218/snyder.pdf (last visited May 2, 2005) (on file with author) [hereinafter *Warez Groups and Enforcement*] (history of warez scene and defines terms used by scene participants such as warez, cracking, courier, deploying, et al.)

[7] *Copyright Piracy, and H.R. 2265, the No Electronic Theft (NET) Act: Hearings on H.R. 2265 Before the Subcomm. on Courts and Intellectual Prop. of the House Comm. on the Judiciary*, 105th Cong. (1997) (statement of Sandra A. Sellers, V.P. of Intellectual Property Education and Enforcement for the Software Publishers Association)

[8] *Road to No Warez* at 370-371.

intellectual property rights holders around the world. It is generally agreed that most of the pirated … software available on the Internet come from these high-level warez groups."[9] Some estimates claim that almost 90% of Internet sites offering downloads of pirated software are tied to the warez community.[10]

This paper will give a brief definition of warez and warez trading before discussing what motivates warez traders and explaining how warez groups work. The scale and scope of warez trading is increasing in proportion to the availability lower-cost, and faster high bandwidth Internet connections. High-speed, always-on Internet connections are revolutionizing distribution of both legitimate and pirated software. Increasing adoption of high-speed Internet connections by residential customers means that less software is distributed on physical media as software suppliers, be they publishers or pirates, and their customers opt for downloads in lieu of more costly optical discs.

My hypothesis is that warez groups, whether they identify with the warez scene or not, are the source of most pirated software available on the Internet and that copyright enforcement should focus on these suppliers instead of individual couriers, downloaders, and deployers of pirated software. Some commentators have downplayed or minimized the importance of warez groups, but this is due to the fact that most warez

---

[9] *International Copyright Piracy: A Growing Problem with Links to Organized Crime and Terrorism: Hearings Before the Subcomm. on Courts, the Internet and Intellectual Property, House Comm. on the Judiciary*, 108th Cong. 11 (March 13, 2003) (testimony of John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice), available at http://www.usdoj.gov/criminal/cybercrime/malcolmTestimony.htm (last visited April 29, 2005) (on file with author)

[10] Press Release, US Customs, *US. Customs Dismantles One of the World's Most Sophisticated Internet Piracy Networks 'Operation Buccaneer' Targets 'Warez' Cyberspace Gangs and their Multi-Billion-Dollar Software Piracy Scheme* (Dec. 11, 2001) available at http://www.customs.ustreas.gov/hot-new/pressrel/2001/1211-00.htm (last visited May 10, 2005) "the *WAREZ* community is responsible for nearly 90% of the Internet sites that offer pirated software"

traders and groups no longer self-identify as being part of the warez scene.[11] This is due more to a (realistic) fear of criminal prosecution in the wake of high-profile DOJ investigations than a decline in warez-like software piracy. This paper will examine enforcement actions under the NET Act that have attempted to turn off the 'spigot' of cracked software supply by shutting down high volume warez groups.

This paper also addresses public policy questions regarding criminal investigations and prosecutions of small-scale, individual software piracy on P2P networks. Enforcement is much more expensive and difficult after pirated software moves from the relatively small number of high level warez cracking groups to the large number of P2P clients. The NET Act combined with the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA) have criminalized warez trading, but have also cast a wide net that could potentially be used to prosecute small scale software trading and sharing that a broad cross section of individuals and businesses engage in frequently.

**Motivations for Warez Trading and Effect of Criminalizing Trading**

Warez traders are a varied group, and there are therefore many reasons why they conduct criminal copyright infringement. Some crack software for the challenge and fun of it. For most, ego is the primary motivator. Earning a reputation as the fastest to crack, and release pirated software over the Internet is most important.[12] Warez groups compete against each other, and some have web sites celebrating their software piracy.[13] For warez crackers and distributors, "the whole point ... is to get the pirate program released and

[11] Road to No Warez (expresses sentiment that in wake of PWA, Operation Buccaneer and other DOJ prosecutions, importance of warez groups in contributing to software piracy is exaggerated)
[12] *Fact Sheet, U.S. Customs Service, The "DrinkOrDie" Group: What is It? Who Are They? What is the DrinkOrDie Group?* (December 11, 2001) available at http://www.customs.ustreas.gov/hot-new/pressrel/2001/1211-01.htm (last visited May 10, 2005).
[13] *Id.*

distributed before any other group."[14] A distributor's success is measured by releasing warez as quickly as possible before anyone else, with the crowning achievement being a '0-day' release, a release made before the program's official commercial release.[15] Quickly distributing infringed software proves the warez group's collection, cracking, and distribution skills, which in turn contributes to a reputation for speed and/or quality cracking.[16] For participants in the warez scene, distribution and collection is a competition.[17] Many warez traders get a thrill from committing illicit crimes, in the words of one warez trader/distributor, "deep down everyone is a little scared [of criminal prosecution] but that is also what keeps us going."[18]

Warez traders also see themselves as Robin Hood figures who pirate software so it can be shared and distributed for free online. Almost all warez traders believe software should be free, and they see themselves as helping the oppressed and overcharged software consumers get free programs.[19] Most warez traders view software publishers as oppressive and see the software industry as the enemy.[20] In the past, the warez community had an informal code of conduct that stipulated that warez downloaders should post their own

---

[14] Jason Farnon, *Evolution of a Warez D00d*, at http://www.flashback.se/archive/AWA-001.TXT (last visited May 9, 2005)
[15] David McCandless, *Warez Wars*, Wired (April 1997) available at http://hotwired.wired.com/collections/hacking_warez/5.04_warez_wars_pr.html (last visited May 3, 2005) (on file with author) [hereinafter Warez Wars]
[16] *Warez Wars* ("a group's reputation is paramount"; *US Customs DrinkorDie Fact Sheet* "sticker prices mean nothing - except inasmuch as more expensive programs are harder to crack, and that makes them the most desirable, spectacular trophies... The more the [software] manufacturers harden a product, with tricky serial numbers and anticopy systems, the more fun it becomes to break.")
[17] *Id.* (Warez trading is "a game, a pissing contest.")
[18] David Tetzlaff, *Yo-Ho-Ho and a Server of Warez*, The World Wide Web and Contemporary Cultural Theory, 108 (Andrew Herman & Thomas Swiss eds. 2000). [hereinafter Yo-Ho-Ho and a Server of Warez] (Quoting warez site operator NXSonic)
[19] *Id.* at 114.
[20] *Warez Wars* ("In warez world, the software companies are the criminals")

warez in return.[21] Now many, if not most, warez traders distribute warez freely, without the expectation of anything in return.[22]

