7-1-2003

A Road to No Warez: The No Electronic Theft Act and Criminal Copyright Infringement

Eric Goldman
Santa Clara University School of Law, egoldman@gmail.com

ERIC GOLDMAN*

A Road to No Warez: The No Electronic Theft Act and Criminal Copyright Infringement

In the second half of the 1990s, copyright owners repeatedly sought Congress's help addressing the challenges posed by the Internet and other new technologies. Congress responded with a suite of new protections, including restrictions against circumvention,[1] longer copyright terms,[2] increased statutory damages,[3] and criminalization of willful non-commercial infringement.

This Article examines the latter of those changes, effectuated through the No Electronic Theft Act[4] (the "Act" or the "NET Act"). The Act represents a significant change to copyright law be cause it subtly shifts the paradigm underlying criminal copyright infringement. For 100 years, criminal infringement punished infringers who derived a commercial benefit based on someone else's copyrighted work. However, through the Act,

* Eric Goldman (*eric.goldman@marquette.edu*) is an Assistant Professor at Marquette University Law School in Milwaukee, WI. His personal home page is at http://eric_goldman.tripod.com. Julia Alpert Gladstone, a legal studies professor at Bryant College in Smithfield, RI, played a key role during the preparation of this Article, and the author extends special thanks to her. The author also thanks Orin Kerr, Lydia Pallas Loren, and Michael O'Hear for helpful comments and Theodore Potter and Camilla Tubbs for their research assistance. This Article originated from a project by the Intellectual Property Subcommittee, Cyberspace Law Committee, Business Law Section, American Bar Association.

[1] *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998), *available at* http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?Paddress=162.140.64.21&filename=publ304.pdf&directory=/diskc/wais/data/105_cong_public_laws (the DMCA).

[2] *See* Sonny Bono Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827 (1998), *available at* http://www.copyright.gov/legislation/s505.pdf.

[3] *See* Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, Pub. L. No. 106-160, 113 Stat. 1774 (1999), *available at* http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.3456.ENR.

[4] 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.

Congress adopted a paradigm that criminal copyright infringement is like physical-space theft,[5] specifically shoplifting.[6] As a result, the Act significantly extends the boundaries of criminal copyright infringement.[7]

Despite the extended criminal boundaries, a review of the post-passage developments suggests that the Act has been unexpectedly ineffective. To fully understand why, this Article focuses on a group of infringers known as warez traders. Warez, pronounced the same as "wares," are copies of infringed copyrighted works (often commercial software) with any copy protection mechanisms removed.[8] A warez trader has been defined as an individual "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."[9] More generally, warez traders are enthusiasts who trade or distribute warez as an avocation[10] and thus are a sociological

[5] *See*, *e.g.*, 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Leahy) ("[W]e value intellectual property . . . in the same way that we value the real and personal property of our citizens.").

[6] *Id.* ("Just as we will not tolerate the theft of software, CDs, books, or movie cassettes from a store, so we will not permit the stealing of intellectual property over the Internet."); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte) (analogizing between online piracy and retail shoplifting, saying that "[p]irating works online is the same as shoplifting a videotape, book or record from a store" and expressing a desire to prevent the Internet from becoming the "Home Shoplifting Network.").

[7] *See* 4 Melville B. Nimmer & David Nimmer, NIMMER ON COPYRIGHT § 15.01[B][2] (2002) (the NET Act defines criminal activity under the Copyright Act "much more widely than it had ever been drawn before under U.S. criminal copyright strictures.") [hereinafter NIMMER ON COPYRIGHT].

[8] *See The New Hacker's Dictionary: "W"*, *at* http://www.jargon.8hz.com/jargon 38.html#SEC45 (last visited Nov. 7, 2003). "Warez" is shorthand for "software," with the "z" a naming convention for pirated items (i.e., "applications" is shortened to appz, "games" becomes gamez, etc.). Stephen Granade, *Warez, Abandonware, and the Software Industry*, Brasslantern.com, *at* http://brass-lantern.org/community/companies/warez.html (last visited Nov. 7, 2003) [hereinafter Granade, *Warez*].

[9] *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) [hereinafter *Hearings*] (statement of Sandra A. Sellers, V.P. of Intellectual Property Education and Enforcement for the Software Publishers Association), *available at* http://commdocs.house.gov/committees/judiciary/hju48724.000/hju48724_0.htm.

[10] David Tetzlaff, *Yo-Ho-Ho and a Server of Warez*, *in* The World Wide Web and Contemporary Cultural Theory 104 (Andrew Herman & Thomas Swiss eds. 2000) ("Trading warez is not something its participants only do every now and then. It's a full-blown avocation that takes up a considerable amount of time."); *see* David McCandless, *Warez Wars*, WIRED, Apr. 1997 (discussing one warez trader who spent 12

group unique to the Internet.

While Congress did not specifically reference warez trading in the Act, warez traders were its prime target.[11] Yet, Congress did not fully understand this sociological group or their motivations, resulting in a law poorly tailored to conforming their behavior. But in drafting a broad law to cover warez trading, the Act overstates the harm experienced by copyright owners. This expansive standard for harm covers activities necessary to function in a digital society, unnecessarily turning too many average Americans into criminals. Corrective legislation is required to more precisely distinguish between truly culpable behavior and socially beneficial conduct.

Part I of this Article discusses the Act's development, from the *LaMacchia* case in 1994 through the President's signature in 1997. Part II discusses development since the Act's passage, including the difficulties implementing it and prosecutions brought under the Act. Part III analyzes the Act's consequences, including its weak effect on piracy and its misunderstanding of how to change warez traders' behavior. Part IV talks about problems created by the Act's scope, including the problems created by a weak definition of willfulness and a failure to distinguish between infringers and facilitators. Part V discusses a proposal to set an appropriate policy basis for imposing criminal liability for copyright infringement. The Article concludes with Part VI.

