

Warez Trading and Criminal Copyright Infringement

By Eric Goldman*

1. INTRODUCTION.

In 1994, David LaMacchia became the first person criminally prosecuted for warez trading. At the time, criminal copyright infringement required infringement for commercial advantage or private financial gain. Because LaMacchia acted without commercial motives, the government chose not to prosecute LaMacchia for criminal copyright infringement and instead prosecuted him under conspiracy to commit wire fraud. However, a U.S. Supreme Court case had already declared that copyrighted works were not capable of being taken by fraud,¹ so the judge quickly dismissed the case.²

It took copyright owners three years, but they finally addressed the perceived hole exposed by LaMacchia's prosecution when Congress enacted the No Electronic Theft (NET) Act (the "NET Act")³ in 1997. The NET Act modified the existing criminal copyright infringement statute to address LaMacchia's conduct in two principal ways: first, by expanding the definition of "financial gain" to cover bartering implicit in warez trading, and second, by creating a new basis of criminal copyright infringement liability that requires only a minimum quantum of infringement irrespective of motive.

There is no real question that the NET Act successfully criminalized most warez trading.⁴ This Article explores how criminal copyright laws apply to warez trading, some of the enforcement actions under the law, and some of the policy concerns about criminalizing warez trading. The Article concludes by discussing why it appears inevitable that warez traders will continue to be jailed for their activities.

* Eric Goldman (eric.goldman@marquette.edu) is an Assistant Professor at Marquette University Law School in Milwaukee, WI. My personal website is located at http://eric_goldman.tripod.com. This Article is based on the "Legislative Efficacy" series of projects being conducted by the Intellectual Property Subcommittee, Cyberspace Law Committee, Business Law Section, American Bar Association.

Readers are cautioned that criminal copyright infringement laws are tricky and this Article provides only a summary discussion about the law. Therefore, readers wanting legal advice are urged to retain a competent attorney who can provide individualized guidance. While I welcome comments and feedback on this Article, regrettably I do not practice criminal law and therefore cannot provide legal representation.

¹ Dowling v. United States, 473 U.S. 207 (1985), available at <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=473&invol=207>.

² United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994), available at http://www.loundy.com/CASES/US_v_LaMacchia.html; see also Indictment, United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994) (No. 9410092-RGS), available at <http://www-tech.mit.edu/Bulletins/LaMacchia/indictment.html>.

³ No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997), available at <http://www.usdoj.gov/criminal/cybercrime/17-18red.htm>.

⁴ Note that the Department of Justice has taken the position that the bartering implicit in warez trading constituted illegal "financial gain" even prior to the NET Act. See United States Consolidated Response to Defendants' Pre-Trial Motions, United States v. Rothberg, No. 00-CR-85, at 7 n.1 and 11 (N.D. Ill. 2002).

2. WHAT IS WAREZ TRADING?

It is common to use the generic term “warez trading,” but this term imprecisely lumps together disparate activities. In fact, a number of sub-communities comprise the warez scene.

Warez distributors are fairly large and organized operations optimized to generate high volumes of new warez quickly. These operations divide up several discrete tasks that require different skill sets and personality types. These tasks include sourcing new warez, cracking any technological protection devices, testing the cracked warez to make sure they still work, packing the warez for easy distribution, couriering the warez from site to site, doing systems administration, and handling management and oversight of the operations. As discussed below, usually all participants in the group will be liable for criminal actions taken by any of them, but the different actions and functions trigger different bases of criminal prosecution.

Warez collectors collect and trade warez more autonomously. They may be trying to gain admission to a warez distribution group, or they may be enthusiasts who want to be on technology’s cutting edge or just like showing off trophies.

Warez downloaders do not trade warez per se. Instead, they download warez to use them (or, at least, try them). Many warez downloaders are just looking for free software or the latest cutting edge stuff. However, international piracy operations also download warez as new product to press on CDs and sell.

Finally, abandonware enthusiasts deserve a mention. They collect, trade and distribute software (specifically games) that is no longer being published. While many abandonware enthusiasts claim their activities are less detrimental to copyright owners than warez trading (because, by definition, the copyright owners have stopped commercializing the work), abandonware trading is functionally and legally indistinguishable from warez trading.

3. THE CRIMINAL COPYRIGHT INFRINGEMENT STATUTE.

Criminal copyright infringement is defined as the willful infringement of a copyright (a) for purposes of commercial advantage or private financial gain (“Section 506(a)(1)”)⁵ or (b) by the reproduction or distribution (including by electronic means), during any 180-day period, of copyrighted works with a total retail value of more than \$1,000 (“Section 506(a)(2)”)⁶.

For a first-time violation where the infringement involved reproducing or distributing at least 10 copies with a total retail value of more than \$2,500, criminal penalties include up to 5 years imprisonment (in the case of Section 506(a)(1)) or up to 3 years imprisonment (in the case of Section 506(a)(2)), and in each possibly a fine.⁷ Because it offers greater penalties, generally the government prefers to prosecute under Section 506(a)(1).⁸ Otherwise, all other criminal

⁵ 17 U.S.C. §506(a)(1), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

⁶ 17 U.S.C. §506(a)(2), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

⁷ 18 U.S.C. §2319(b) and (c), available at <http://www4.law.cornell.edu/uscode/18/2319.html>. 18 U.S.C. §3571 (<http://www4.law.cornell.edu/uscode/18/3571.html>) governs the amount of fines.

⁸ U.S. Department of Justice, Computer Crime and Intellectual Property Section, Prosecuting Intellectual Property Crimes Manual §III(B)(5) (also noting that a commercial motivation has better jury appeal), available at

violations can lead to up to one year imprisonment and possibly a fine. In all cases, defendants should forfeit the equipment used to commit infringement.⁹

The Sentencing Guidelines informs judges' determination of actual sentences, and Section 2B5.3 specifically applies to criminal copyright infringement.¹⁰ In the portions most relevant to warez trading, provisions increase the offense level based on uploading infringing items (including setting a minimum offense level),¹¹ decrypting or circumventing technological protection measures to gain access to the work,¹² and participating in an organized criminal enterprise,¹³ and a provision reduces the offense level when the offense is not committed for commercial advantage or private financial gain.¹⁴

4. ELEMENTS OF A PROSECUTION AND APPLICABLE DEFENSES.

A criminal copyright infringement conviction requires the government to prove, beyond a reasonable doubt, the following elements: (1) a valid copyright exists, (2) it was infringed, (3) the infringement was willful, and (4) either (a) the infringement was for commercial advantage or private financial gain or (b) the retail value of the infringed works exceeded the statutory thresholds.¹⁵

Element #1: A Valid Copyright Exists

The government must demonstrate the existence of a valid copyright. Although copyright protection technically attaches when a work is created, the work's copyright must be registered before the work can be the basis of a prosecution.¹⁶ If made within five years of the work's publication, the registration is *prima facie* evidence that the copyright is valid.¹⁷ Even without such a presumption, establishing a valid copyright for works that are the subject of warez usually should be relatively easy, so this factor will rarely be relevant in a warez trading case.

Element #2: Infringement

Unauthorized reproductions or distributions of a copyrighted work constitute copyright infringement. Uploading warez to Usenet, IRC, a website or anywhere else permitting downloads should constitute both reproduction (making a copy from a local computer to the file

<http://www.cybercrime.gov/ipmanual/03ipma.htm> [hereinafter DOJ IP Crimes Manual].

⁹ 17 U.S.C. §506(b), available at <http://www4.law.cornell.edu/uscode/17/506.html>

¹⁰ U.S. SENTENCING GUIDELINES MANUAL §2B5.3, available at <http://www.ussc.gov/2002guid/2002guid.pdf>.

¹¹ *Id.* §2B5.3(b)(2).

¹² *Id.* §2B5.3 app. 4 (pointing out that §3B1.3, applicable to the use of special skills, applies).

¹³ *Id.* §2B5.3 app. 5(B).

¹⁴ *Id.* §2B5.3(b)(3).

¹⁵ See generally DOJ IP Crimes Manual, *supra* note 8; A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 263-89 (2001).

¹⁶ 17 U.S.C. §411(a), available at <http://www4.law.cornell.edu/uscode/17/411.html>.

¹⁷ 17 U.S.C. §410(c), available at <http://www4.law.cornell.edu/uscode/17/410.html>.

server) and distribution (when received by downloaders).¹⁸ Downloading a file¹⁹ and executing the file on a local computer²⁰ should each constitute reproduction of the file.

A defendant's best defense is to question the government's evidence that the defendant actually performed the allegedly infringing uploads or downloads. There several ways the government can try to prove infringement, but no method is foolproof.²¹

- The government can show infringing activity associated with a username and password, but a defendant can claim that the username and password were stolen or shared.
- The government can show infringing activity associated with an IP address, but the government then needs to further show that the defendant was using this IP address at the applicable time.
- The government can obtain witness testimony that the defendant committed the infringing acts, but there are rarely "eyewitnessed" accounts of warez trading. However, even if they did not specifically see the defendant engaged in infringement, other group members can often offer damaging testimony.
- The government can obtain evidence from the defendant's computers, although defendants could make the government's job more difficult through encryption and regular data purging.
- Finally, the government can try to prove infringement circumstantially. Prosecutions based solely on circumstantial evidence make it hard to convince potentially sympathetic juries and thus may not be worth pursuing.