**Mere Threat of Criminal Prosecution May Not Deter Warez Trading**

Because of their varied motivations, warez traders do not respond to the threat of criminal prosecution directly.[23] Warez traders have standards and codes of ethics, but they are indifferent to rules they do not believe in.[24] Most warez traders are unlikely to obey externally-imposed rules, and criminalizing trading has stroked warez traders' egos by increasing the thrill of their cracking and trading.[25]

Congress's efforts with the NET Act and the DMCA may counterproductively encourage, not deter, warez trading. Criminalizing warez trading may also reinforce the warez traders' self-perception as being online Robin Hoods who are fighting unduly oppressive and unjust copyright laws. As copyright laws become more restrictive, warez traders see them as being increasingly unjust, and subsequently are able to justify their copyright infringement. Because of the non-monetary and philosophical motivations that drive the warez scene, the NET Act may fail at its unstated, but core objective of deterring warez traders. The Act may actually be counterproductively encouraging warez trading by adding to the allure and thrill of warez trading by branding traders as outlaws.

---

[21] *Id.* "warez are no longer gifts - they're trade goods ... there are no free lunches - every piece of software has to be paid for, in software"

[22] Stephen Granade, *Beelzebub Interview*, Brasslantern.com, available at http://brasslantern.org/community/interviews/beelzebub.html (last visited April 4, 2005). Quotes operator of a warez site, "No one who is involved in the scene trades anymore, nor do they profit from uploading, instead warez is freely distributed to whoever wants it"

[23] Tom R. Tyler, *Compliance with Intellectual Property Laws: A Psychological Perspective*, 29 N.Y.U. J. INT'L L & POL. 219, 234 (1997). "reliance upon threats of punishment to enforce intellectual property laws is a strategy that is likely to be ineffective."

[24] *Warez Wars* Characterizes warez traders' "commandments" as "good manners, good use of bandwidth, and good warez. Give unto others as you would have them give unto you.". "Cardinal sins" include distributing virus-infected files, … posting partial releases, posting a release in a single file instead of smaller pieces, and posting URLs of secret warez FTP sites where warez are uploaded to and downloaded from.

[25] *Yo-Ho-Ho and a Server of Warez* at 108. Quoting warez trader: "There's a feeling of empowerment that comes with beating the system. The thrill rises with the stakes - there are real government agents who could conceivably come and arrest you."

## Anatomy of Warez Groups: How Warez Trading Works

The warez scene is comprised of cells of hierarchical, close-knit groups linked via the Internet. Participants in the scene use pseudonyms and aliases to hide their identities and attempt to keep their intra-group communications private through use of closed, invite-only Internet Relay Chat (IRC) channels, Pretty Good Privacy (PGP) encrypted email, Instant Messaging (IM), private chat rooms, direct connect P2P networks, messages posted to Usenet groups, and other electronic communications means designed to avoid detection and identification by law enforcement.[26] Although the warez scene is underground, warez groups are online communities comprised of individuals and organized groups whose large-scale, illegal distribution of copyright protected software has been enabled by the Internet.[27]

"Warez traders" includes three major sub-communities within the overall warez scene: suppliers, crackers, and couriers (includes distributors, downloaders, and collectors). To understand the warez scene, each sub-community must be separately analyzed. The distinctions are important, as evidenced by the longer jail sentences that warez leaders have received as compared to lower-level couriers and members who merely download pirated software.[28]

---

[26] Press Releases, U.S. Department of Justice, *Leader of Oldest Game Piracy Group Gets 50-Month Prison Sentence* (February 10, 2004) available at http://www.usdoj.gov/criminal/cybercrime/breenSent.htm (last visited April 29, 2005) (on file with author) Discusses warez group Razor1911's use of IRC and encrypted email for communications, and *Attorney General Ashcroft Announces First Criminal Enforcement Action Against Peer-To-Peer Copyright Piracy*, (August 25, 2004) available at http://www.usdoj.gov/criminal/cybercrime/operation_gridlock.htm(last visited May 2, 2005) Discusses use of Direct Connect P2P network by warez group 'The Underground Network'.

[27] Press Release, U.S. Department of Justice, *Internet Distributor of Pirated Software Pleads Guilty to Criminal Copyright Infringement* (June 18, 2004), available at http://www.usdoj.gov/criminal/cybercrime/wiedmaierPlea.htm (last visited April 29, 2005) (on file with author). Provides background on warez scene within context of conviction of warez trader Stephen Weidmaier.who operated the "Fusion" warez group and server from his university apartment.

[28] Eric Goldman, *Warez Trading and Criminal Copyright Infringement*, 51 J. Copyright Soc'y U.S.A. 395, 412 (2004) [hereinafter *Warez Trading and Criminal Copyright Infringement*]

In the warez scene, "suppliers" provide the original copyrighted software titles, primarily business applications such as Microsoft Office, games, professional utilities such as video editing and software development suites, and operating systems such as Windows. Suppliers are often able to obtain access to copyrighted software before the titles are available to the general public through their employers or connections with employees of software firms.[29] There are parallels between suppliers of software warez and pirated films because both groups use insider connections to distribute infringing copies of copyrighted works before they are released to the general public.[30] The key difference is that most pre-release pirated films are sold on the Internet or as DVDs, whereas '0-day' warez are usually freely traded without any direct financial gain.[31] This gap in sales of pirated films versus non-commercial trading of warez is narrowing as home DVD recording equipment comes down in price and increasingly affordable high-bandwidth residential Internet connections make downloads of feature-length films feasible.

"Crackers" use their technical skills in programming, reverse engineering, and decryption to circumvent or "crack" software copyright protections on software they receive from suppliers.[32] Crackers are motivated by the challenge of circumventing copy protection and DRM employed by software publishers.[33]

---

[29] *Id.*

[30] Press Release, U.S. Department of Justice, *First U.S. Convictions in Largest Ever Multinational Investigation of Internet Piracy* (March 8, 2005), available at http://www.usdoj.gov/criminal/cybercrime/kleinbergPlea.htm (last visited April 29, 2005) (on file with author). Explains how warez groups compete with each other to be the first to place a pirated works such as software and games onto the Internet, "often before the work is legitimately available to the public."; Brian Krebs, *FBI Pursuing More Cyber-Crime Cases*, Washington Post, November 4, 2004 at C1 Film studio screening attendee, screenwriter, and then-fugitive Johnny Ray Gasca was placed on FBI's most-wanted list for releasing pirated film DVDs before their theatrical release; Lorenza Munoz, *Year on Lam Ends for Suspected Film Pirate,* L.A. Times, April 6, 2005 at A1. Gasca was arrested in his Florida hotel room while making pirate DVDs on April 5, 2005 and will stand trial for copyright infringement of pre-release films.