I

DEVELOPMENT OF THE ACT

A. The LaMacchia *Case*

Prior to the Act, criminal copyright infringement required willful infringement committed for commercial advantage or private financial gain.[12] A case involving David LaMacchia highlighted the limits of this statute.[13]

David LaMacchia was a twenty-one-year-old student at the

---

hours a day online and another who spent 6-10 hours a day during the week and 12-16 hours a day on the weekends), *available at* http:// hotwired.wired.com/collections/hacking_warez/5.04_warez_wars_pr.html [hereinafter McCandless, *Warez Wars*].

[11] *See infra* section I(c).

[12] NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[A][2].

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

Massachusetts Institute of Technology ("MIT").[14] From late 1993 to early 1994, he used MIT's equipment to operate Cynosure, a bulletin board system ("BBS") that allowed users to upload and download infringing software applications and videogames.[15] LaMacchia was not accused of uploading or downloading any infringing programs himself. However, prosecutors asserted that he maintained the BBS (including deleting files and transferring files between servers) and asked BBS users to upload specific software programs.[16] Judge Stearns described LaMacchia's behavior as, at best, "heedlessly irresponsible, and at worst as nihilistic, self-indulgent, and lacking in any fundamental sense of values."[17] Although the term was not widely used at the time, LaMacchia was an early warez trader.

Like a typical warez trader, LaMacchia operated the BBS for fun and without any commercial advantage or private financial gain. Therefore, prosecutors could not charge him with criminal copyright infringement. Instead, prosecutors charged him with one count of conspiracy to commit wire fraud.[18] Judge Stearns applied the U.S. Supreme Court case of *Dowling v. United States*, which had ruled that intangible intellectual property was not capable of being stolen, converted or taken by fraud.[19] That case, he concluded, "precludes LaMacchia's prosecution for criminal copyright infringement under the wire fraud statute,"[20] and he dismissed the indictment.

Despite the dismissal, Judge Stearns issued a challenge to Congress:

> Criminal as well as civil penalties should probably attach to willful, multiple infringements of copyrighted software even absent a commercial motive on the part of the infringer. One

[14] *Id.* at 536.

[15] *Id.* Prosecutors alleged that these websites operated "on an international scale" and caused losses of more than $1 million. *Id.* at 536-37. The loss estimates have been characterized as unsupported estimates. *See* Joseph F. Savage, Jr. & Kristina E. Barclay, *When the Heartland is "Outside the Heartland:" the New Guidelines for NET Act Sentencing*, 9 GEO. MASON L. REV. 373, 377 (2000).

[16] 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.

[17] *LaMacchia*, 871 F. Supp. at 545.

[18] *Id.* at 541-42. Wire fraud does not require the government to prove that the defendant sought to personally profit from the scheme.

[19] 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.

[20] *LaMacchia*, 871 F. Supp. at 545.

> can envision ways that the copyright law could be modified to permit such prosecution. But, it is the legislature, not the Court, which is to define a crime, and ordain its punishment.[21]

B. A Legislative Response to LaMacchia

Copyright owners seized upon Judge Stearns's challenge and lobbied Congress for just such a law. In August 1995, Sen. Leahy introduced the Criminal Copyright Improvement Act of 1995, which included provisions for punishing infringement without financial gain or commercial advantage.[22] Though that bill did not pass, a subsequent bill led to the NET Act, which was enacted in 1997.[23]

The Act effected six principal changes to criminal copyright law. First, the NET Act expanded the Copyright Act's definition of "financial gain" to include the receipt (or expectation of receipt) of anything of value, including other copyrighted works.[24] Second, in addition to willful infringement for commercial advantage or private financial gain, the Act criminalized the reproduction or distribution, in any 180 day period, of copyrighted works with a total retail value of more than $1,000.[25] Third, the Act said that evidence of reproducing and distributing copyrighted works does not, by itself, establish willfulness.[26] Fourth, the Act changed the punishments for criminal infringement. For infringements of more than $1,000, the punishment includes imprisonment of up to one year and a fine. For infringements of $2,500 or more, the punishment includes imprisonment of up to three years and a fine. For second or subsequent offenses involving commercial advantage or private financial gain, the punishment includes imprisonment of up to six years.[27] Fifth, the Act permits copyright infringement victims to submit victim impact

[21] *Id*. (quotation omitted).

[22] S.1122, 104th Cong. § 2(b) (1995), *available at* http://www.eff.org/Legislation/Bills_by_number/s1122_95.bill. *See generally* 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, 861-62 (1999), *available at* http://www.wulaw.wustl.edu/WULQ/77-3/773-835.pdf.

[23] 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. .

[24] *Id.* § 2(a).

[25] *Id.* § 2(b).

[26] *Id.*

[27] *Id.* § 2(d).

statements.[28] Finally, the Act instructed the United States Sentencing Commission (the "Sentencing Commission") to adjust the United States Sentencing Guidelines[29] (the "Sentencing Guidelines") for criminal copyright infringement to make the punishments sufficiently stringent to deter the crimes and to reflect the infringed items' retail value and quantity.[30]

C. *The Act's Goals*

Because the *LaMacchia* case directly instigated the Act,[31] the law is often characterized as being intended to close the *LaMacchia* loophole.[32] Indeed, the House Report said it desired to "reverse the practical consequences of" the *LaMacchia* case,[33] and several legislators reiterated this goal.[34] However, accepting these statements on their face still leaves open a central question: Exactly what aspects of *LaMacchia* did Congress intend to reverse?

Some legislators specifically targeted LaMacchia's warez trading, referencing targets such as "commercial scale" piracy[35] and self-aggrandizing infringers.[36]

[28] *Id.*

[29] U.S. SENTENCING GUIDELINES MANUAL § 3E1.1.1 (2002), *available at* http://www.ussc.gov/2002guid/2002guid.pdf.

[30] *Id.* § 2(g).

[31] *Hearings*, *supra* note 9 (statement of Rep. Coble) ("The NET Act constitutes a legislative response to the so-called *LaMacchia* case . . . .").

[32] NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[B][2].

[33] H.R. REP. NO. 105-339, at 3 (1997).

[34] *See* 143 CONG. REC. S12689, S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch); 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte).