Government-operated or -infiltrated file servers or websites provide the government the best opportunity to obtain credible proof connecting the warez trader with infringing activity. This method is obviously difficult for the government, but it has been used successfully in, among others, the Fastlane and Operation Bandwidth (Rogue Warriorz) cases.

A warez distributor or collector can try to defend against distribution liability by requiring the government to show that an uploaded file was actually downloaded.²² However, an infringing distribution may occur merely when the defendant makes a copy *available* for distribution.²³ Further, this defense will not negate the liability for reproducing the file made during the upload and download process.

The "first sale doctrine" is a common defense in physical-space criminal copyright cases. The doctrine allows a person who legitimately acquires a physical copy of a copyrighted work to

¹⁸ A&M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (discussing liability of P2P file traders), *available at* http://www.law.cornell.edu/copyright/cases/239_F3d_1004.htm.

¹⁹ *Id.* (discussing liability of P2P file downloaders).

²⁰ It is well accepted that loading a copy into RAM is a reproduction. *See* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511 (1993), *cert. dismissed*, 510 U.S. 1033 (1994), *available at* http://www.law.cornell.edu/copyright/cases/991_F2d_511.htm.

²¹ *See generally* DOJ IP Crimes Manual, *supra* note 8, §III(E)(2).

²² Although the case mostly focused on whether programs were functional, this argument was at issue in determining the proper retail value of the infringed items in the Pirates With Attitude case. *See* United States v. Rothberg, 2002 U.S. Dist. LEXIS 1569 (N.D. Ill. 2002).

²³ *Hotaling v. Church of Jesus Christ of Latter-Day Saints*, 118 F.3d 199, 203 (4th Cir. 1997), *available at* <http://www.law.emory.edu/4circuit/june97/961399.p.html>.

redistribute that copy.²⁴ Because the first sale doctrine only applies to physical copies (not electronic ones), and further is a defense only against distribution (not reproduction), it does not apply to warez trading cases.

A more relevant defense to warez traders is fair use. Fair use is a multi-factor equitable test designed to balance the relatively absolute nature of a copyright monopoly with the social benefits that can derive from limited uses of those copyrighted works. The factors are:

- the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- the nature of the copyrighted work;
- the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- the effect of the use upon the potential market for or value of the copyrighted work.²⁵

Because fair use is an equitable defense, courts routinely manipulate their multi-factor analyses to reach a result they think is appropriate. As a consequence, the fair use defense remains highly unpredictable, making it a poor basis to rely on prospectively.

Having said that, it is possible to predict how many courts will apply the factors to warez trading. For example, it is likely that the second and third factors will usually weigh against a warez trader. While software is not a traditionally core copyrighted work like books or articles, software is nevertheless closer to copyright's core than fringe works like factual databases. Also, the warez trader also usually makes a complete (or near-complete) copy of the work.

The first factor is harder to apply. By definition, warez traders do not infringe for profit. Some commentators have suggested that noncommercial infringement should be presumptively considered fair use,²⁶ which would make noncommercial warez trading immune from prosecution.

However, the NET Act revised the definition of financial gain to include the receipt or expectation of receipt of copyrighted works. This makes it now more plausible to say that warez traders infringe for "financial gain."²⁷ Further, the *Napster* court proposed that "repeated and exploitative" copying for personal benefit could constitute a *commercial* infringement because it permits the infringer to avoid spending the money to purchase legitimate copies, and on that

²⁴ 17 U.S.C. §109(a), available at <http://www4.law.cornell.edu/uscode/17/109.html>.

²⁵ 17 U.S.C. §107, available at <http://www4.law.cornell.edu/uscode/17/107.html>.

²⁶ See Lydia P. Loren, *Digitization, Commodification, Criminalization: the Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L. Q. 835, 887 (1999), available at <http://www.wulaw.wustl.edu/WULQ/77-3/773-835.pdf>; James E. Neuman, *Copyright Violations Face Criminal Exposure*, N.Y.L.J., Oct. 13, 2001, at S3; see also DOJ IP Crimes Manual, *supra* note 8, §III(C)(3). In 1984, the Supreme Court said that noncommercial use was presumptively fair, *Sony Corp. v. Universal City Studios*, 464 U.S. 417, 449 (1984), available at http://www.law.cornell.edu/copyright/cases/464_US_417.htm, but effectively abandoned this presumption in 1994. *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 584 (1994), available at <http://supct.law.cornell.edu/supct/html/92-1292.ZS.html>.

²⁷ The *Napster* ruling specifically noted the financial gain definition to conclude that P2P file traders were engaged in commercial infringement for purposes of the fair use analysis. *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1015 (9th Cir. 2001), available at http://www.law.cornell.edu/copyright/cases/239_F3d_1004.htm.

basis found that P2P file traders engaged in commercial infringement.²⁸ If P2P file traders make “repeated and exploitative” copies, warez traders probably do too.

Some courts tilt the first factor in favor of fair use if the copy is “transformative,” meaning that it “adds something new, with a further purpose or different character, altering the first with new expression, meaning or message.”²⁹ Although a warez copy may not be identical (due to the removal of copy protection devices, the addition of .nfo files, etc.), these changes do not “transform” the work into something different. However, some courts have found transformative uses based on a different purpose even nothing new is added.³⁰ In this approach, warez have different purposes as evaluation copies or trophies (instead of functional objects). It remains to be seen how many courts will follow the lighter definition of transformative. Otherwise, warez traders are unlikely to have the first fair use factor weigh in their favor.

The fourth factor is generally regarded as the most important fair use factor,³¹ so a warez trader can go a long way towards achieving a fair use defense if he or she can convince the fact-finder that warez trading does not detrimentally affect the copyright owner’s market. In practice, most warez trading has absolutely no effect on the market. Many warez distributors and warez collectors never use the warez they trade or archive, and certainly they would never purchase those works. Thus, a warez trader who merely collects warez might be able to argue that those activities do not adversely affect the market.

Justifying uploading/distribution under the fourth factor is harder. A warez trader could argue that most downloads are made by other warez traders, cycling warez through a group of people who would never buy them. However, some downloaders do use warez as a substitute for buying the original, and those are lost sales. Further, some commercial pirates, especially in Asia, use warez sites as a reliable source of new inventory. Even though warez traders usually strongly object to commercial piracy, warez distribution can facilitate commercial piracy and thus detrimentally affect the market for traded works. As a result, many fact-finders will be reluctant to weigh the fourth factor in favor of warez trading defendants.

Given the nature of their commodity, abandonware traders may have a little more luck on the fourth factor. By definition, abandonware does not hurt a market that the copyright owner has stopped pursuing. However, some courts protect a copyright owner’s right not to exploit a market,³² and in those cases, even the abandonware trader will find little relief under fair use.

This analysis of the fair use factors provides little optimism that fair use will be a strong defense for warez traders. Warez trading is not the type of behavior that fair use was intended to encourage, and courts are not likely to interpret the defense broadly to help out warez traders.

²⁸ *Id.*

²⁹ *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994), available at http://supct.law.cornell.edu/supct/html/92-1292_ZS.html.

³⁰ *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002), available at http://images.chillingeffects.org/cases/Kelly_v_Arriba.html.

³¹ *Harper & Row v. Nation Enters.*, 471 U.S. 539 (1985), available at http://www.law.cornell.edu/copyright/cases/471_US_539.htm.

³² *Castle Rock Entm’t v. Carol Publ’g Group, Inc.*, 150 F.3d 132 (2d Cir. 1998), available at http://www.law.cornell.edu/copyright/cases/150_F3d_132.htm.

Element #3: Willfulness

The government has the burden to prove the defendant's conduct was willful. Willfulness is "a word of many meanings whose construction is often dependent on the context in which it appears."³³ In the criminal copyright infringement context, the word's meaning remains unresolved.

There are two different standards used to define "willfulness." The minority position is that willfulness requires the government to prove only that the defendant had the intent to copy.³⁴ Under this position, warez trading will be characterized as willful. However, this position has justifiably received significant criticism,³⁵ and a number of commentators believe that the language added to Section 506(a)(2) by the NET Act ("evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement") ends any credible argument that the minority position applies to criminal copyright infringement.³⁶

The majority position is that willfulness requires the government to prove that the defendant specifically intended to infringe such that the infringement was a voluntary, intentional violation of a known legal duty.³⁷ Under this position, defendants can assert several additional defenses:

- The defendant (incorrectly) believed in good faith that he or she did not infringe because the original and copy are dissimilar or because of the First Sale doctrine.³⁸ This defense offers limited hope to warez traders. As discussed earlier, the First Sale doctrine does not apply to electronic copies, and warez are usually faithful copy of the originals. Rarely will these questions be debatable enough to allow a court to conclude that the belief was reasonable.
- The defendant (incorrectly) believed in good faith that the use was fair.³⁹ This defense has a little more merit. Although warez trading probably is not fair use, the question is debatable enough that a warez trader could believe that his or her conduct was privileged. However, if the court concludes that this belief was not reasonable, the defense will fail.
- The defendant did not know the law.⁴⁰ This defense could have a little merit as well. Criminal copyright infringement laws are technical and opaque, so understandably many warez traders do not understand how their behavior violates the law. However, the defense may apply only if the defendant did not know the laws applicable to *civil*

³³ Bryan v. United States, 524 U.S. 184 (1998), available at <http://supct.law.cornell.edu/supct/html/96-8422.ZS.html>.