[31] *Id.* L.A. Times article: Gasca boasted of making up to $4,000 a week by selling bootleg movies on the Internet

[32] *Id.*

[33] McCandless, *Warez Wars* "For the Inner Circle, cracking software is a challenge. For the wannabe underground, collecting it is an obsession. For the software industry, it's a billion-dollar nightmare."

"Couriers" distribute or “deploy” the cracked, pirated software to various file servers (i.e., FTP and HTTP servers) on the Internet for downloaders and collectors in the warez group to access, reproduce, and further distribute. Couriers often distribute warez across different warez groups, which is when the Pandora’s box of infringement is opened.

Warez groups are large, but regimented operations optimized to generate high volumes of new warez quickly. The participant’s activities are geared towards ‘spreading the word’ about new cracked software titles. Besides ego and braggadocio, furthering the ‘common good’ of providing free software is the motivation for participating in these groups. The groups divide up several discrete tasks among their members, including sourcing new warez; cracking, disabling, and neutralizing any technological protection devices; testing the cracked warez to make sure the software still works; packaging or ‘ripping’ the warez for easy distribution; couriering the warez to propagate the warez to other sites and throughout the Internet; performing systems administration on the computers (i.e., FTP servers) used by the group; and managing/overseeing the operations.[34] The volunteer status and lack of profit motive of warez operations further promotes the participant’s self perception as being moral or acting heroically. Warez group members have not changed their views of themselves in the wake of successful convictions of many scene participants; for many, prosecutions by enforcement agents only fuels their heroic self-image.

Warez collectors actively collect and trade warez outside of the organized distribution groups. Collectors may be trying to gain admission to a warez distribution group or are obsessive enthusiasts who like showing off cracked software as trophies.[35] Warez downloaders do not trade warez; they download warez to use them on a trial or permanent basis. Many warez downloaders just want free software or access to the latest cutting edge

[34] *Warez Trading and Criminal Copyright Infringement* at, 396-397.
[35] McCandless, *Warez Wars*

software releases (including pre-release 'beta' software). Downloaders want to install & use new releases without having to purchase them. Commercial piracy operations also download warez as new product to press on CDs and sell.

Abandonware enthusiasts collect, trade and distribute out-of-print software, especially 'retro' or 'classic' games. Some abandonware enthusiasts consider themselves historians or archivists, but in all other respects their actions are indistinguishable from other warez traders because these software titles are not in the public domain and have not been 'abandoned' by the copyright owners.

**Software Piracy Common Despite High-Profile Enforcement Operations**

Despite many high-profile criminal convictions[36] and civil copyright infringement suits by large software firms, online software piracy by warez groups and subsequent mass distribution via Internet still has catastrophic affects on small software companies. Unlike Microsoft, large game publishers, and software trade associations, small software startups cannot afford to prosecute individual infringers. Software startups also lack resources and the investigative powers to determine which warez group(s) pirated their software. Because of budgetary constraints, small software firms are unlikely to be dues-paying members of industry trade associations such as the Business Software Alliance (BSA), Software and Information Industry Association (SIAA), or the Entertainment Software Alliance (ESA). In addition to infringement suits brought by large software firms, groups such as the BSA, SIAA, and ESA are aggressive in bringing infringement suits on behalf of their members.[37] Despite successful and well-publicized convictions stemming from the

[36] See http://www.usdoj.gov/criminal/cybercrime/ipcases.htm and http://www.usdoj.gov/criminal/cybercrime/ob/Dchart.htm (last visited April 29, 2005) (on file with author). Lists felony convictions associated with Operations Digital Gridlock, Digital Piratez, Buccaneer, Bandwidth, and Fastlane under 18 U.S.C. § 2, 371, and 2319.

[37] See http://www.bsa.org/usa/antipiracy/Piracy-and-the-Law.cfm, http://www.spa.org/piracy/faq.asp http://www.spa.org/piracy/whatis.asp#Internet (SIAA piracy information), and http://www.theesa.com/ip/anti_piracy.php (last visited May 2, 2005). Trade associations are comprised of

US Department of Justice investigations such as Operations Buccaneer, Bandwidth and Digital Piratez in the past few years, it has been estimated that up to 40% of all software used in the United States is illegal and that approximately 85% users of software overseas use pirated software.[38] The increasing availability of high-bandwidth residential Internet connections in the US, Europe, and Asia has enabled broad distribution of warez whose widespread distribution over the Internet has contributed to software piracy rates in excess of 90% in large software markets such as the People's Republic of China and the Russian Federation.[39] According to William J. Cook, author of the Justice Department's manual on computer prosecution, software firms often swallow losses associated with copyright infringement instead of reporting it to law enforcement because of fear of broadcasting vulnerability to shareholders, clients, customers, and potential investors and customers.[40] Thus, the losses are likely far greater than reflected in published reports.

**Software Industry Differs from Other Content Industries**

Unlike other commercial enterprises that profit from copyrighted content, software companies are often entirely dependent on a single copy of a copyrighted work, a program 'title.' Software firms differ from other content-driven industries such as publishing and entertainment, which rely on a stream of sources to stay afloat.[41] Book publishers, record labels, television networks, and film studios rarely rely on a single book, musical

---

dues-paying members with membership primarily consisting of large software and game publishers. BSA, SIAA (spa.org) and ESA sites mention civil and criminal copyright infringement litigation they have assisted with involving pirated business, information services, and game software, respectively.

[38] See http://www.bsa.org (last visited May 2, 2005). BSA estimates 36% of all software is pirated/counterfeit; Marc S. Friedman and Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway*, 507 PLI/Pat 1107, 1110 (February, 1998) [hereinafter *Infojacking*]. Estimates that 40% of all software in US is illegal;

[39] See http://www.iipa.com/pdf/2004_April_08_losses_full.pdf (last visited April 29, 2005). US Trade Representative (USTR) "Special 301" Report shows estimated piracy rates exceeding 90% for business and entertainment software in China and Russia in 2003.

[40] *Infojacking*.