[35] *See* 143 CONG. REC. S12689, S12689-90 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch) (saying the Act's purpose is to "prosecute commercial-scale pirates who do not have commercial advantage or private financial gain from their illegal activities" and "eliminate willful, commercial-scale pirating of copyrighted works"); 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl) (the targets are "willful, commercial-scale pirates"); 143 CONG. REC. S12689, S12690 (daily ed. Nov. 13, 1997) (statement of Sen. Leahy) (stating that the targets are individuals who "use computer networks for quick, inexpensive and mass distribution of pirated, infringing works"); *see also* Letter from Andrew Fois, Assistant Attorney General of the DOJ, to Sen. Orrin Hatch, Chair of the Senate Judiciary Committee (Nov. 7, 1997), *reprinted in* 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (stating that the Act will permit "the Department to prosecute *large-scale* illegal reproduction or distribution of copyrighted works where the infringers act without a discernable profit motive") (emphasis added).

[36] *See* 143 Cong. Rec. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl) (targeting software pirates who seek notoriety instead of money); 143 CONG.

LaMacchia's BBS primarily traded software (as opposed to other copyrighted works), and the legislative history also extensively discussed software piracy. As the House Report says, "copyright piracy flourishes in the software world" despite existing sanctions.[37] The report cited industry estimates that software counterfeiting and piracy cost copyright owners $11 billion in 1996,[38] resulting in "130,000 lost U.S. jobs, $5.6 billion in corresponding lost wages, $1 billion in lower tax revenue, and higher prices for honest purchasers of copyrighted software."[39] Individual legislators also expressed a desire to target software pirates[40] and to protect the software industry.[41]

Finally, even though the Act criminalizes infringements regardless of distribution media, several legislators specifically targeted Internet-based piracy.[42] Of course, the Act's title ("No

REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Cannon) (targeting "Robin Hood" types); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Frank) (the Act aims at "seriously maladjusted" individuals who infringe not for profit but to show their smarts and get attention).

[37] H.R. REP. NO. 105-339, at 4 (1997); *see also* Rep. Howard Coble, *The Spring 1998 Horace S. Manges Lecture—The 105th Congress: Recent Developments in Intellectual Property Law*, 22 COLUM.-VLA J.L. & ARTS. 269 (1998) (reprinting the House Report with some additional commentary by Rep. Coble).

[38] H.R. REP. NO. 105-339, at 4 (1997). The report paranethetically adds that "others believe the figure is closer to $20 billion." *Id.*; *see also infra* Section III(A) (further examining these numbers).

[39] H.R. REP. NO. 105-339, at 4 (1997). Some of these statistics were reiterated by individual legislators. *See*, *e.g.*, 143 CONG. REC. H9883, H9887 (daily ed. Nov. 4, 1997) (statement of Rep. Delahunt).

[40] *See* 143 CONG. REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Cannon) (stating that the Act enables the Justice Department to go after software pirates); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte) (stating that he expects the Act to deter potential software pirates).

[41] *See* 143 CONG. REC. S12689, S12691 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl) (saying that the Act will "help protect the interests of the entire software industry"); 143 CONG. REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Cannon) (saying that the Act will benefit the software industry); *cf.* 143 CONG. REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Rohrabacher) (discussing how software and entertainment media play important roles in managing the United States' balance of payments with other countries).

[42] *See* 143 CONG. REC. S12689, S12690 (daily ed. Nov. 13, 1997) (statement of Sen. Leahy) (stating that the Act encourages "the continued growth of the Internet"); 143 CONG. REC. H9883, H9887 (daily ed. Nov. 4, 1997) (statement of Rep. Berman) (the Act is "essential to the continuing growth of the Internet"); 143 CONG. REC. H9883, H9887 (daily ed. Nov. 4, 1997) (statement of Rep. Delahunt) ("I believe this measure will help preserve the creative incentive on which so much of our prosperity—and the future of the Internet itself—depend."); 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte) (stating that the Act "helps consumers realize the promise and potential of the Internet").

Electronic Theft," with the acronym "NET") reinforces that objective.

Therefore, the legislative history suggests Congress targeted LaMacchia's use of the Internet to distribute infringing software on a commercial scale but without a profit motive. In other words, Congress specifically targeted warez trading.

D. Enactment

For a law three years in the making and effecting a major change in criminal law, there was surprisingly little organized opposition.[43] For example, none of the witnesses testifying about the Act before the House Judiciary Committee's Subcommittee on Courts and Intellectual Property on September 11, 1997 (the "1997 Subcommittee Hearings") raised any serious objections to the Act's passage.[44] Two witnesses did express specific concerns that the then-current version of the Act swept too broadly,[45] but both ultimately supported Congressional action (or at least claimed to).[46] During the Act's floor debates, no legislator spoke in opposition or raised any serious concerns.[47] The Act passed both the House and Senate by voice vote.[48]

[43] The DMCA was being considered at the same time as the NET Act, and the attention given to the DMCA probably overshadowed the NET Act.

[44] *Cf.* 143 CONG. REC. H9883, H9885 (daily ed. Nov. 4, 1997) (statement of Rep. Frank) ("This is a bill which was noncontroversial in its purpose."). However, of the eight witnesses testifying at the Subcommittee hearing, two witnesses were government employees and the remaining six were industry lobbyists. *See Hearings*, *supra* note 9 (witness list), *available at* http://www.house.gov/judiciary/41101.htm. No law professors, lobbyists for the academic or scientific community, criminal defense counsel or consumer protection lobbyists testified at the hearing. Also, no organizations representing musicians, artists or authors were included either. Brian P. Heneghan, *The NET Act, Fair Use, and Willfulness—Is Congress Making a Scarecrow of the Law?*, 1 SUFFOLK J. HIGH. TECH. L. 27, 29 (2002), *available at* http://www.law.suffolk.edu/stuservices/jhtl/V1N1/BHENEGHANV1N1N.pdf.