³⁴ SCOTT, *supra* note 15, at 277.

³⁵ Scott characterizes the minority view as "doubtful." *Id.* Loren says the minority cases "are not nearly as definite as commentators have made them out to be." Loren, *supra* note 26, at 877.

³⁶ Scott says the added language casts doubts on the minority view's viability. SCOTT, *supra* note 15, at 277. Nimmer says that the added language precludes any prosecutions based on simple proof of conduct violating the Copyright Act. 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT §15.02[B][2] (2002).

³⁷ SCOTT, *supra* note 15, at 277 (citing United States v. Moran, 757 F. Supp. 1046 (D. Neb. 1991)). Nimmer characterizes this as the "better" view. NIMMER, *supra* note 36, §15.02[A][2].

³⁸ See NIMMER, *supra* note 36, §15.02[A][2].

³⁹ See *id.*

⁴⁰ See SCOTT, *supra* note 15, at 278; Loren, *supra* note 26, at 869. See generally DOJ IP Crimes Manual, *supra* note 8, §III(B)(3).

infringement. Warez traders generally know that they are infringing. In fact, committing infringement is a key point—what reputable warez trader wants to distribute or collect public domain material or open source software? Because most warez traders know they are doing *something* wrong, this defense will likely fail.

While the majority definition of willfulness is a reasonably high standard for the government to overcome, warez trading is probably willful under either the majority or minority standards.

Element #4(a): Commercial Advantage or Private Financial Gain

To prosecute under Section 506(a)(1), the government must prove that the infringement was made for commercial advantage or private financial gain. The post-NET Act definition of “financial gain” covers the “receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.”⁴¹ Thus, to the extent that a warez trader barter (implicitly or explicitly) copyrighted works, that activity can be characterized as being for financial gain. Although warez traders often trade hundreds or even thousands of copyrighted works, even a single barter violates the statute.

Some warez traders assert that they trade warez without any expectation of return. Even in these cases, the government can respond that the warez trader’s need to maintain a reputation for distributing new warez creates an implicit expectation of return. These arguments have not yet been tested.

Element #4(b): Retail Value of Infringed Works

A felony conviction under Section 506(a)(1) requires the government to prove the defendant reproduced or distributed copyrighted works with a retail value of at least \$2,500.⁴² Alternatively, if the government prosecutes under Section 506(a)(2), the government must prove that the defendant, in any 180 period, reproduced or distributed copyrighted works with a retail value over a minimum threshold. For felony prosecutions, the minimum threshold is \$2,500.⁴³ For misdemeanor prosecutions, the minimum threshold is \$1,000.⁴⁴

Copyrighted works have a wide disparity of retail values, ranging from the manufacturer’s list price to the street price to the price paid for an infringing copy (which, for warez, is zero). So how is retail value determined? The statute intentionally does not define the term.⁴⁵ The

⁴¹ 17 U.S.C. §101, available at <http://www4.law.cornell.edu/uscode/17/101.html>.

⁴² 18 U.S.C. §2319(b)(1), available at <http://www4.law.cornell.edu/uscode/18/2319.html>. In addition, the defendant must have reproduced or distributed at least 10 copies of copyrighted works, a standard easily met in most warez cases.

⁴³ 18 U.S.C. §2319(c)(1), available at <http://www4.law.cornell.edu/uscode/18/2319.html>. In addition, the defendant must have reproduced or distributed at least 10 copies of copyrighted works, a standard easily met in most warez cases.

⁴⁴ 18 U.S.C. §2319(c)(2), available at <http://www4.law.cornell.edu/uscode/18/2319.html>.

⁴⁵ From the House Report accompanying 1992 Copyright Felony Act (the criminal copyright law amendment preceding the NET Act):

The term "retail value" is deliberately undefined, since in most cases it will represent the price at which the work is sold through normal retail channels. At the same time, the Committee recognizes that copyrighted works are frequently infringed before a retail value has been established, and that in some cases,

Sentencing Guidelines do define retail value, but its definition only controls sentencing once the defendant has been found guilty. However, some courts will consider that definition as persuasive.

The Sentencing Guidelines' definition sets up a shifting standard for determining retail value. The default calculation is the price paid for the infringing copies.⁴⁶ However, the standard shifts to the retail value of legitimate copies in (among others) the following circumstances:

- the infringing item is identical or substantially equivalent to the infringed item, or is a digital or electronic reproduction;
- the infringing item's retail value is difficult or impossible to calculate without unduly complicating or prolonging the proceedings; or
- the infringed item's retail value more accurately assesses the pecuniary harm suffered by the owner.⁴⁷

Based on these factors (especially the first), the retail value used in warez trading cases should be the retail value of legitimate copies. This should make retail values high. Indeed, the DrinkOrDie defendants stipulated to infringing works with retail value of between \$2,500,000 and \$5,000,000, and the judge set the retail value for the Pirates With Attitude ("PWA") defendants at \$1,424,640.

However, the retail value infringed by the foregoing defendants probably vastly exceeded those amounts. Retail value computations are suppressed by the government's evidentiary challenge of connecting infringing copies with defendants. However, with high dollar values attached to the most attractive warez, most warez traders should easily clear both the \$1,000 and \$2,500 thresholds.⁴⁸

One other note about retail values. All infringements committed during the 180 day period counts towards the threshold. Should the government desire, it could combine any infringements committed offline with warez trading to boost the overall retail value of infringement.

Statute of Limitations

The statute of limitations for criminal copyright infringement is five years.⁴⁹ In practice, the government has shown little interest in prosecuting older cases, which present significant evidentiary problems that may make them impossible to win.

copyrighted works are not marketed through normal retail channels. Examples include motion pictures prints distributed only for theatrical release, and beta-test versions of computer programs. In such cases, the courts may look to the suggested retail price, the wholesale price, the replacement cost of the item, or financial injury caused to the copyright owner.

H.R. REP. 102-997, at 6-7 (1992).

⁴⁶ U.S. SENTENCING GUIDELINES MANUAL §2B5.3, app. 1, available at <http://www.ussc.gov/2002guid/2002guid.pdf>.

⁴⁷ *Id.*, §2B5.3, app. 2.

⁴⁸ Even smaller players like Levy, Thornton and Fitzgerald easily cleared the felony threshold (stipulating to \$5,000, \$9,638 and over \$40,000, respectively).

⁴⁹ 17 U.S.C. §507(a), available at <http://www4.law.cornell.edu/uscode/17/507.html>.

5. OTHER CRIMINAL LIABILITY OF WAREZ TRADING.

Congress has made a significant number of changes to intellectual property-oriented criminal laws in the past decade, giving the government a greater number of tools available to prosecute warez traders than were available at the time of LaMacchia's prosecution. So even if the government cannot or does not want to prosecute for copyright infringement, a warez trader may not be in the clear.⁵⁰

Anti-Circumvention Laws

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA), which included restrictions on circumventing technological measures that effectively control access to a copyrighted work.⁵¹ In addition, the law prohibits manufacturing, importing, offering to the public, providing, or otherwise trafficking in a device or service that circumvents such technological measures.⁵² Punishments for the first offense include a fine of up to \$500,000 and imprisonment of up to five years.⁵³

Every major warez distribution group has a cracker who specializes in disabling or bypassing software manufacturers' copyright protection devices. The cracker's behavior should violate the DMCA. Other members in the group should be eligible for prosecution as conspirators or aiders/abettors. While there are some exceptions to the law,⁵⁴ these exceptions are very technical in nature, and any person engaged in typical warez trading cannot make a credible argument to be covered by the exceptions.

Anti-Hacking Laws

The Computer Fraud and Abuse Act (the "CFAA"),⁵⁵ historically designed as an anti-hacking statute, has morphed into a general-purpose federal anti-trespassing law. Several provisions may apply to activities committed frequently by warez traders.

First, the CFAA criminalizes accessing computer systems without authorization to obtain information,⁵⁶ a provision that could apply to illegitimately obtaining warez from a copyright owner's computer system. Thus, for example, the CFAA may have been violated when Justin

⁵⁰ Of course, warez traders can be civilly sued for copyright infringement as well.

⁵¹ 17 U.S.C. §1201(a)(1), available at <http://www4.law.cornell.edu/uscode/17/1201.html>.

⁵² 17 U.S.C. §1201(a)(2) and §1201(b), available at <http://www4.law.cornell.edu/uscode/17/1201.html>. This law was used to prosecute David Rocci for distributing and selling mod chips that could allow game warez to be played on game consoles. See Press Release, U.S. Department of Justice, Justice Department Seizes Top Internet Site Involved in Copyright Piracy (Feb. 26, 2003), available at <http://www.usdoj.gov/criminal/cybercrime/rocciPlea.htm>.

⁵³ 17 U.S.C. §1204, available at <http://www4.law.cornell.edu/uscode/17/1204.html>.

⁵⁴ 17 U.S.C. §1201(d)-(j), available at <http://www4.law.cornell.edu/uscode/17/1201.html>. These exceptions cover libraries and universities, law enforcement, reverse engineering (in very limited circumstances), encryption research (in very limited circumstances), devices that protect minors from accessing harmful material on the Internet, the circumvention of devices to protect personal information, and security testing (in very limited circumstances).

⁵⁵ 18 U.S.C. §1030, available at <http://www4.law.cornell.edu/uscode/18/1030.html>.