[41] Christian Nadan,, *Software Licensing in the 21st Century*, AIPLA Quarterly Journal, Vol. 32, Number 4, 555 (Fall 2004).

recording, or motion picture to survive. Software piracy can be and is usually fatal to a startup whose revenue comes from a single or only a very few popular titles. Once a single 'cracked' or decrypted/deciphered infringing copy of a program is available on the Internet, multitudes of copies will typically be made and distributed. This subsequent production of perfect digital copies that are available for virtually no cost on the Internet can have disastrous effects on software companies that rely on profits from a popular program. From the perspective of copyright owners, once a infringing 'cracked' or unprotected copy of a software title is available on the Internet, the damage is irreversible. The key to minimizing lost sales from software piracy is keeping cracked copies from moving from relatively small, close-knit, warez groups into loose-knit, global P2P networks. Once a decrypted or cracked program is widely available on P2P file sharing networks, the 'genie is out of the bottle' and enforcement becomes vastly more difficult and expensive, if not impossible.

**Stemming Warez Trading Not Analogous to Fighting Other Crimes**

Regardless of whether one views the ongoing 'war on drugs' as a success or not, battling software copyright infringement with a similar multi-pronged attack on supply, demand, and shipment is unlikely to work. Warez trading is not analogous to the vertically integrated narcotics cartels that are being battled with a multi-pronged attack on supply and demand. While attempting to simultaneously interdict illegal drugs en route to the US, reduce the supply from countries such as Colombia, and reduce domestic demand for drugs may yet prove to be an efficient use of DEA, FBI, DoD, and U.S. Immigration and Customs Enforcement resources, this multi-pronged approach is not applicable to warez trading. Unlike the illegal narcotics trade, the use of illegally acquired software does not result in visible symptoms for the user, supplier, or distributor. The illegal transfer of

infringed software is extremely fast and since there is no financial transaction, few traces are left behind. Despite the criminalization of warez trading, sporadic, individual instances of warez trading seldom leave sufficient evidence to enable successful prosecutions.

Combating warez groups requires different investigative resources and expertise than other computer crimes. Warez traders differ from hackers whose unauthorized access to servers and malware, viruses, and worms violate the CFAA. Warez traders do not actively seek to damage or access servers, and unlike many other software copyright infringers, warez groups are not motivated by direct profits or financial gains from their crimes. Despite the enactment of the No Electronic Theft (NET) Act in 1997 and the Digital Millennium Copyright Act (DMCA) in 1998, many participants in the warez scene **still** claim to not understand that their acts are criminal.[42]

The warez scene is an online subculture that uploads valuable copyrighted programs for each other's benefits, with the only quid pro quo being that "You give what you have, get something you need. No money needed."[43] The first person prosecuted for warez-like trading, David LaMacchia, was not a member of an organized warez group, but saw himself as a Robin Hood of the Internet (or "cyberanarchist") who gave away other people's goods without any expectation at all in return.[44] Unlike software counterfeiters whose CDs are sold, warez groups believe software should be free and therefore freely trade software they have cracked.[45] Warez traders are motivated by ego; it is more important to be the first to release a cracked software title, than to profit from selling it.

The best use of limited enforcement resources is to target the finite number of suppliers of pirated software 'warez' instead of the vastly more expensive and less-effective task of

[42] 17 U.S.C. § 506 (a) (1-2) (NET Act); 17 U.S.C. § 1201 (a) (DMCA – anticircumvention clause provides enforcement agents with tool to use against warez crackers who circumvent software copy protection)
[43] 4-15 Nimmer on Copyright § 15.01
[44] See *Id.*
[45] *Challenges of Regulating Warez* at 2-3.

prosecuting individual downloaders and users who install pirated software. There are private sector mechanisms such as civil copyright infringement suits initiated by software vendors such as Microsoft and aggressive software trade groups such as the BSA, and ESA who have demonstrated their willingness to expend resources to sue individual users and deployers (file sharers) of pirated software.[46] Warez traders and individual downloaders can be civilly sued for copyright infringement, but these cases are more likely to be brought by large software firms and their trade associations than small software startups. The limited criminal investigation and prosecution budget for software copyright infringement would be better spent on interdiction of the suppliers of pirated software than chasing thousands, if not millions, of individuals who obtain and use pirated software. Criminal software copyright infringement is a crime where the contraband goods are largely 'shipped' over Internet connections and often shared freely with a community of peer users. As long as there is a supply free or nearly free pirated copies of software titles, demand for contraband software will outpace demand for the full-price legitimate versions of programs. Only a sharp reduction in the supply 'cracked' software will lead to a corresponding reduction in the amount of illegal P2P trading of software (i.e., consumption). As compared to the debate on drug interdiction versus treatment, warez consumption costs users (even addicts) nothing beyond the price of their existing computer hardware and Internet connection, so as long as there is a supply of free software, no amount of education by the government or software firms (i.e., treatment) is likely to convince them to give up their 'habit.' Only interdiction of the supply of warez will stem use.

[46] See http://www.bsa.org/usa/antipiracy/Piracy-and-the-Law.cfm and http://www.theesa.com/ip/anti_piracy.php (last visited May 2, 2005). Trade associations mention civil copyright infringement litigation involving business and game software, respectively.

**Many Forms of Software IP, Criminal Cases Limited to Copyright Infringement**

Software developers and publishers rely on a combination of copyright, trade secrecy, patents, and trademarks to protect their Intellectual Property (IP). Software developers and publishers rely more heavily on copyright than patents, non-disclosure agreements, or trade secrecy to protect their IP. The choice as to which form of IP protection to employ varies along with the type of software – open-source vs. proprietary, commercial vs. free or 'shareware', utilities vs. business applications; the development setting – university labs vs. commercial software publishers; the target audience/customer base for the software – personal computers and game consoles vs. mainframes, and the business plan and goals of the developer(s). Software developed in university labs or via online open-source collaboration for a broad customer base is less likely to be patented or held as a trade secret and more likely to be copyrighted. Software developers who place high importance upon attribution of their works are unlikely to write software that is subject to non-disclosure agreements or otherwise enforce trade secrecy. Custom programs developed by commercial software companies for specific customers are more likely to be held as trade secrets. Patents also protect software, but this is less common than trade secrecy because of the public disclosure requirements and time required to obtain patents.[47] Software developed for classified or sensitive markets such as national security, financial, or defense, is unlikely to be disclosed publicly as required for patents. Software made for specialized environments such as avionics or real-time systems used in defense and power utilities is usually held in secrecy (in some cases the code and algorithms themselves are classified as secret by governments) or patented, but is rarely open-source. Software