[45] Kevin DiGregory raised concerns about the lack of a financial threshold for criminal infringement. *See Hearings*, *supra* note 9, at 45 (statement of Kevin DiGregory, Deputy Assistant Attorney General, Criminal Division of the DOJ). David Nimmer expressed concerns that the term "willfully" was not defined and thus could expose Internet service providers to criminal liability. *See id.* at 148-56 (statement of David Nimmer, attorney at Irell & Manella LLP, testifying on behalf of the United States Telephone Association).

[46] *See Hearing*, *supra* note 9, at 46 (statement of Kevin DiGregory) ("The Department is highly supportive of the goals of H.R. 2265"); *id.* at 149 (statement of David Nimmer) stating that his client "approves the spirit animating this legislative fix").

[47] Some legislators discussed their concerns about the Act's scope and definition of willfulness. *See infra* Section IV.

[48] *Fighting Internet Theft*, Cong. Q. Almanac 3-15 (1997).

While the Act was awaiting presidential signature, a group of scientists led by the Association of Computing Machinery ("ACM") asked President Clinton to veto the Act,[49] asserting that the Act would have "a negative impact on the rich scientific communications that have developed on the Internet."[50] This last-minute request failed, and President Clinton signed the Act on December 16, 1997.

II

DEVELOPMENTS AFTER THE ACT'S ENACTMENT

A. Congressional Oversight of Implementation and Use

No convictions under the Act were announced in the first eighteen months following the Act's passage. This perceived lack of action prompted Rep. Howard Coble, one of the Act's co-sponsors, to convene hearings of the House Judiciary Committee's Subcommittee on Courts and Intellectual Property in May 1999 (the "Oversight Hearings"). As Rep. Coble said at the hearings:

> Since the enactment of the NET Act in December 1997, there have been no prosecutions brought by the Department of Justice under the Act. This is very troubling because, according to U.S. intellectual property based industries, there is no shortage of potential prosecutions that could be pursued under the Act.[51]

Kevin DiGregory of the United States Department of Justice (the "DOJ") responded by enumerating several general challenges to prosecuting digital piracy,[52] including: (1) Internet pirates do not have sizable or easily-located manufacturing operations; (2) calculating damages and losses is difficult because it is hard to count the number of illegitimate copies made over the Internet; (3) no government agency has primary responsibility for enforcing Internet-based crimes, and prosecutions often cut across prosecutors' territories; and (4) Internet-savvy law en-

[49] Letter from Dr. Barbara Simons, Chair, U.S. Public Policy Committee, Association For Computing, to President William J. Clinton (Nov. 25, 1997), *available at* http://www.acm.org/usacm/copyright/usacm-hr2265-letter.html.

[50] *Id.*; *see infra* Section IID (addressing the ACM's specific arguments).

[51] *Implementation of the "Net" Act and Enforcement Against Internet Piracy: Oversight Hearing Before the Subcomm. on Courts and Intellectual Prop., House Comm. on the Judiciary*, 106th Cong. (1999) [hereinafter *Hearing*] (statement of Rep. Coble), available at http://www.house.gov/judiciary/cobl0512.htm.

[52] *Id.* (statement of Kevin DiGregory, Deputy Assistant Attorney General, Criminal Division of the DOJ), *available at* http://www.house.gov/judiciary/ digr0512.htm.

forcement officials are hard to retain and often asked to help with other computer crime enforcements.[53]

Mr. DiGregory also identified specific difficulties with enforcing the Act against pirate website operators:[54] (1) for-profit criminals are a higher priority;[55] (2) operators are often juveniles; (3) websites move overseas, complicating investigation and enforcement; (4) establishing an operator's identity can be challenging; (5) prosecutors cannot prove willfulness; (6) young not-for-profit operators are sympathetic defendants;[56] (7) the Sentencing Commission had not established the mandated changes to the Sentencing Guidelines; and (8) the Sentencing Guideline's computation of retail value leads to low penalties. He concluded that "although there are many websites on the Internet offering illegal software and other copyrighted materials, investigating and prosecuting the offenders is hardly shooting fish in a barrel."[57]

Despite the dozen challenges mentioned by Mr. DiGregory, the DOJ also quickly responded to the Oversight Hearings, delivering the first criminal conviction under the Act just three months later. Since then, the prosecution machine has ramped up significantly, and nearly eighty defendants have been convicted under the Act.[58]

B. Amendment of the Sentencing Guidelines

As mentioned earlier, the Act instructed the Sentencing Commission to amend the Sentencing Guidelines to toughen the ap-

[53] *Id.* In July 1999, the DOJ addressed some of these concerns through its Intellectual Property Rights Initiative, which increased the priority of intellectual property crime enforcement, provided more training to prosecutors, expedited referrals of matters, pursued equipment forfeiture and advocated changes to the Sentencing Guidelines. Press Release, U.S. Department of Justice and Department of Treasury, Justice Department, FBI and Customs Service to Combat Intellectual Property Crime (July 23, 1999), *available at* http://www.cybercrime.gov/ipinitia.htm.

[54] *Hearing*, *supra* note 51 (statement of Kevin DiGregory).

[55] Among other reasons, these individuals are higher priority because they tend to run larger operations, make less sympathetic defendants and have records that are more readily accessible as evidence. *Id.*

[56] *See* Computer Crime & Intellectual Property Section, U.S. Department of Justice, Prosecuting Intellectual Property Crimes Manual § III(E)(4) (2001) (advising prosecutors not to proceed with criminal infringement cases against sympathetic defendants unless the prosecutor can show egregious conduct), *available at* http://www.cybercrime.gov/ipmanual/03ipma.htm [hereinafter DOJ IP CRIMES MANUAL].

[57] *Hearing*, *supra* note 51 (statement of Kevin DiGregory).