⁵⁶ 18 U.S.C. §1030(a)(2)(C), available at <http://www4.law.cornell.edu/uscode/18/1030.html>. Portions of the Electronic Communications Privacy Act could also apply if the conduct involves hacking into email servers to obtain emails. 18 U.S.C. §2701, available at <http://www4.law.cornell.edu/uscode/18/2701.html>.

Robbins allowed PWA to take software from Microsoft's internal computer network. Punishment for the first offense can include imprisonment of up to five years and a fine if the act was committed for commercial advantage or private financial gain, if the value of the information taken was over \$5,000, or if the act furthered other crimes or torts (such as copyright infringement).⁵⁷

Second, the CFAA criminalizes accessing computer systems without authorization and causing damage.⁵⁸ In the warez context, this provision could apply to using third party computer networks without authorization to distribute warez or conduct group business (with the damage being the use of network resources). Punishment for the first offense can include imprisonment of up to five years and a fine if the damage was caused "recklessly."⁵⁹

In addition to the federal CFAA, many states have anti-hacking or anti-computer trespass statutes that would allow state prosecutors to bring suit.

Anti-Theft Laws

A warez trading operation may involve the theft of physical items. For example, Intel employees exchanged stolen Intel servers for access to PWA's warez database. At minimum, the Intel employees could be prosecuted for theft, and the other PWA members could be prosecuted for receiving stolen property or participating in a conspiracy to commit theft.

Trade Secret Protection Laws

In 1996, Congress passed the Economic Espionage Act,⁶⁰ which in practice has established a federal anti-trade secret misappropriation statute. Many states also have their own anti-misappropriation criminal laws. These laws could apply to warez trading with respect to any pre-release software versions (whether alpha, beta or golden master versions) that qualify as trade secrets, which should include many of the most coveted warez.

Copyright Management Information Integrity Laws

While the anti-circumvention provisions of the DMCA receive most of the media's attention, another portion of the DMCA—the "integrity of copyright management information"—could also apply to warez trading. Copyright management information ("CMI") includes, among other things, a copyrighted work's title, author and other named contributors ("credits"), user agreement and identifying numbers like ISBN or serial numbers.⁶¹

⁵⁷ 18 U.S.C. §1030(c)(2), available at <http://www4.law.cornell.edu/uscode/18/1030.html>.

⁵⁸ 18 U.S.C. §1030(a)(5)(A), available at <http://www4.law.cornell.edu/uscode/18/1030.html>. 18 U.S.C. §1030(a)(4) may also apply if the conduct was done knowingly with the intent to defraud and the value of the network usage exceeds \$5,000 in a year.

⁵⁹ 18 U.S.C. §1030(c)(4)(B), available at <http://www4.law.cornell.edu/uscode/18/1030.html>. The same penalties applies if the prosecution is brought under 18 U.S.C. §1030(a)(4).

⁶⁰ 18 U.S.C. §§1831-39, available at <http://www4.law.cornell.edu/uscode/18/p1ch90.html>. Section 1832 most specifically applies to the warez trading context.

⁶¹ Copyright Management Information is defined as "(1) the title and other information identifying the work, including the information set forth on a notice of copyright, (2) the name of, and other identifying information about, the author of a work, (3) the name of, and other identifying information about, the copyright owner of the work,

The CMI integrity provisions prohibit providing (or distributing or importing for distribution) false CMI “knowingly and with the intent to induce, enable, facilitate, or conceal infringement.”⁶² They also prohibit removing or altering CMI, or distributing (or importing for distribution) CMI knowing it has been improperly removed or altered.⁶³ Punishments mirror those applicable to the anti-circumvention provisions: for the first offense, a fine of up to \$500,000 and imprisonment of up to five years.⁶⁴

Warez trading can implicate the CMI integrity provisions in two ways. First, in some cases, crackers may remove or alter CMI as part of the crack. Second, adding a .nfo file could be interpreted as providing false CMI with the intent to induce or enable infringement. The .nfo file’s wording may make a difference, but claiming “authorship” of a crack approaches the line (if not crossing it). Once again, all participants in a group should have joint liability for violation, either directly for distributing or indirectly as conspirators or aiders/abettors.

In addition to the DMCA’s CMI integrity provisions, the Copyright Act separately prohibits, with fraudulent intent, placing a false copyright notice⁶⁵ or removing or altering a copyright notice.⁶⁶ Because the associated punishment is only a \$2,500 fine, these provisions are rarely enforced.

6. CRIMINAL COPYRIGHT PROSECUTIONS OF WAREZ TRADERS.

As can be seen from the discussion in Section 4, a typical warez trader has few viable defenses to a criminal copyright prosecution. Not surprisingly, warez traders have been successfully convicted of criminal copyright infringement. Appendix A provides a table of publicized warez-related prosecutions that have resulted in a conviction and sentence.

Impressively, the Department of Justice has won every publicized case they have brought under the NET Act. This suggests that the department is carefully selecting defendants and preparing cases.

Not coincidentally, almost all warez trading defendants plead guilty when charged. At least some defendants do so because accepting responsibility can reduce sentences.⁶⁷ Others may

including the information set forth in a notice of copyright, (4) with the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work, (5) with the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work, (6) terms and conditions for use of the work, (7) identifying numbers or symbols referring to such information or links to such information, and (8) such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.” 17 U.S.C. §1202(c), available at <http://www4.law.cornell.edu/uscode/17/1202.html>.

⁶² 17 U.S.C. §1202(a), available at <http://www4.law.cornell.edu/uscode/17/1202.html>.

⁶³ 17 U.S.C. §1202(b), available at <http://www4.law.cornell.edu/uscode/17/1202.html>.

⁶⁴ 17 U.S.C. §1204, available at <http://www4.law.cornell.edu/uscode/17/1204.html>.

⁶⁵ 17 U.S.C. §506(c), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

⁶⁶ 17 U.S.C. §506(d), available at <http://www4.law.cornell.edu/uscode/17/506.html>.

⁶⁷ U.S. SENTENCING GUIDELINES MANUAL §3E1.1, available at <http://www.uscourts.gov/2002guid/2002guid.pdf>.

plead because of the culture of warez traders, who know that they are playing a game that involves both winning and losing and thus may willingly accept losing if they feel they were outsmarted by the Feds.

Whatever the reasons, only two defendants, Christian Morley (PWA) and Tony Walker (Fastlane) have taken their case to a jury, and both lost. Morley's decision may have cost him because he received the longest sentence of any PWA defendant (even longer than the purported ringleader, Robin Rothberg). The effect of Tony Walker's decision on his sentence is not clear.

At least 19 warez trading defendants have received jail sentences. Of the defendants receiving jail sentences, the average length has been 25.7 months; the longest jail sentence was 46 months and the shortest was 4 months.⁶⁸ It is hard to draw many conclusive inferences about variations in sentences due to a defendant's role in the warez distribution group. Generally, a warez group leader is likely to get the harshest sentence of the group, and mere participants (as opposed to leaders) often get probation instead of jail time. Otherwise, there has not been a discernable pattern illustrating variations in sentence based on having a role as a cracker, a courier, a systems administrator or something else.

Some specific details about some of the prosecutions:

Jeffrey Levy

In August 1999, Jeffrey Levy, a 22-year old University of Oregon senior, became the first individual convicted under the Act. He was a small-time trader of music and movies in addition to traditional warez. A "conservative estimate" of his warez's retail value was \$70,000.⁶⁹ but he pleaded guilty to distributing warez with a retail value of at least \$5,000 and was sentenced to 2 years probation.⁷⁰

Because Levy was not a major warez trader, normally he would have escaped prosecutorial attention. However, three months prior to his arrest, Congress angrily demanded that the government deliver some scalps under the NET Act,⁷¹ and Levy appears to have been a timely and easy target.

Eric Thornton

⁶⁸ Note that these calculations are based on the initial sentence. Some defendants, especially some DrinkOrDie defendants, subsequently received reduced sentences, presumably due to their cooperation with the government.

⁶⁹ Press Release, U.S. Department of Justice, Defendant Sentenced for First Criminal Copyright Conviction Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet (Nov. 23, 1999), available at <http://www.cybercrime.gov/levy2rls.htm>.

⁷⁰ *Id.*

⁷¹ At a hearing of the House Judiciary Committee's Subcommittee on Courts and Intellectual Property in May 1999, Rep. Coble demanded to know why there had been no convictions under the NET Act in 18 months despite the industry lobbyists' arguments that "there is no shortage of potential prosecutions that could be pursued under the Act." *Oversight Hearing on the Implementation of the NET Act and Enforcement Against Internet Piracy Before the House Judiciary Committee's Subcomm. on Courts and Intellectual Property* (May 12, 1999) (statement of Rep. Coble), available at <http://www.house.gov/judiciary/cobl0512.htm>.

Eric John Thornton, another small warez trader who operated a website called “No Patience,” was the second person convicted under the NET Act. In one specific instance, a third party downloaded 20 software programs with a retail value of \$9,638.⁷² Thornton pleaded guilty to a misdemeanor violation of the Act⁷³ and was sentenced to five years probation.⁷⁴ In an unusual twist, he was required to post a cautionary tale on his website for 18 months.⁷⁵ Thornton’s prosecution resembles Levy’s in import and timing, suggesting that both prosecutions were hurriedly initiated in response to Congress’ scalp demands but Thornton’s just took longer.