[47] Interview with Jon 'Maddog' Hall, esq., President and Executive Director of Linux International, (April 14, 2005). Mr. Hall, software industry executive, advocate for open-source software, and co-author of *Linux for Dummies*, expressed view that due to the relatively short 'shelf life' for commercial software, software patents that often take years to issue are of little value compared to instantaneous copyright protection.

utilities and programs used for internet-based business methods are often patented. There are U.S. and international trademarks registered for software titles that include operating systems, graphical interfaces, logos, icons, business applications, and games.[48]

Regardless of the form of IP rights protection used, the most critical software IP 'asset' is the program code, and only copyright infringement of the code is criminally punished.[49] Patent infringement associated with software is the subject of civil suits, and trade secrecy violations are litigated as contract breaches (i.e., breaching the terms of an employment contract or a non-disclosure agreement relating to software code). Although the Trademark Counterfeit Act of 1984 provides for criminal fines and imprisonment for trafficking in goods with counterfeit marks, it is most often used to prosecute cases where pirated programs are distributed on counterfeit media with counterfeit labels, and CD cases.[50] The Trademark Counterfeit act is rarely used to prosecute online software infringement because warez are not shipped as pressed CDs with counterfeit labels or packaging and warez trademark violations are limited to on-screen interfaces and displays, which limits evidence and thus makes trademark prosecution difficult.[51]

Computer programs, whether in object code or source code, are "literary works" within the meaning of Copyright Act and are protected from unauthorized copying, whether from

---

[48] Examples of software-related trademark registrations include names, logos, and icons associated with the Apple Macintosh, Microsoft Windows, and RedHat Linux operating systems in addition to product names such AppleWorks, iPhoto, iTunes, Microsoft Office, Netscape, and game titles, characters, and graphics.

[49] 17 U.S.C. § 506 (a) (1-2); 18 U.S.C. § 2319.

[50] 18 U.S.C. § 2320. The Trademark Counterfeit Act of 1984 states that an individual who "intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services shall … be fined not more than $2,000,000 or imprisoned not more than 10 years, or both" and groups/businesses can be fined "not more than $5,000,000." A second offense by an individual increases the penalty to a maximum of $5,000,000 and/or 20 years imprisonment and increases non-individual fines to a maximum of $15,000.000; Roy Girasa, *Cyberlaw: National and International Perspectives*, ch. 5, 127-128 (Prentice Hall 2002).

[51] See http://www.usdoj.gov/criminal/cybercrime/ipcases.htm and http://www.usdoj.gov/criminal/cybercrime/ob/Dchart.htm (last visited April 29, 2005) (on file with author). Lists felony convictions associated with Operations Digital Gridlock, Digital Piratez, Buccaneer, Bandwidth, and Fastlane under 18 U.S.C. § 2, 371, and 2319. Convictions from Operation Buccaneer were under 18 U.S.C. § 2, 371, and 2319, not 2320.

their binary object or human-readable source code version.[52] The US and other World Trade Organization (WTO) members must comply with Article 10 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which states that computer software source, and object code is protected as a copyrightable literary work pursuant to the Berne Convention.[53] This is consistent with the US Copyright Act that states that computer software is copyrightable subject matter.[54] Both human readable ASCII source code and machine readable, binary object code for computer software programs are treated as literary works under US copyright law.[55] Although the 1976 Copyright Act provided for criminal penalties for infringement of literary works such as software, its scope was limited to infringement done for financial gain and reproduction and distribution of **physical** copies.[56]

Early warez traders thought they were above the law because they did not seek to directly profit from their activities. Some warez traders see giving away cracked and pirated copies of proprietary software as furthering the goals of the Free Software, Open Source, and shareware communities, even though shareware, free and open-source software is legal.[57] Many warez participants draw similarities between the illegal warez scene and the goals of the law-abiding Open Source movement because both groups advocate making software freely available. The Open Source and 'free software'

---

[52] *Apple Computer Inc. v. Franklin Computer Corp*., 714 F.2d 1240 (1983), the court held that 17 U.S.C. §§ 101, 102(a) does not require human readability of software code in order for it to be copyrightable

[53] Roy Girasa, *Cyberlaw: National and International Perspectives*, ch. 6, 157 (Prentice Hall 2002). See Chapter 6: *Copyright Issues Raised by the Internet*

[54] *Id*.; 17 U.S.C. § 101.

[55] *Apple Computer Inc. v. Franklin Computer Corp*., 714 F.2d 1240 (1983)

[56] Roy Girasa, *Cyberlaw: National and International Perspectives*, ch. 5, 127 (Prentice Hall 2002). See Chapter 5: *Criminal Aspects of Cyberspace* Discusses NET Act Copyright Act amendment as a Congressional Reaction to *US v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994) where non-commercial software copyright infringement was not wire fraud (i.e., did not violate 18 U.S.C. § 1343).

[57] Interview with Jon 'Maddog' Hall, esq., President and Executive Director of Linux International, (April 14, 2005). Mr. Hall discussed legal and copyrighted, but 'free' and open-source software.

movements do not advocate software piracy or copyright infringement.[58] In response to *United States v. Lamacchia*, where an MIT student was acquitted of wire fraud because he was not profiting from his software copyright infringement, Congress amended the Copyright Act by passing the No Electronic Theft Act (NET Act) in 1997.[59] The NET act addressed a hole in the Copyright act by stipulating that no financial gain is required to convict someone of criminal copyright infringement.[60] LaMacchia's acquittal was based on the fact that his warez trading on a BBS was not motivated by profit. The Net Act modified criminal copyright law to address LaMacchia's conduct in two ways: first, it expanded the definition of "financial gain" to cover bartering implicit in warez trading, and second, it created a new basis of criminal infringement based only on a minimum quantum of infringement (irrespective of motive). The NET Act criminalized warez trading, and the Department of Justice (DOJ) has used the act in many successful warez prosecutions, with over eighty warez traders convictions under the act (or analogous doctrines like conspiracy where the underlying claim was a NET Act violation), and over twenty of those defendants have received jail sentences.[61]

**Why Prioritize Software Piracy and Why Target Warez Groups?**

Software losses due to Internet-based infringement are rising in proportion to increasing market share of high-speed Internet connections. Internet-based warez trading is contributing to an increasing percentage of overall global software piracy losses, which

---

[58] See www.fsf.org (last visited April 11, 2005) (home of the Free Software Foundation) and http://www.gnu.org/philosophy/free-sw.html (last visited April, 11, 2005) Discussions of philosophy behind and motivations behind legally licensed, free, and non-infringing, open-source software.