[58] *See infra* Section II(c).

plicable penalties and better define the applicable retail value. Responding to this instruction, in January 1998 the Sentencing Commission published a proposal and requested comments.[59] A hearing was held in March 1998, which resulted in a revised proposal in April 1998 with a public comment period running through August 1998.[60]

Analyzing these comments and other sources, a Policy Development Team developed and released a report with recommended changes in February 1999 (the "Team Report").[61] At the Oversight Hearings, Rep. Coble criticized the Team Report as failing "to address the NET Act's explicit instructions to consider that deterrence be adequately addressed" in the Guidelines.[62] In any case, the Sentencing Commission did not act on the Team Report because it lacked voting commissioners.[63]

On December 9, 1999, Congress reiterated its instructions to the Sentencing Commission in the Digital Theft Deterrence and Copyright Damages Improvement Act:

> Within 120 days after the date of the enactment of this Act, or within 120 days after the first date on which there is a sufficient number of voting members of the Sentencing Commis sion to constitute a quorum, whichever is later, the Commission shall promulgate emergency guideline amend ments to implement section 2(g) of the No Electronic Theft (NET) Act (29 U.S.C. 994 note) in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987, as though the authority under that Act had not expired.[64]

New commissioners were confirmed on November 15, 1999, and the Sentencing Commission issued proposed emergency guidelines on December 23, 1999 that took effect temporarily on May 1, 2000 and became permanent on November 1, 2000.[65]

[59] Notice of Proposed Amendments to Sentencing Guidelines, Policy Statements and Commentary, 63 Fed. Reg. 602 (proposed Jan. 6, 1998).

[60] U.S. SENTENCING COMM'N, NO ELEC. THEFT ACT: POLICY DEV. TEAM REPORT 1 (1999), *available at* http://www.ussc.gov/agendas/02_99/NETBRF99.PDF [hereinafter Team Report].

[61] *Id.*

[62] *Hearing*, *supra* note 51 (statement of Rep. Coble).

[63] *Hearing*, *supra* note 51 (statement of Timothy McGrath, Interim Staff Director, U.S. Sentencing Commission), *available at* http://www.house.gov/judiciary/mcgr0512.htm.

[64] Digital Theft Deterrence and Copyright Damages Improvement Act of 1999, Pub. L. No. 106-160, 113 Stat. 1774.

[65] Notice of: (1) Promulgation of Temporary, Emergency Amendment to the Sentencing Guidelines for Copyright and Trademark Infringement, Effective May 1, 2000; (2) Submission to Congress of Amendments to the Sentencing Guidelines;

Section 2B5.3 of the Sentencing Guidelines, applicable to NET Act prosecutions, now specifies:

- there must be a Base Offense Level of eight;[66]
- infringements between $2,000 and $5,000 receive a one level increase and infringements over $5,000 receive an increase pursuant to a table;[67]
- offenses involving the "manufacture, importation, or uploading of infringing items" receive a two level increase (but an offense level of no less than twelve);[68]
- offenses "not committed for commercial advantage or pri vate financial gain" receive a two level deduction (but an offense level of no less than eight);[69]
- offenses involving "conscious or reckless risk of serious bodily injury" or involving a dangerous weapon receive a two level increase (but an offense level of no less than thirteen);[70]
- offenses where the defendant decrypted or circumvented technology to gain initial access to infringed items receive an adjustment in accordance with the provisions applicable to Section 3B1.3 of the Sentencing Guidelines;[71] and
- an upward adjustment may be appropriate when the Sentencing Guidelines understate the offense's seriousness, such as if the offense substantially harms the owner's reputation or the offense was part of an organized criminal enterprise.[72]

Retail value generally is computed using the *infringing* item's value,[73] but the *infringed* item's value is used when:

- the infringing item is "identical or substantially equivalent to the infringed item, or . . . is a digital or electronic reproduction";
- the infringing item's retail price is not less than seventy-five percent of the infringed item's retail price;
- the infringing item's retail value is difficult or impossible to calculate without unduly complicating or prolonging the proceedings;

and, (3) Request for Comment, 65 Fed. Reg. 26,880 (May 9, 2000), *available at* http://www.ussc.gov/FEDREG/FR2000.htm; *see also* U.S. SENTENCING COMM'N OFFICE OF EDUC. & SENTENCING PRACTICE, *2000 Amendments to the Federal Sentencing Guidelines*, at 1, *available at* http://www.ussc.gov/2000guid/2000amd high00.pdf.

[66] U.S. SENTENCING GUIDELINES MANUAL § 2B5.3(a) (2002), *available at* http://www.ussc.gov/2002guid/2002guid.pdf.

[67] *Id.* § 2B5.3(b)(1).

[68] *Id.* § 2B5.3(b)(2).

[69] *Id.* § 2B5.3(b)(3).

[70] *Id.* § 2B5.3(b)(4).

[71] *Id.* § 2B5.3, cmt. 4.

[72] *Id.* § 2B5.3, cmt. 5.

[73] *Id.* § 2B5.3, app. 1.

- satellite cable transmissions are illegally intercepted; or
- the infringed item's retail value more accurately assesses the pecuniary harm suffered by the owner.[74]

C. Prosecutions under the Act

As mentioned above, nearly eighty defendants have been convicted under the Act. This subsection discusses some of the publicized convictions.

1. Jeffrey Levy

In August 1999, Jeffrey Levy, a twenty-two-year old University of Oregon senior, became the first individual convicted under the Act. He operated a website that allowed third parties to download thousands of software and game programs, songs, and movies, at least some of which Levy uploaded himself.[75] After Levy was arrested and an information was filed against him, he was given a choice: he could remain in prison six months while the FBI analyzed his computers to determine the value of the infringing works, or he could plead guilty.[76] Levy chose the latter and pleaded guilty to distributing software with a retail value of at least $5,000 (although a "conservative[ ] estimate" of the actual retail value was $70,000).[77] He was sentenced to two years probation.[78]

2. Eric Thornton

Eric Thornton, a twenty-four-year old Navy avionics technician, operated a website called "No Patience" permitting users to download software such as Adobe Premiere and Adobe Illustrator.[79] In one specific instance, a third party downloaded twenty

---

[74] *Id.* § 2B5.3, app. 2.

[75] 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.

[76] Karen J. Bernstein, *Net Zero: The Evisceration of the Sentencing Guidelines Under the No Electronic Theft Act*, 27 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 57, 63 (2001) [hereinafter Bernstein, *Net Zero*].

[77] 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.