Brian Baltutat

Brian Baltutat was a more substantial warez trader than Levy or Thornton, but only slightly. He operated a website called “Hacker Hurricane” that offered 142 software programs for downloading and was visited by 65,000 people.⁷⁶ He was sentenced to 3 years probation and 180 days home confinement.⁷⁷

Fastlane

In February 2001, the government finally scored a major bust by arresting nine members of the warez distribution group Fastlane.⁷⁸ The FBI infiltrated the group by setting up and

⁷² Press Release, U.S. Department of Justice, Virginia Man Pleads Guilty to Charges Filed Under the “No Electronic Theft” (NET) Act for Unlawful Distribution of Software on the Internet (Dec. 22, 1999), *available at* <http://www.cybercrime.gov/thornton.htm>.

⁷³ Bill Miller, *Giveaways Costly for Web Pirate*, WASH. POST, Dec. 23, 1999, at B1.

⁷⁴ *Internet Pirate to Pay Restitution*, WASH. POST, Mar. 4, 2000, at B2.

⁷⁵ Miller, *supra* note 73, at B1. The announcement, perhaps ghost-written by the Department of Justice, reads:
All you WaReZ ToadZ out there need to read this!!!

I am out of the WaReZ business. I have been contributing to the WaReZ scene for some time. OK!
OK! I guess I knew it was illegal - but hell, everyone was doing it.

One day, I was minding my own business at home when I heard a knock on my door. When I opened it, I was staring at gold badges being held by two FBI agents. They explained to me that I had been committing federal copyright infringement. They had been investigating my website with the assistance of the Business Software Alliance. They had even seized evidence from my ISP. Since I was facing a very serious felony charge I came clean with them. I was charged and now have a federal conviction.

I didn’t think anyone cared about WaRez distribution on the Internet.

Boy! Was I wrong!

⁷⁶ Press Release, U.S. Department of Justice, Man Sentenced in Michigan for Offering Software Programs for Free Downloading on “Hacker Hurricane” Web Site (Jan. 30, 2001), *available at* <http://www.cybercrime.gov/baltutatsent.htm>.

⁷⁷ *Id.*

⁷⁸ The individual Fastlane defendants are:

Ryan Breeding, aka “river,” 26, of Oklahoma City, OK.

Steve Deal, aka “Doobie” and “Dewbie,” 36, of Trenton, NJ.

Glendon Martin, aka “TeRRiFiC,” 25, of Garland, TX.

Shane McIntyre, aka “Crypto,” 22, of Boynton Beach, FL.

James Milne, aka “lordchaos” and “lc,” 19, of Shawnee, KN.

Bjorn Schneider, aka “airwalker,” “a|walker” and “aw,” 20, of Falmouth, MA.

Kevin Vaughan, aka “DaBoo,” 19, of Raleigh, NC.

Tony Walker, aka “SyS,” 31, of San Diego, CA.

Tae Yuan Wang, aka “Terry Wang” and “Prometh,” 19, of Bellevue, WA.

Press Release, U.S. Department of Justice, Nine Indicted in Chicago in \$1 Million “Fastlane” Software Piracy Conspiracy (Feb. 16, 2001), *available at* <http://www.cybercrime.gov/fastlane.htm>.

surreptitiously operating a computer site known as Super Dimensional Fortress Macros (SDFM).⁷⁹ SDFM had 697 gigabytes uploaded and 1.9 terabytes downloaded between January to September 2000, with a total retail value over \$1 million.⁸⁰

All defendants were charged with one count of conspiracy to commit copyright infringement, and eight were charged with one count of committing copyright infringement.⁸¹ Eight of the nine defendants pleaded guilty, while one defendant (Tony Walker) was found guilty at a jury trial.⁸² Three defendants received jail sentences ranging from five to thirty months,⁸³ and the others received probation of three years.

Pirates With Attitude

Following Fastlane, PWA⁸⁴ was the next major warez distribution group busted. The group operated 13 FTP servers, with its flagship site Sentinel housed at the University of Sherbrooke.⁸⁵ Sentinel had over 30,000 warez and more than 100 users.⁸⁶

⁷⁹ *Id.*

⁸⁰ *Id.* Other Fastlane-associated websites include Sacred Halls (SH) (operated by Milne), The Good News (TGN) (operated by Martin) and 4:20 (operated by Vaughan). *Id.*

⁸¹ *Id.* Kevin Vaughan was not charged with committing copyright infringement.

⁸² See *United States v. Deal*, No. 00-CR-774 (N.D. Ill. 2002), available at <http://pacer.ilnd.uscourts.gov>.

⁸³ See *id.*

⁸⁴ The individual Pirates With Attitude defendants are:

Convicted members of Pirates With Attitudes:

Steven Ahnen, aka "Code3," 44, of Sarasota, FL.

Diane Dionne, aka "Akasha," 41, of West Palm Beach, FL.

Christian Morley, aka "Mercy" 29, of Salem, MA.

Thomas Oliver, aka "Rambone," 36, of Aurora, IL.

Jason Phillips, aka "Corv8," 31, of Plano, TX.

Justin Robbins, aka "Warlock," 26, of Lake Station, IN (Microsoft employee).

Robin Rothberg, aka "Marlenus," 34, of Newburyport, MA.

Jason Slater, aka "Technic," 31, of Sunnyvale, CA.

Mark Stone, aka "Stoned," 36, of Fountain Valley, CA.

Todd Veillette, aka "Gizmo," 42, of Oakdale, CT.

Convicted Intel employees:

Tyrone Augustine, 30, of New Rochelle, NY.

Brian Boyanovsky, aka "Boynger," 26, of Aloha, OR.

John Geissberger, 39, of Knoxville, TN.

Brian Riley, 32, of Portland, OR.

Gene Tacy, 27, of Hampstead, NH.

Fugitive members of Pirates With Attitude:

Kaj Bjorlin, aka "Darklord," Sweden.

Mark Veerboken, aka "Shiffie," Belgium.

Press Release, U.S. Department of Justice, Leader Of Software Piracy Sentenced To 18 Months In Prison (May 15, 2002), available at http://www.cybercrime.gov/rothbergSent_pirates.htm [hereinafter Rothberg Sentenced Press Release]. See generally *United States v. Rothberg*, No. 00-CR-85 (N.D. Ill. 2002), available at

<http://pacer.ilnd.uscourts.gov>; Special November 1999 Grand Jury Indictment, *United States v. Rothberg*, No. 00-CR-85 (N.D. Ill. 2002).

⁸⁵ Rothberg Sentenced Press Release, *supra* note 84.

⁸⁶ *Id.*

Seventeen defendants were indicted: twelve PWA members and five Intel employees who supplied computer hardware in exchange for access rights to the warez servers.⁸⁷ Following the indictments, many defendants entered into plea agreements. The government then claimed the warez had a retail value of over \$10 million.⁸⁸ A group of defendants jointly moved to limit this retail value based on expectations the defendants formed while negotiating their plea agreements. The judge rejected the motion but permitted defendants to rescind their plea agreements, and thus withdraw their guilty pleas, if they chose to.⁸⁹ None did.⁹⁰

A group of defendants then petitioned the court to set a lower retail value, and using debatable methodologies, the court set the value at \$1,424,640.⁹¹ With the retail value established, individual defendants were sentenced.

Robin Rothberg, the PWA's purported leader, entered a blind guilty plea⁹² but subsequently requested downward departure from the Sentencing Guidelines.⁹³ After obtaining some relief from the court on that front, he was sentenced to eighteen months in prison.⁹⁴

Another PWA member, Christian Morley, did not negotiate a plea agreement and instead took his case to trial. A jury found him guilty, and he was sentenced to two years in prison.⁹⁵ Two other defendants, Jason Slater and Justin Robbins, received jail sentences of eight months and seven months, respectively.⁹⁶ Nine defendants received 5 years probation, and two defendants (Thomas Oliver and Steven Ahnen) each received 3 years probation.⁹⁷ Two defendants remain at large.⁹⁸

Operations Buccaneer, Bandwidth and Digital Piratez

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.⁹⁹

⁸⁷ *Id.*

⁸⁸ United States v. Rothberg, 2002 WL 171963, *1 (N.D. Ill. 2002).

⁸⁹ United States v. Rothberg, 2001 WL 1654758 (N.D. Ill. 2001).

⁹⁰ United States v. Rothberg, 2002 WL 171963, *2 (N.D. Ill. 2002).

⁹¹ *Id.* at *6.

⁹² A "blind" plea is made without the benefit of a plea agreement. United States v. Rothberg, 222 F. Supp. 2d 1009, 1012 (N.D. Ill. 2002).

⁹³ *Id.* Rothberg received a 2 level downward revision based on his absence of a profit motive, his extraordinary acceptance of responsibility and his family circumstances. *Id.*

⁹⁴ Rothberg Sentenced Press Release, *supra* note 84.

⁹⁵ *Id.*

⁹⁶ See United States v. Rothberg, No. 00-CR-85 (N.D. Ill. 2002), available at <http://pacel.ilnd.uscourts.gov>.

⁹⁷ See *id.*

⁹⁸ The fugitives are Mark Veerboken and Kaj Bjorlin. Rothberg Sentenced Press Release, *supra* note 84.