[59] *United States v. LaMacchia*, 871 F.Supp. 535 (D.Mass 1994), available at http://www.loundy.com/CASES/US_v_LaMacchia.html. (MIT student LaMacchia was the first person criminally prosecuted for warez trading. LaMacchia was indicted for conspiracy to violate 18 U.S.C. 1343 (wire fraud) because his use of a bulletin board service (BBS) to trade Excel, WordPerfect, and software games was not motivated by profit. 17 U.S.C. § 506(a) of the Copyright Act required a profit motive at the time)

[60] 18 U.S.C. § 506(a).

[61] *Warez Trading and Criminal Copyright Infringement* at 396; http://www.usdoj.gov/criminal/cybercrime/ipcases.htm

have been estimated to be as high as $11 billion each year.[62] The economic impact of software piracy extends beyond direct damage to software companies, the losses harm the global economy by greatly reducing tax revenues, which in turn results in lost jobs, and losses in education, infrastructure and research and development. In 1998, software piracy cost the U.S. economy 109,000 jobs, $4.5 billion in wages and nearly $991 million in tax revenues. By 2008, global losses due to software piracy may rise to 175,000 lost jobs, $7.3 billion in lost wages and $1.6 billion in lost tax revenues.[63]

The DMCA can be directed at the criminal circumvention activities of warez crackers, but is less useful for prosecution of low-level collectors, deployers, and end users of pirated software. Despite its relative lack of use in warez prosecutions, the DMCA does criminalize warez activities by programmers who make tools to decrypt and crack software. In the 'drug war analogy', the DMCA can be used in conjunction with the NET act to target the warez traders who are akin to drug distributors/dealers, instead of wasting law enforcement resources on P2P users who are comparable to street dealers and drug users. DMCA prosecutions of warez groups has been rare to date because of their secrecy, and the difficulty involved in proving who originally circumvented software copyright protection measures. Congress intended the DMCA to be used as a criminal prosecution tool, and can still play an important role in prosecuting the cracking conducted by high-level warez groups.

Despite competing law enforcement priorities such as terrorism and other high profile violent crimes, criminal software copyright infringement must be addressed. Continuing software piracy has the potential to wreak havoc upon an industry that has become a key

---

[62] See BSA White Paper, *Software Theft: Stopping the Piracy of Intellectual Property* (2005) available at http://www.bsa.org/usa/policy/Software-Theft.cfm (last visited May 13, 2005). BSA estimates $11 billion in annual losses due to software piracy – including warez-related losses.
[63] *Id.*

component of the US economy and one of the few US industries that enjoys a net trade surplus with the rest of the world. CCIPS actively investigates and prosecutes warez trading because of the recognition that most pirated software available on the Internet comes from warez groups.[64] The DOJ has noted a growing illegal trade in IP, including pirated software, among organized crime syndicates and mentioned possible links between software piracy profits and terrorism.[65] Without cutting off the 'head' of the software infringement serpent that Warez groups and sites represent, profits from sales of pirated software is likely to find its way into the coffers of international organized crime syndicates and may ultimately be funneled into funding terrorist operations.[66] The notion that law enforcement resources are stretched too thin to simultaneously investigate terrorism and copyright infringement misses the point that there is a very real link between software infringement and terrorism.[67]

Congress acted to attack warez groups in the wake of *LaMacchia*; the NET Act was passed in 1997 to directly target warez traders whose copyright infringement is not based on monetary incentives.[68] There has also been action from the law enforcement, namely DOJ Operations Buccaneer, Bandwidth and Digital Piratez from late 2001 through 2004, with prosecutions stemming from these operations ongoing.[69]

---

[64] *International Copyright Piracy: A Growing Problem with Links to Organized Crime and Terrorism: Hearings Before the Subcomm. on Courts, the Internet and Intellectual Property, House Comm. on the Judiciary*, 108th Cong. 11 (March 13, 2003) (testimony of John G. Malcolm, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice), available at http://www.usdoj.gov/criminal/cybercrime/malcolmTestimony.htm (last visited April 29, 2005) (on file with author)

[65] *Id*., *DOJ Stands Ready. to Fight International Piracy*, 3 No. 7 Cybercrime L. Rep. 8 (April 7, 2003). Statement of John G. Malcolm: "… because organized crime syndicates engage in many types of illicit enterprises, including terrorist activities… CCIPS, the Counterterrorism Section and the Organized Crime and Racketeering Section, will do everything within their power to make sure that intellectual property piracy does not become a vehicle for financing or supporting acts of terror."

[66] *Id.*

[67] *Id.*

[68] Roy Girasa, *Cyberlaw: National and International Perspectives*, ch. 5, 126-127 (Prentice Hall 2002).

[69] *Warez Trading and Criminal Copyright Infringement*, at 416-418.

Operations Buccaneer, Bandwidth and Digital Piratez were major government operations targeting warez distribution groups that, on December 11, 2001, led to the execution of approximately 100 search warrants in the U.S., Canada, the United Kingdom, Australia, Sweden, Norway and Finland.[70]

**Criminal Warez Prosecutions Successful Within Existing Copyright Regime**

Unlike other areas of online copyright infringement, criminal prosecutions of Warez crackers, traders, couriers, and, deployers are possible within the bounds of the existing copyright act. No sweeping legislative 'fix' or copyright amendment is needed to convict warez groups. When adequate resources for investigation and prosecution are committed, more success stories will follow. Unlike other types of alleged copyright infringement, software pirates seldom invoke Constitutional free speech issues or fair use defenses, and are likely to plead guilty once indicted.