[78] *Id.*

[79] Bill Miller, *Giveaways Costly for Web Pirate*, WASH. POST, Dec. 23, 1999, at B1 [hereinafter Miller, *Giveaways*].

software programs with a retail value of $9,638.[80] Thornton used the third party software to attract traffic to his website.[81] However, when his Internet access provider noticed the traffic spike, his provider shut down the website and notified the FBI.[82]

In December 1999, Thornton pleaded guilty to a misdemeanor violation of the Act.[83] He received five years probation and had to pay restitution of $9,600.[84] In addition, for eighteen months Thornton's website described his arrest and conviction.[85]

3. *Brian Baltutat*

In October 2000, twenty-one-year-old Brian Baltutat pleaded guilty to violating the Act.[86] He operated a website called "Hacker Hurricane," visited by 65,000 people, that offered 142 software programs for downloading.[87] Baltutat received three years probation, 180 days home confinement (including a tether), restitution, and forty hours of community service.[88]

4. *Jason Spatafore*

In December 2000, Jason Spatafore, a twenty-five-year-old

[80] 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.

[81] Miller, *Giveaways*, *supra* note 79, at B1.

[82] *Id.*

[83] *Id.*

[84] *Internet Pirate to Pay Restitution*, WASH. POST, Mar. 4, 2000, at B2.

[85] Miller, *Giveaways*, *supra* note 79, at B1. Specifically, the site said:

> 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!

Bernstein, *Net Zero*, *supra* note 76, at 64 n.58.

[86] 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.

[87] *Id.*

[88] *Id.*

computer technician, pleaded guilty to a single violation of the Act.[89] He posted parts of *Star Wars Episode I: The Phantom Menace* on various websites for downloading and encouraged people to download the film.[90] He received two years probation and a $250 fine.[91]

5. *Fastlane*[92]

Fastlane was a major warez group. It had an organizational structure and held weekly meetings to discuss matters such as membership and sources of pirated software.[93] Fastlane's websites were not publicly accessible. The FBI infiltrated Fastlane by surreptitiously operating a computer site known as Super Dimensional Fortress Macros (SDFM), which members used to exchange copyrighted works such as Microsoft operating systems, application software from Adobe and Corel, and system utilities from Symantec and McAfee.[94] During SDFM's operation from January to September 2000, members uploaded over 697 gigabytes of software and downloaded 1.9 terabytes with a total retail value over $1 million.[95]

In February 2001, nine Fastlane members were charged with one count of conspiracy to commit copyright infringement, and eight of those defendants were charged with one count of com-

[89] 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.

[90] *Id*.

[91] Jason Spatafore, *DisMan's Online Journey*, *at* http://www.spatafore.net/disman/thephoenixmenace.shtml (last visited Nov. 16, 2003).

[92] The individual Fastlane defendants are: Ryan Breding, 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.

[93] *Id.*

[94] *Id.*

[95] *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.*

mitting copyright infringement.[96] Eight of the nine defendants pleaded guilty, while a jury found Tony Walker guilty.[97] Three defendants received jail sentences ranging from five to thirty months.[98] The other defendants received probation of three years.

6. *Pirates With Attitude*[99]

Pirates With Attitude (PWA) was another major warez group, characterized as "the 'oldest and most sophisticated' band of software pirates in Internet history."[100] PWA operated thirteen FTP servers for software uploading and downloading.[101] Its flagship site was Sentinel, located at the University of Sherbrooke in Quebec, which operated from late 1995 to January 2000.[102] Sentinel users obtained the right to download software by uploading pirated software or by performing other services to the group.[103] During Sentinel's operation, over 30,000 software programs (in-

[96] *Id.* Kevin Vaughan was not charged with committing copyright infringement. *Id.*

[97] *See* United States v. Deal, No. 00-CR-774 (N.D. Ill. filed Sept. 20, 2000).

[98] *See id.*

[99] The individual Pirates With Attitude defendants are:

> Convicted members of Pirates With Attitude: 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.
>
> Fugitive members of Pirates With Attitude: Kaj Bjorlin, aka "Darklord," Sweden; Mark Veerboken, aka "Shiffie," Belgium.
>
> 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.

Press Release, U.S. Department of Justice, Leader Of Software Piracy Sentenced To 18 Months In Prison (May 15, 2002), *available at* http://www.cyber crime.gov/rothbergSent_pirates.htm [hereinafter Rothberg Sentenced Press Release]. *See generally* United States v. Rothberg, No. 00-CR-85 (N.D. Ill. filed Feb. 3, 2000); Special November 1999 Grand Jury Indictment, United States v. Rothberg (N.D. Ill. 2002) (No. 00-CR-85).

[100] Darryl van Duch, *Eyes on 'Pirates' Trial in Chicago,* NAT'L L.J. (New York City), Mar. 26, 2001, at B1.

[101] Rothberg Sentenced Press Release, *supra* note 99.

[102] *Id.*

[103] *Id.*

cluding games, MP3 files, operating systems, utilities, and applications from vendors such as Microsoft, Adobe, Norton, Oracle, IBM, Lotus, and Novell, some of which were pre-release versions) were uploaded to Sentinel and downloaded by more than 100 individuals.[104] The FBI cracked the case when a confidential informant helped them gain access to Sentinel.[105] PWA members claimed their activities were "for fun and entertainment, not to try to make ourselves rich."[106]

Seventeen defendants were indicted in 2000.[107] Twelve defendants were PWA members, and five were Intel Corporation employees who provided computer hardware to PWA for access rights to the warez library.[108]

Following the indictments, many defendants negotiated plea agreements. After the plea agreements were entered into, the government contended that the infringements had a retail value over $10 million.[109] A group of defendants jointly moved to limit the retail value based on expectations defendants formed while negotiating their plea agreements. The judge denied the motion but permitted defendants to rescind their plea agreements (and thus withdraw their guilty pleas) if they wanted.[110] None chose to rescind.[111]

A group of defendants then petitioned the court for a lower retail value, and the court agreed, setting the retail value at $1,424,640.[112] With the retail value set, individual defendants were sentenced.