⁹⁹ Press Release, U.S. Department of Justice, Federal Law Enforcement Targets International Internet Piracy Syndicates (Dec. 11, 2001), available at <http://www.cybercrime.gov/warezoperations.htm>.

Operation Buccaneer¹⁰⁰ primarily targeted DrinkOrDie, one of the oldest and best-known warez distribution groups.¹⁰¹ Among other accomplishments, the group claimed to have released Microsoft Windows 95 two weeks prior to its commercial release.¹⁰² The group allegedly had two leaders, two or three council members, twelve to fifteen staff members, and approximately 65 general members.¹⁰³ The groups' archives contained, in some cases, two terabytes of warez estimated to have a retail value in the hundreds of millions of dollars.¹⁰⁴ However, as part of plea agreements, Operation Buccaneer defendants admitted that the retail value of their pirated software was between \$2.5 million and \$5 million.¹⁰⁵

¹⁰⁰ Individual defendants prosecuted pursuant to Operation Buccaneer include:

Richard Berry, aka "Flood," 34, of Rockville, MD (VP and CTO at Streampipe.com).

Anthony Buchanan, aka "spaceace," of Eugene, OR.

Andrew Clardy, 49, aka "DooDad," of Galesburg, IL (network technician at Carl Sandburg College).

Myron Cole, aka "t3rminal," of Warminster, PA.

Derek Eiser, aka "Psychod," of Philadelphia, PA.

Barry Erickson, aka "rads1," 35, of Eugene, OR (systems engineer at Symantec Corporation).

Hew Raymond Griffiths, aka "Bandido," 40, of Bateau Bay, Australia.

David A Grimes, aka "Chevelle," 25, of Arlington, TX (computer engineer at Check Point Software).

Robert Gross, aka "targetpractice," of Horsham, PA.

Nathan Hunt, aka "Azide," 25, of Waterford, PA.

Kentaga Kartadinata, aka "Tenkuken," 29, of Los Angeles, CA.

Michael Kelly, aka "Erupt," 21, of Miama, FL (network administrator for Gator Leasing).

Stacey Nawara, aka "Avec," 34, of Rosenberg, TX.

Mike Nguyen, aka "Hackrat," 26, of Los Angeles, CA.

Sabuj Pattanayek, aka "Buj," 20, of Durham, NC.

Shane Pitman, aka "Pitbull," 31, of Conover, NC.

John Riffe, aka "blue" or "blueadept," 32, of Port St. John, FL.

David Russo, aka "Ange," 49, of Warwick, RI.

John Sankus, aka "eriFilleH," 28, of Philadelphia, PA.

Christopher Tresco, aka "BigRar," 23, of Boston, MA (MIT systems administrator).

Press Release, U.S. Department of Justice, Warez Leader Sentenced to 46 Months (May 17, 2002), *available at* <http://www.cybercrime.gov/sankusSent.htm>; U.S. Department of Justice, Operation Buccaneer Defendants (Jan. 27, 2003), *available at* <http://www.cybercrime.gov/ob/Dchart.htm>; Press Release, U.S. Department of Justice, Defendant Indicted in Connection with Operating Illegal Internet Software Piracy Group (Mar. 12, 2003), *available at* <http://www.cybercrime.gov/griffithsIndict.htm>; Press Release, U.S. Department of Justice, Warwick Man Admits Participation in Software Piracy Network (Apr. 24, 2003), *available at* <http://www.cybercrime.gov/russoPlea.htm>; Press Release, U.S. Department of Justice, Former Leader of Razor 1911, the Oldest Game Software Piracy Ring on the Internet, Sentenced (June 6, 2003), *available at* <http://www.cybercrime.gov/pitmanSent.htm>.

Specific sentences are described in *United States v. Berry*, No. 02-CR-246 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Buchanan*, No. 02-CR-374 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Clardy*, No. 02-CR-10035 (C.D. Ill. 2003), *available at* <http://pacer.ilcd.uscourts.gov>; *United States v. Cole*, No. 02-CR-300 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Eiser*, No. 02-CR-284 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Erickson*, No. 02-CR-89 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Gross*, No. 02-CR-299 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Hunt*, No. 02-CR-106 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Kelly*, No. 02-CR-112 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Nawara*, 02-CR-90 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Nyugen*, No. 02-CR-63 (C.D. Cal. 2003), *available at* <http://pacer.cacd.uscourts.gov>; *United States v. Pattanayek*, 02-CR-118 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Riffe*, No. 02-CR-156 (E.D. Va. 2003), *available at* <http://pacer.vaed.uscourts.gov>; *United States v. Tresco*, No. 02-CR-132 (E.D. Va. 2003), *available at*

Of the 17 Operation Buccaneer defendants sentenced as of July 1, 2003, eleven received jail sentences ranging from 18 to 46 months (although at least five of these defendants had their sentences reduced in exchange for government cooperation), one received five years probation, one received one year probation and the other four received two years probation.¹⁰⁶ Also, the Department of Justice has announced the indictment and intended extradition of Australian resident Hew Raymond Griffiths, an alleged DrinkOrDie co-leader.¹⁰⁷

Operation Bandwidth¹⁰⁸ primarily targeted the group Rogue Warriorz (RWZ), another major warez distribution group. Undercover FBI, EPA and Defense Criminal Investigative Services

<http://pacer.vaed.uscourts.gov>.

¹⁰¹ Fact Sheet, U.S. Customs Service, The DrinkOrDie Group: What is It? Who Are They? What is the DrinkOrDie Group? (Dec. 11, 2001), available at <http://www.customs.ustreas.gov/hot-new/pressrel/2001/1211-01.htm>. But see Farhad Manjoo, Were DrinkOrDie Raids Overkill?, Wired News (Dec. 13, 2001), at <http://www.wired.com/news/print/0,1294,49096,00.html> (arguing that “DrinkOrDie was small potatoes in the world of software theft”). Other groups targeted by Operation Buccaneer include Razor1911, RiSCISO, MYTH, POPZ, RequestToSend (RTS), WeLoveWarez (WLW), and RiSC. U.S. Department of Justice, Operation Buccaneer: The Investigation (July 19, 2002), available at <http://www.cybercrime.gov/ob/OBinvest.htm>.

¹⁰² Fact Sheet, U.S. Customs Service, The DrinkOrDie Group: What is It? Who Are They? What is the DrinkOrDie Group? (Dec. 11, 2001), available at <http://www.customs.ustreas.gov/hot-new/pressrel/2001/1211-01.htm>.

¹⁰³ Statement of Facts, United States v. Tresco, No. 02-CR-132-A, at 2 (E.D. Va. 2002).

¹⁰⁴ U.S. Department of Justice, Operation Buccaneer: The Investigation (July 19, 2002), available at <http://www.cybercrime.gov/ob/OBinvest.htm>. A single file server operated by DrinkOrDie, “Fatal Error,” was alleged to have over 900 gigabytes and 15,000 titles of software. Criminal Information, United States v. Tresco, No. 02-CR-132-A, at 3 (E.D. Va. 2002).

¹⁰⁵ See, e.g., Plea Agreement, United States v. Tresco, No. 02-CR-132-A, at 2 (E.D. Va. 2002); Software Pirate Pleads Guilty, GlobeandMail.com, Apr. 4, 2002, at http://www.globeandmail.com/servlet/RTGAMArticleHTMLTemplate?tf=RT/fullstory_print.html&cf=RT/config-neutral&slug=gtcopy&date=20020404&archive=RTGAM&site=Technology; Press Release, U.S. Department of Justice, Leader of Internet Software Piracy Organization Pleads Guilty to Conspiracy (Feb. 27, 2002), available at <http://www.cybercrime.gov/sankusPlea.htm>.

¹⁰⁶ U.S. Department of Justice, Operation Buccaneer Defendants (Jan. 27, 2003), available at <http://www.cybercrime.gov/ob/Dchart.htm>.

¹⁰⁷ Press Release, U.S. Department of Justice, Defendant Indicted in Connection with Operating Illegal Internet Software Piracy Group (Mar. 12, 2003), available at <http://www.cybercrime.gov/griffithsIndict.htm>.

¹⁰⁸ Individual defendants prosecuted pursuant to Operation Bandwidth include:

John J. Amorosi, aka “Sloanman”, 22, of Falls Church, VA.

Wolf Bachenor, aka Walter Bachenor, aka “Drinfotheif”, “DrinfoTHV” and “Doctor”, 51, of Park Slope, NY.

David Brandt, aka “Bocephus”, 35, of Wake Village, TX.

Alexander Castaneda, aka “Prentice” and “Alex”, 20, of Federal Way, WA.

Jacob Paul Clapton, aka “Axxess”, 29, of Livermore, CA.

Lukasz Doupal, aka “Luk@s”, 24, of Brooklyn, NY.

Jonathan Dow, aka “Demon Furby”, 34, of Ilion, NY.

Jorge Garcia, Jr., aka “Lh” and “Lordhacker”, 29, of Reddick, FL.

Bryan Ray Harshman, aka “Carrier”, 22, of St. Joseph, MO.

Mark Konarske, aka “Markus” and “Markruss”, 41, of Flat Rock, MN.

Timothy J. Lastoria, aka “Waldorf”, 24, of Brecksville, OH.

David Lowe, aka “Dragon”, 41, of Akron, OH.

Christopher Mastrangelo, aka “Floyd”, 31, of Toms River, NJ.