*United States v. Rothberg* is an example of a successful prosecution of a warez group using the existing copyright regime, including the NET act. Rothberg was charged along with sixteen other members of the "Pirates with Attitudes" (PWA) warez group as a co-conspirator pursuant to 18 U.S.C. § 371 because of his participation in a conspiracy to commit copyright infringement in violation of 17 U.S.C. § 506(a)(2) and 18 U.S.C. § 2319(c)(1).[71] The PWA warez group was "dedicated to the illegal reproduction and distribution of copyrighted software over the Internet, for the use and benefit of members of PWA, and of those persons to whom PWA members further distributed that software."[72] PWA set up a hierarchy with a global, but tight-knit membership of hundreds of members linked via the Internet. PWA stored libraries of pirated software on thirteen File Transfer

[70] *Id.* at 416-417
[71] *United States v. Rothberg* , 222 F. Supp. 2d 1009, 1012 (D. Ill., 2002); *United States v. Rothberg* 2002 WL 171963, 1, 2002 U.S. Dist. LEXIS 1569, 2-3 (D. Ill., 2002).
[72] *Id.*

Protocol (FTP) servers, including a flagship FTP site called Sentinel, which hosted over 30,000 warez and was online from 1995 until January 2000.[73] Access (via login IDs and passwords) to Sentinel was not open to the public and was controlled by senior members of PWA, and members with access were able to download pirated computer software programs to their own computers and subsequently distribute them to others.[74] Due to the strength of incriminating evidence against him, one of PWA's leaders, Robin Rothberg, entered a "blind" guilty plea (i.e., without a plea agreement) to a charge of conspiracy under 18 U.S.C. § 371 to commit copyright infringement in violation of 17 U.S.C § 506(a)(2) and 18 U.S.C. § 2319(c)(1).[75] The PWA conspiracy involved a highly-organized, hierarchical Internet-based software piracy group that included at least one hundred of participants and members-only (authenticated with login IDs and passwords shared amongst members) web sites that made $1.4 to $10 million worth of computer software for available for downloading by members.[76]

**Online Software Infringement Growing Along With Bandwidth**

Criminal software piracy has increased over the past decade in proportion to the growth and commoditization of high bandwidth residential Internet connections. Increasingly fast download transfer rates offered by ISDN, DSL, cable modems (via terrestrial cable and satellite-based ISPs), and T1 business and residential connections have enabled relatively fast downloads of large software installation files, software CD disc images, and decrypted software DVD-RAM disc images. While music file MP3 file sharing represents the current majority of infringement on P2P networks, the immediate, near-term, looming threat is software program sharing, with a long-term, future threat of feature-length

[73] *Warez Trading and Criminal Copyright Infringement*, at 415.
[74] *Id.*
[75] United States v. Rothberg, 222 F. Supp. 2d 1009, 1012 (D. Ill., 2002)

[76] *United States v. Rothberg*, No. 00 CR 85, 2002 WL 171963, *6 (N.D. Ill. Feb. 4, 2002).

movie/DVD image sharing.[77] The latter two categories of illegal file sharing have been numerically dwarfed by music infringement to date because of the comparatively larger file sizes for software and films. The file size barrier which has acted as a de-facto protection for larger software titles, copyright television programs (encoded as MPEGs), or decrypted DVD disc images of films is coming down, and as it does, a new wave of Internet-enabled infringement will occur. Software publishers are distributing their increasingly large software installation files on DVD media instead of multiple, smaller-capacity CD ROMS, but as with the film industry, this will not protect them from online infringement.

Pirated software files (i.e., binaries needed to install and run the software) were prohibitively large to download via 28k or 56k baud modem dial-up connections that accounted for the vast majority of residential Internet connections in the 1990s. When the majority of illegal bulletin board system (BBS) downloads, P2P file sharing, Warez site downloads, and FTP file transfers occurred over dial-up modem connections, infringing content was largely relegated to smaller files such as images (JPEGs, TIFFs, GIFs) and music/audio files such as MP3s. Internet-based software copyright infringement in the form of file downloads, 'Warez' trading, email attachments with compressed software installation files, FTP file transfers, and P2P sharing of commercial software application programs, games, and operating systems has increased as more residential Internet connections have converted from dial-up modem connections to always-on high speed

[77] Saul Hansell and Jeff Leeds, *A Supreme Court Showdown for File Sharing*, N.Y. Times, March 28, 2005 at C1. Shows that vast majority (75%) of P2P volume is comprised of audio files, but P2P sharing of software and other large files is increasing; also see *OECD Information Technology Outlook 2004: Peer to Peer Networks in OECD Countries*, ch. 5 (October, 2004), available at http://www.oecd.org/dataoecd/55/57/32927686.pdf (last visited April 29, 2005) (on file with author) Reveals that growth in file-sharing of software, movies, and other non-audio files on the Internet in the industrialized countries outpaced music file-sharing for the first time in 2003 and sharing of software and other non-music files is related to broadband connectivity.

connections.[78] Although the majority of P2P copyright infringement in the US still involves music and other non-software files, for the first time, in 2003, music file-sharing in developed countries was outpaced by the copying non-audio files (including software).[79] The warez scene remains primarily focused on software (including games) and an increasing share of P2P file sharing involves software.[80]

**Criminal Prosecutions Key: Civil Suits Insufficient**

Compared to the sheer volume of software infringement occurring online and number of 'cracked' software titles available, the NET Act and DMCA has not deterred willful software copyright infringement. Circumventing copyright protection measures in software and subsequent trading of the cracked warez are already criminal violations of the copyright act, so more legislation is not needed to prosecute warez crackers and traders.[81] Unlike software protections afforded by patents and trade secrecy, copyright infringement of software code is a criminal violation and punishable with jail time. The No Electronic Theft Act (NET Act) stipulates that willful copyright infringement is punishable by up to three years imprisonment.[82] The NET Act modified criminal copyright law to address previously non-criminal infringement (i.e., infringement without commercial gain) in two key ways. The first NET Act modification to the copyright act was an expansion of the definition of "financial gain" to cover non-commercial trading and bartering such as warez

---

[79] *Id.*; also see *OECD Information Technology Outlook 2004: Peer to Peer Networks in OECD Countries*, ch. 5 (October, 2004), available at http://www.oecd.org/dataoecd/55/57/32927686.pdf (last visited April 29, 2005) (on file with author) Report published by the Organization for Economic Cooperation and Development (OECD) reveals that growth in file-sharing of software, movies, and other non-audio files on the Internet in the 30 industrialized OECD member countries outpaced music file-sharing for the first time in 2003 and sharing of software and other non-music files is related to broadband connectivity in member countries.

[80] *Warez Trading and Criminal Copyright Infringement*, at 395. Mentions that warez trading is primarily comprised of proprietary, copyrighted software, not freeware, shareware, open-source, or public domain software.

[81] 17 U.S.C. § 506(a)(1-2) 17 U.S.C. § 1201

[82] 17 U.S.C. § 506(a)(2) (The NET Act is an amendment to the Copyright act designed to address criminal infringement of electronic 'works', including software).

trading. The second important NET Act amendment was the creation of a new basis of criminal copyright infringement solely based upon a minimum quantum of infringement, no matter what the motive or mens rea of the infringer was at the time the infringement occurred.