Robin Rothberg, the PWA leader, entered a blind guilty plea[113] but requested downward departure from the Sentencing Guidelines.[114] The court granted him some relief, and he was

[104] *Id.*

[105] *Id.*

[106] Pirates With Attitude Proudly Presents Xing Audio Catalyst 2.1 (August 10, 1999), *at* http://www.geocities.com/CapitolHill/7919/NFO/audio2_1.txt [hereinafter PWA Announcement].

[107] Rothberg Sentenced Press Release, *supra* note 99.

[108] *Id.*

[109] United States v. Rothberg, No. 00-CR-5, 2002 WL 171963, at *1 (N.D. Ill. Feb. 4, 2002).

[110] United States v. Rothberg, No. 00-CR-85, 2001 WL 1654758 (N.D. Ill. Dec. 20, 2001).

[111] *Rothberg*, 2002 WL 171963, at *2.

[112] *Id.* at *6.

[113] 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).

[114] *Id.* Rothberg received a two-level downward revision based on his absence of

sentenced to eighteen months in prison.[115]

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 received two years in prison.[116] Two other defendants, Jason Slater and Justin Robbins, received jail sentences of eight months and seven months, respectively.[117] Nine defendants received five years probation (and most of these defendants also received a $5,000 fine), and two defendants, Thomas Oliver and Steven Ahnen, each received three years probation.[118] Two defendants, Mark Veerboken and Kaj Bjorlin, are fugitives.[119] In November 2003, two defendants, Jason Slater and Christian Morley, appealed the case to the Seventh Circuit Court of Appeals.[120] The Seventh Circuit upheld the district court's refusal to instruct the jury on fair use[121] and its calculation of retail value.[122]

7. *Operations Buccaneer, Bandwidth, and Digital Piratez*[123]

Operations Buccaneer, Bandwidth, and Digital Piratez were major government operations targeting warez groups that, on December 11, 2001, led to the execution of approximately 100 search warrants both nationally and in Canada, the United Kingdom, Australia, Sweden, Norway, and Finland.[124] The raid had a

a profit motive, his extraordinary acceptance of responsibility, and his family circumstances. *Id.*

115 Rothberg Sentenced Press Release, *supra* note 99.

116 *Id.*

117 *See* United States v. Rothberg, No. 00-CR-85 (N.D. Ill. filed Feb. 3, 2000).

118 *See id.*

119 Rothberg Sentenced Press Release, *supra* note 99.

120 *See* U.S. v. Slater, 348 F.3d 666 (7th Cir. 2003).

121 *Id.* at 669.

122 *Id.* at 671.

123 Although these operations involved the warez community, in some cases the government's theory of prosecution did not directly specify that prosecutions were made under the Act. Some participants in the larger warez organizations sell warez for commercial gain, and distributed warez often find their way to commercial pirates who put the warez on CD-Roms or pay-for-access websites where users pay a monthly subscription fee or per-download fee. U.S. Department of Justice, Operation Buccaneer: Illegal "Warez" Organizations and Internet Piracy (July 19, 2002), *available at* http://www.cybercrime.gov/ob/OBorg&pr.htm [hereinafter DOJ Warez Organizations]. However, at least some defendants pleaded guilty to copyright infringement for financial gain based on having received other copyrighted works. *See* Keith J. Winstein, *Tresco Receives Three-Year Sentence*, The Tech (MIT), Aug. 26, 2002, *available at* http://www-tech.mit.edu/V122/N32/32tresco.32n.html.

124 Press Release, U.S. Department of Justice, Federal Law Enforcement Targets

major effect on the warez community globally.[125]

Operation Buccaneer[126] primarily targeted DrinkOrDie, one

International Internet Piracy Syndicates (Dec. 11, 2001), *available at* http://www.cybercrime.gov/warezoperations.htm.

[125] Robert Lemos, *FBI Raids Cripple Software Pirates*, CNET News.com, Dec. 18, 2001, *at* http://news.com.com/2100-1023-277226.html. *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").

[126] 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; Kent 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 "eriFlleH," 28, of Philadelphia, PA; Mark Shumaker, 21, of Orlando, FL; Kirk Patrick St. John, aka "the saint," 34, of Gilbert, AZ; 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; Press Release, U.S. Department of Justice, Online Music Piracy Leader Pleads Guilty (Aug. 21, 2003), *available at* http://www.cybercrime.gov/shumakerPlea.htm; Press Release, U.S. Department of Justice, Valley Man Indicted in International Software Piracy Scheme (Nov. 26, 2003), *available at* http://www.cybercrime.gov/stjohnIndict.htm.

In addition to the foregoing sources, specific sentences are described in United States v. Berry, No. 02-CR-246 (E.D. Va. filed Apr. 18, 2002); United States v. Buchanan, No. 02-CR-374 (E.D. Va. filed June 27, 2002); United States v. Clardy, No. 02-CR-10035 (C.D. Ill. filed Mar. 21, 2002); United States v. Cole, No. 02-CR-300 (E.D. Va. filed May 8, 2002); United States v. Eiser, No. 02-CR-284 (E.D. Va. filed May 2, 2002); United States v. Erickson, No. 02-CR-89 (E.D. Va. filed Mar. 5, 2002); United States v. Gross, No. 02-CR-299 (E.D. Va. filed May 8, 2002); United States v. Hunt, No. 02-CR-106 (E.D. Va. filed Mar. 14, 2002); United States v. Kelly, No. 02-CR-112 (E.D. Va. filed Mar. 14, 2002); United States v. Nawara, 02-CR-90

of the oldest and best-known warez groups.[127] Founded in Moscow in 1993, the group expanded worldwide in 1995.[128] Among other accomplishments, the group claimed to have released Microsoft Windows 95 two weeks prior to its commercial release.[129] The group was alleged to have two leaders, two or three council members, twelve to fifteen staff members, and approximately sixty-five general members.[130]