Michael Meacham, aka “Dvorak”, 35, of Barberton, OH

Suzanne Peace, aka “Peaces”, 37, of Lombard, IL.

Lindle Romero, aka “Rahman”, 37, of Houston, TX.

Elisa Sarino, aka “Elisa” and “ElisaEGO”, 27, of San Jose, CA.

agents infiltrated the group's Shatnet site,¹⁰⁹ which contained over 9,000 warez with a retail value of approximately \$7 million.¹¹⁰ The Operation Bandwidth prosecutions are ongoing, as are those associated with Operation Digital Piratez.

William Fitzgerald

William Fitzgerald, a 53 year old computer technician for Arlington County, Virginia, obtained warez from IRC and posted them on three computers he ran from his home.¹¹¹ Fitzgerald stipulated that the warez were worth between \$40,000 and \$70,000.¹¹² He pleaded guilty to one count of criminal copyright infringement and was sentenced to four months in prison and four months of home confinement.¹¹³ Given the Department of Justice's recent large initiatives to take down major warez groups, the decision to prosecute Fitzgerald for relatively small-scale activity is a little puzzling.

Movie Traders

While not typical warez traders, two individuals have been prosecuted for distributing pre-release versions of movies. Jason Spatafore distributed parts of *Star Wars Episode I: The Phantom Menace*,¹¹⁴ for which he sentenced to two years probation.¹¹⁵ Kerry Gonzalez posted an unfinished "work print" copy of *The Hulk* to a movie bootleg website two weeks prior to the movie's opening;¹¹⁶ his sentence is pending.

7. CASUALTIES IN THE WAR AGAINST WAREZ.

In Congress' legislative debates about the NET Act, warez traders were portrayed as the poster children for rampant Internet piracy. However, other infringement activities, such as "softlifting" (exceeding a license to make unauthorized copies) and commercial piracy have a

Jeffrey Sasser, aka "Inferno" and Inferno00", 41, of Charlotte, NC.

Peter M. Semadeni, aka "Davinci" and "Rev. Wolf", 28, of Overland Park, KS.

Dean Wuestenberg, aka "Xochi", 44, of Donahue, IA.

Joseph Yano, aka "Jozef", 34, of Saskatoon, SA.

Press Release, U.S. Department of Justice, Federal Indictments Returned in Las Vegas Against Software Pirates Nabbed in Operation Bandwidth (June 11, 2002), available at <http://www.cybercrime.gov/bandwidth.htm>.

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ Statement of Facts, United States v. Fitzgerald, Case No. 0-2620-A (E.D. Va. 2003), available at <http://www.usdoj.gov/usao/vae/ArchivePress/FebruaryPDFArchive/fitzgeraldsof020303.pdf>.

¹¹² Press Release, U.S. Department of Justice, Arlington, Virginia Man Pleads Guilty to Distributing Pirated Software Over the Internet (Feb. 3, 2003), available at <http://www.cybercrime.gov/fitzgeraldPlea.htm>.

¹¹³ Press Release, U.S. Department of Justice, Arlington County Man is Sentenced to Federal Prison for Distributing Pirated Computer Software over the Internet (Apr. 25, 2003), available at <http://www.cybercrime.gov/fitzgeraldSent.htm>.

¹¹⁴ Press Release, U.S. Department of Justice, Man Pleads Guilty to Internet Piracy of Star Wars Film (Dec. 15, 2000), available at <http://www.cybercrime.gov/spataforeplea.htm>.

¹¹⁵ Jason Spatafore, DisMan's Online Journey, at <http://www.spatafore.net/disman/thephoenixmenace.shtml> (last visited May 19, 2003).

¹¹⁶ Troy Graham, *Federal Case Made of 'Hulk' Piracy*, PHILADELPHIA INQUIRER, June 26, 2003, at H12, available at http://www.philly.com/mld/inquirer/news/local/states/new_jersey/6172522.htm?template=contentModules/printstory.jsp.

significantly greater impact on copyright owner revenues. So why did Congress target warez traders despite their relatively small footprint on overall piracy?

Despite the obvious inspiration—the *LaMacchia* judge invited Congress to fix the problem¹¹⁷—another reason may offer a better explanation. Americans hate enemies that are impossible to locate and destroy using command-and-control tactics. And that describes warez traders; they operate stealthily, behind the Internet’s opaque veil, and are impossible to spot offline. Further, online, warez traders exude an air of cockiness and invincibility that members of Congress may interpret as a provocative challenge to their power and authority.

These attributes make warez traders the unseen enemy that must be destroyed. In a sense, Congress declared war against warez traders through the NET Act. Now Congress wants to triumphantly claim victory over villains who do not fight fair.

While a few scalps have been taken in Congress’ war against warez, there has been no victory, and it will never come. No quantum of stiffened criminal penalties will change that result. Warez trading is about ego, prestige and reputation, and so long as intangible assets are fenced off, a group of enthusiasts will seek recognition for breaching the fences. In that sense, increased criminal penalties counterproductively make warez trading more attractive by making it a little more daring and impressive.

Meanwhile, every war has a collateral cost, and the war against warez is no exception. In the process of outlawing warez trading, Congress also criminalized most American citizens. For example, tens of millions of Americans engage in P2P file sharing, which should be just as criminal as warez trading. But even Americans who do not trade files may break the law by willfully infringing \$1,000 of retail value in 180 days, or. In our digital society, the average American makes copies, lots of them, every day just to function. This makes \$5.56 of infringing copies per day a criminal threshold that far too many Americans meet easily.

But so what? Systematic noncompliance with the law is a fact of life in our overregulated society, and we have found ways to tolerate or ignore the associated risks. Meanwhile, with stretched prosecutorial resources, the risk of an average American being prosecuted for routine acts of copyright infringement is effectively zero. Warez traders get a little more prosecutorial attention,¹¹⁸ but even the number of “garden-variety” warez traders who have been prosecuted is trivial.

¹¹⁷ The judge wrote:

Criminal as well as civil penalties should probably attach to willful, multiple indictments of copyright infringement even absent a commercial motive on the part of the infringer. One can envision ways that the copyright law could be modified to permit such prosecution. But, [i]t is the legislature, not the Court, which is to define a crime, and ordain its punishment.

United States v. LaMacchia, 871 F. Supp. 535, 545 (D. Mass. 1994) (quotation omitted), *available at* http://www.loundy.com/CASES/US_v_LaMacchia.html.

¹¹⁸ See DOJ IP Crimes Manual, *supra* note 8, §III(E)(4) (discussing the factors that evidence “egregious” Internet infringement).

On the other hand, criminal copyright infringement has gone too far, and everyone—even Congress—knows it.¹¹⁹ By over-criminalizing activities made mandatory by our digital society, criminal copyright law has become unjust, making it impossible for the average American to respect the law.¹²⁰

Despite this, the trend is for tougher and more pervasive criminal laws. Congress has been captured by well-funded special interests who have successfully convinced Congress that the piracy situation is cataclysmic. Thus, Congress regularly holds hearings demanding more pirate scalps,¹²¹ and the newly introduced Piracy Deterrence and Education Act of 2003¹²² is yet another attempt to force compliance with the law. And when Sen. Hatch “jokes” about blowing up the computers of copyright infringers,¹²³ he is not joking at all—he is expressing frustration at Congress’ seeming inability to get Americans to respect the laws that industry lobbyists have persuaded him and his peers are so desperately needed.

To satisfy Congress, the Department of Justice will have to pursue high-profile enforcements. However, to avoid mass panic, the cases the Department of Justice pursues must permit the average Americans to distinguish the criminal’s conduct from their own. Warez traders provide a perfect target for the Department of Justice to balance these conflicting objectives. As a result, it seems likely that more warez traders will be going to prison.

¹¹⁹ Lisa Friedman, Web Pirates Plunder On, L.A. Daily News, June 22, 2003, at <http://www.dailynews.com/cda/article/print/0,1674,200%257E20954%257E1471539,00.html> (quoting several members of Congress admitting that legislative efforts to stop piracy have failed).

¹²⁰ Tom R. Tyler, *Compliance with Intellectual Property Laws: A Psychological Perspective*, 29 N.Y.U. J. INT’L L. 219 (Fall 1996-Winter 1997).

¹²¹ E.g., DOJ, Hill Subcommittee Agree on Need for Piracy Prosecutions, Warren’s Wash. Internet Daily, Mar. 14, 2003, available at 2003 WL 16116847.

¹²² Piracy Deterrence and Education Act of 2003, H.R. 2517, 108th Cong. (2003), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2517ih.txt.pdf.

¹²³ Declan McCullagh, Senator OK with Zapping Pirates’ PCs, CNET News.com, June 18, 2003, at http://news.com.com/2102-1028_3-1018845.html?tag=ni_print.