The NET Act has achieved the goal of criminalizing most warez trading of cracked or pirated copies of commercial software.[83] The Department of Justice (DOJ) is increasingly successful in its warez prosecutions, which have increased in both numbers of indictments, and prosecutions.[84] Between the 1997 passage of the NET Act and 2004, over eighty warez traders were convicted either directly under the Act's provisions or received conspiracy convictions where there was a conspiracy to commit a NET Act violation. Importantly, twenty of these defendants received jail sentences.[85]

Beyond copyright provisions such as the NET Act and 18 U.S.C. §§ 2318-2319 (Trafficking in counterfeit computer programs, and Criminal Infringement of a Copyright, respectively); Federal criminal statutes such as 18 U.S.C. § 2 (Aiding and Abetting), 18 U.S.C. § 371 (Conspiracy), and Computer Fraud and Abuse Act of 1984, 18 U.S.C. §1030 (1984) (the "CFAA") have been successfully used to prosecute and convict warez traders, crackers, and couriers.[86]

Other criminal statutes such as the Digital Millennium Copyright Act (DMCA) and 18 U.S.C. § 2314 have proven to be less useful for criminal prosecutions.[87] Given the

---

[83] *Warez Trading and Criminal Copyright Infringement* at 396.
[84] *Id.*
[85] *Id.*
[86] See http://www.usdoj.gov/criminal/cybercrime/ob/Dchart.htm (last visited April 29, 2005) (on file with author). Lists felony convictions associated with Operation Buccaneer under 18 U.S.C. § 2, 371, and 2319.
[87] 17 U.S.C. § 1201 (anti-circumvention); *US v. Elcom, Ltd. and Sklyarov,* 203 F. Supp. 2d 1111 (N.D. Ca. 2002). The first DMCA prosecution under 17 USC § 1201 (b) (1) (A) and (C) for trafficking and marketing software that circumvented Adobe's eBook copyright protection measures did not result in a conviction in part because Adobe did not cooperate in the investigation; also see Michael Hatcher, Jay McDannell, and Stacy Ostfeld, *Computer Crimes*, 36 Am. Crim. L. Rev 397 (Summer 1999). Discusses how although 18 U.S.C. § 2314 criminalizes transportation of stolen or fraudulently obtained goods in interstate commerce,

challenges faced by the law enforcement community, particularly the acute problem of the need for Federal resources to be diverted to higher priority investigations and prosecutions related to terrorism over the past few years, fewer investigations of online software piracy or lower criminal penalties (including restitution, fines, and jail sentences) for software pirates/copyright infringers may result in an explosion of Internet-enabled worldwide software piracy. There are policy implications of government abdication of software copyright enforcement because of the inherent shortcomings involved in allowing commercial software publishers to police infringers of their choice solely through civil suits. As is the case with IRS audits odds and tax evaders, if software pirates perceive that there is little-to-no chance of facing a criminal investigation or prosecution, they are more likely to continue trading cracked and pirated warez and take their chances with being named as civil defendants by the likes of the Business Software Alliance (BSA) or Microsoft. The BSA is more aggressive in filing civil litigation suits than other trade associations like the Motion Picture Association of America (MPAA) and Recording Industry Association of America (RIAA), and the BSA is more cooperative in assisting law enforcement with prosecuting criminal software copyright infringement as well. Like many other computer crimes, software piracy rarely involves violent acts, but sentences must be harsh enough to deter future piracy.

If enforcement is left to civil suits from the content industry trade groups such as the BSA (whose members include Adobe, Apple, Dell, Microsoft, and other major software vendors and publishers), the same uneven prosecution that has been employed by similar trade groups such as the RIAA and MPAA will be applied to software infringers. Groups such as the BSA, RIAA, and MPAA often name defendants in infringement suits based on

---

pirated software was not held to be goods covered by § 2314 in *US v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), *US v. Brown*, 925 F.2d 1301, 1308 (10th Cir. 1991) and *US v. Wang*, 898 F. Supp. 758, 760 (D.Colo. 1995).

their public relations value and not their level of culpability. Although the DOJ is not immune to 'cherry picking' defendants based on the likelihood of a conviction, nature of crime, and ability of a prosecution to 'send a message', the DOJ and State District Attorneys are more likely to apply an even handed approach to software copyright infringement than the BSA or individual software companies who will only prosecute infringers who are hurting their bottom lines.

Copyright infringement accounts for large amounts of lost software sales, but the software industry selectively targets whom they prosecute. The DOJ, unlike the BSA and individual software publishers, is able to pursue criminal charges against software pirates. The DOJ has been more successful in shutting down warez operations by identifying and prosecuting high-level warez groups than software companies are likely to be through civil infringement suits. Contributory infringers who provide sales forums, host pirated copies of software on their servers, or otherwise provide technology that enables direct infringement are also targeted by software vendors, but direct, individual infringers are rarely sued by copyright holders. The problem with leaving copyright enforcement up to software vendors is that unlike music publishers (e.g., the RIAA) and filmmakers (e.g., MPAA) who have sued direct infringers, software companies want to avoid negative press and bad consumer relations that is inherent when children and customers are sued rather than warez groups who make the infringing copies of software initially available. To date, software companies have chosen a different path than music publishers and movie studios, who have gone after contributory infringers like Napster, Grokster, and other P2P file sharing services while simultaneously suing direct infringers who download and use illegal copies of copyrighted songs, so it is up to law enforcement to fill this void with criminal prosecution of warez groups.

Software producers choose not toe pursue individual infringers to avoid negative publicity that the RIAA and MPAA have encountered, but by doing so, some users interpret this as an invitation to use infringing software. Not all software publishers are the same, and it is the small startups that have no voice in Congress or within the large software-related trade organizations as to which infringers are pursued and prosecuted. Larger software firms can afford strong cryptography and ciphers to protect what is known in the software industry as 'Code Signature' that is difficult for even skilled warez crackers to circumvent. It is the small software firms who rely on traditional and more-readily circumvented 'key-matching' technology that only verifies software authenticity at install-time. Use of increasingly complex cryptography and DRM is a technological arms race between large software companies and warez crackers, but small software firms cannot afford to enter this race.

The scale and seriousness of damage stemming from warez activities is undeniable. The damage from software piracy goes beyond the lost sales, tax revenues, jobs cited by the BSA. If left unchecked, damage from warez groups can stifle innovation and slow the flow of venture capital that is necessary to drive future technological innovations and fuel growth in a critical sector of the US economy.