Appendix A
Publicized Convictions Under the No Electronic Theft Act
(updated as of July 1, 2003)

Individual	Sentencing Date	Summary of Criminal Activity	Sentence
Jeffrey Levy	August 1999	Posted software, music, entertainment programs and movies with a retail value of at least \$5,000 to his website	2 years probation Internet use restricted
Eric Thornton	December 1999	Posted software with a retail value of at least \$9,638 to his website	5 years probation \$9,600 of restitution Must post notice on website for 18 months Cannot use computers (except for business or educational purposes) for 12 months
Brian Baltutat	October 2000	Posted infringing software to a website that was visited by 65,000 people	3 years probation 180 days home confinement (including a tether) Restitution 40 hours of community service. Cannot use the Internet Required to tell the owners of any computers he uses about his conviction
Jason Spatafore	December 2000	Electronically distributed portions of <i>Star Wars I</i>	2 years probation \$250 fine
Tyrone Augustine (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Brian Boyansky (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation \$2,000 fine
Diane Dionne (PWA)	April 2002	Senior member of and packager for warez group trading software with retail value of \$1,424,640	5 years probation
John Geissberger (PWA)	April 2002	Intel employee who participated warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Christian Morley (PWA)	April 2002	Senior member of warez group trading software with retail value of \$1,424,640	24 months in prison 2 years supervised release [went to trial]
Jason Phillips (PWA)	April 2002	Member of warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Brian Riley (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation
Jason Slater (PWA)	April 2002	Senior member of warez group trading software with retail value of \$1,424,640. Alleged to be a cracker.	8 months in prison 2 years supervised release \$1,000 fine
Mark Stone (PWA)	April 2002	Member of warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Gene Tacy (PWA)	April 2002	Intel employee who participated in warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine

Todd Veillette (PWA)	April 2002	Member of and senior courier for warez group trading software with retail value of \$1,424,640	5 years probation \$5,000 fine
Barry Erickson (Buccaneer)	May 2002	Provided pre-release Symantec software to warez groups RisciISO and DrinkOrDie, founding member of warez group POPZ	33 months in prison (reduced in Nov. 2002 to 15 months) 2 years supervised release
David Grimes (Buccaneer)	May 2002	Provided pre-release Check Point software to DrinkOrDie; operated FTP site High Octane, which was affiliated with warez groups RiSC, MYTH, RTS and DrinkOrDie	37 months in prison
Thomas Oliver (PWA)	May 2002	Council member of warez group trading software with retail value of \$1,424,640	3 years probation \$5,000 fine
Robin Rothberg (PWA)	May 2002	Led and council member of warez group trading software with retail value of \$1,424,640	18 months in prison 3 years supervised release \$1,000 fine
John Sankus (Buccaneer)	May 2002	Led and managed warez group DrinkOrDie, participated in warez group Harm; traded software with retail value of between \$2.5 million and \$5 million	46 months in prison
Nathan Hunt (Buccaneer)	June 2002	Senior member of warez group DrinkOrDie, in 11 month period, provided 120 software programs for cracking and distribution. Stipulated to trading software with retail value of between \$2.5 million and \$5 million	33 months in prison (reduced November 2002 to 24 months) 3 years supervised release \$2,500 fine
Stacey Nawara (Buccaneer)	June 2002	Senior member of warez group RTS, Council member of warez group DrinkOrDie, courier for warez group Razor1911	30 months in prison (reduced in October 2002 to 30 days in jail (straight time or weekends) and 8 months community confinement) 3 years supervised release Assigned to mental health and substance abuse program \$1,000 fine No non-work Internet use
Richard Berry (Buccaneer)	July 2002	Longtime member of DrinkOrDie, provided them hardware, tested cracked warez and operated bounce sites	33 months in prison (reduced in October 2002 to 2 years probation including 12 months home confinement with electronic monitoring) 2 years supervised release
Andrew Clardy (Buccaneer)	July 2002	System administrator for DrinkOrDie's Dynamo server	41 months in prison 2 years supervised release
Michael Kelly (Buccaneer)	July 2002	Senior staff of DrinkOrDie, member of warez groups RISC, AMNESIA, CORE	Initial sentence: 33 months in prison 2 years supervised release 200 hours of community service Must notify employers of conviction In January 2003, the sentence was reduced to: 4 months in prison 3 years supervised release (including 8

			months home detention with electronic monitoring) 200 hours of community service Must notify employers of conviction
Sabuj Pattanayek (Buccaneer)	July 2002	Council member of and cracker for warez group DrinkOrDie, senior member of warez group RTS	41 months in prison 3 years supervised release 100 hours of community service \$1,000 fine
John Riffe (Buccaneer)	July 2002	Member of warez groups ShadowRealm (SRM), EXODUS	2 years probation 6 months home confinement with electronic monitoring 100 hours of community service
Tony Walker (Fastlane)	July 2002	Provided computer hardware to warez group Fastlane in exchange for access to software with retail value of \$1,000,000	5 months in prison (split with community confinement) 1 year supervised release \$3,000 fine [went to trial March 2002]
Anthony Buchanan (Buccaneer)	August 2002	Participated in warez group POPZ, DrinkOrDie	2 years probation 6 months home confinement with electronic monitoring 150 hours of community service
Steve Deal (Fastlane)	August 2002	Led warez group trading software with retail value of \$1,000,000	30 months in prison 3 years of supervised release
Robert Gross (Buccaneer)	August 2002	Participated in warez group DrinkOrDie	5 years probation 6 months home confinement 200 hours of community service
Glendon Martin (Fastlane)	August 2002	System administrator for warez group trading software with retail value of \$1,000,000	3 years probation \$1,000 fine
Shane McIntyre (Fastlane)	August 2002	Managed warez group trading software with retail value of \$1,000,000	3 years probation 180 days home confinement with electronic monitoring \$3,000 fine
James Milne (Fastlane)	August 2002	System administrator for warez group trading software with retail value of \$1,000,000	3 years probation
Bjorn Schneider (Fastlane)	August 2002	Managed warez group trading software with retail value of \$1,000,000	3 years probation
Christopher Tresco (Buccaneer)	August 2002	System administrator for DrinkOrDie (including operating a drop site)	33 months in prison (reduced in October 2002 to 6 months in prison and 7 months of community confinement) 2 years supervised release 100 hours of community service May not use the Internet for non-work related purposes
Kevin Vaughan (Fastlane)	August 2002	System administrator for warez group trading software with retail value of \$1,000,000	3 years probation
Tae Yuan Wang (Fastlane)	August 2002	Managed warez group trading software with retail value of \$1,000,000	3 years probation 300 hours of community service
Steven Ahnen (PWA)	September 2002	Council member for warez group trading software with retail value of \$1,424,640. Alleged to operate channel	3 years probation \$1,000 fine

		for the group and package software.	
Derek Eiser (Buccaneer)	September 2002	Participated in warez group DrinkOrDie	2 years probation, including 6 months home confinement \$500 fine
David Anderson (Buccaneer)	October 2002	Participated in warez group DrinkOrDie	12 months probation \$500 fine
Myron Cole (Buccaneer)	October 2002	Participated in warez group DrinkOrDie	2 years probation 150 hours community service
Justin Robbins (PWA)	October 2002	Council member of warez group trading software with retail value of \$1,424,640; supplied Microsoft software and allowed others to access Microsoft's internal network	7 months in prison 3 years of supervised release
Ryan Breeding (Fastlane)	February 2003	Provided computer hardware to warez group Fastlane in exchange for access to software with retail value of \$1,000,000	15 months in prison 2 years of supervised release \$6,000 fine
William Fitzgerald	April 2003	Operated pirate website allowing downloads of between \$40,000 and \$70,000	4 months in prison 4 months of home confinement \$3,000 fine
Shane Pitman (Buccaneer)	June 2003	Leader of warez group Razor1911	18 months in prison
Kent Kartadinata (Buccaneer)	June 2003	Operated email server for warez group DrinkOrDie	To be determined
Mike Nguyen (Buccaneer)	June 2003	Managed file servers for warez group DrinkOrDie	To be determined
David Russo (Buccaneer)	July 2003	Tester for warez group DrinkOrDie	To be determined
Kerry Gonzalez	September 2003	Distributed advance "work print" copy of <i>The Hulk</i>	To be determined

Appendix B Bibliography

Applicable Statutes

17 U.S.C. §506, <http://www4.law.cornell.edu/uscode/17/506.html>

18 U.S.C. §2319, <http://www4.law.cornell.edu/uscode/18/2319.html>

H.R. 2517, Piracy Deterrence and Education Act of 2003, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2517ih.txt.pdf (June 24, 2003 version)

United States Sentencing Guidelines §2B5.3, <http://www.ussc.gov/2002guid/2002guid.pdf>.

Department of Justice Resources

No Electronic Theft (NET) Act page, <http://www.cybercrime.gov/iplaws.htm#Xb>
[note: the DOJ appears to have stopped updating this page in 2001]

Intellectual Property Cases page, <http://www.cybercrime.gov/ipcases.htm>

Operation Buccaneer page, <http://www.cybercrime.gov/ob/OBMain.htm>

Operation Buccaneer convictions page, <http://www.cybercrime.gov/ob/Dchart.htm>
[note: the DOJ appears to have stopped updating this page January 2003]

Prosecuting Intellectual Property Crimes Manual,
<http://www.cybercrime.gov/ipmanual/03ipma.htm>

Commentators

Eric Goldman, *A Road to No Warez: the No Electronic Theft Act and Criminal Copyright Infringement*, 82 OR. L. REV. ____ (2003) (forthcoming).
[an expanded and more policy-oriented analysis of this subject]

Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L. Q. 835 (1999), <http://www.wulaw.wustl.edu/WULQ/77-3/773-835.pdf>.
[one of the most thoughtful articles on the subject]

Declan McCullagh's Politech, <http://www.politechbot.com/>
]Declan is a journalist who writes frequently on criminal copyright infringement issues]