Other groups targeted by Operation Buccaneer included warez groups involved with creating warez, such as Razor1911, RiSCISO, MYTH, and POPZ, and distributing warez throughout the Internet, such as RequestToSend (RTS), WeLoveWarez (WLW), and RiSC.[131] The groups' archives contained, in some cases, two terabytes of pirated software, estimated to have a retail value of hundreds of millions of dollars.[132] However, as part of plea agreements, Operation Buccaneer defendants admitted that the retail value was between $2.5 million and $5 million.[133]

In conjunction with Operation Buccaneer, Mark Shumaker pleaded guilty to operating the Apocalypse Crew site, which contained pre-released digital music files solicited from DJs and reviewers.[134] Shumaker also admitted to uploading and

(E.D. Va. filed Mar. 5, 2003); United States v. Nguyen, No. 02-CR-63 (C.D. Cal. Filed Jan. 18, 2002); United States v. Pattanayek, 02-CR-118 (E.D. Va. filed Mar. 20, 2002); United States v. Riffe, No. 02-CR-156 (E.D. Va. filed Apr. 12, 2002); United States v. Tresco, No. 02-CR-132 (E.D. Va. filed Mar. 27, 2002).

[127] 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 [hereinafter Customs Fact Sheet].

[128] *Id.*

[129] *Id.*

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

[131] U.S. DEPARTMENT OF JUSTICE, OPERATION BUCCANEER: THE INVESTIGATION (July 19, 2002), *available at* http://www.cybercrime.gov/ob/OBinvest.htm.

[132] *Id.* A single file server operated by DrinkOrDie, "Fatal Error," allegedly had over 900 gigabytes and more than 15,000 titles of software. Criminal Information at 3, United States v. Tresco (E.D. Va. 2002) (No. 02-CR-132-A).

[133] *See, e.g.*, Plea Agreement at 2, United States v. Tresco (E.D. Va. 2002) (No. 02-CR-132-A); *Software Pirate Pleads Guilty*, GlobeandMail.com, Apr. 4, 2002, *at* http://www.globeandmail.com/servlet/RTGAMArticleHTMLTemplate?tf=RT/full-story_print.html&cf=RT/config-neutral&slug>copy&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.cyber-crime.gov/sankusPlea.htm.

[134] *See* Press Release, U.S. Department of Justice, Online Music Piracy Leader Pleads Guilty (Aug. 21, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/shumakerPlea.htm; *see also* Statement of Facts, United States v. Shumaker,

downloading infringing files from DrinkOrDie servers, and his total infringement was stipulated at $40,000-$70,000.[135]

Of the nineteen Operation Buccaneer defendants sentenced as of November, 2003, eleven received jail sentences ranging from eighteen to forty-six months (although at least ten of these defendants had their sentences reduced in exchange for government cooperation), three received five years probation, one received one year probation, and the other four received two years probation.[136]

Operation Bandwidth[137] primarily targeted Rogue Warriorz (RWZ), another major warez group. To make the bust, undercover FBI, EPA, and Defense Criminal Investigative Services agents infiltrated the group's "Shatnet" site.[138] From November 2000 to December 2001, Shatnet contained 8,434 infringing software programs, 356 infringing movies, and 432 infringing computer games with a retail value of approximately $7 million.[139] The group required membership applications and re-

Criminal No. 03-326-A (E.D. Va. 2003), *available at* http://www.usdoj.gov/ usao/vae/ ArchivePress/AugustPDFArchive/schumakersof082103.pdf.

[135] Statement of Facts, *Shumaker* (Criminal No. 03-326-A).

[136] U.S. DEPARTMENT OF JUSTICE, OPERATION BUCCANEER DEFENDANTS (Jan. 27, 2003), *available at* http://www.cybercrime.gov/ob/Dchart.htm.

[137] 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 Clappton, 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, Ruth Lawton; aka "Dragon", 41, of Akron, OH; Christopher Mastrangelo, aka "Floyd", 31, of Toms River, NJ; Brad McGourty; Michael Meacham, aka "Dvorak", 35, of Barberton, OH; Suzanne Peace, aka "Peaces", 37, of Lombard, IL; Lindle Romero, aka "Rahman", 37, of Houston, TX; Eric Rosenquist; Elisa Sarino, aka "Elisa", and "ElisaEGO", 27, of San Jose, CA; 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; Charles Yurek. *See* 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 [hereinafter DOJ Press Release]; Office of the Inspector Gen., Envtl. Prot. Agency, Semiannual Report to Congress (May 2003) [hereinafter OIG May 2003]; OFFICE OF THE INSPECTOR GEN., ENVTL. PROT. AGENCY, SEMIANNUAL REPORT TO CONGRESS (Nov. 2003).

[138] DOJ Press Release, *supra* note 137.

[139] *Id.*

corded statistics for group members who had maintained and moved the greatest number of files.[140] As of January 1, 2004, at least nineteen Operation Bandwidth defendants have pleaded guilty and at least five of those have been sentenced, all to probation.

As of January 1, 2004, Operation Digital Piratez has resulted in two publicized convictions. First, Christopher Motter was sentenced to two years in federal prison for his oversight of the warez server "Wonderland," which allegedly had over forty active users and over 5,000 warez with a retail value in excess of $500,000.[141] Second, Daniel McVay pleased guilty to operating a warez server known as "City Morgue," which contained 1,000 warez.[142] Five additional men have been indicted in connection with Operation Cyber Sweep (a larger government crackdown on Internet crime).[143]

8. William Fitzgerald

In February 2003, William Fitzgerald, a fifty-three-year-old computer technician for Arlington County, Virginia, pleaded guilty to one count of criminal copyright infringement.[144] He operated a website offering infringing business software from vendors such as Adobe, Autodesk, Macromedia, and Microsoft,[145] some of which he uploaded himself. Fitzgerald stipulated that

[140] Press Release, U.S. Department of Justice, Twelve "Operation Bandwidth" Software Pirates Enter into Group Guildty Plea (Dec. 18, 2003), *available at* http://www.cybercrime.gov/bandwidthPlea.htm.

[141] Press Release, U.S. Department of Justice, Iowa Man Receives Two-Year Prison Sentence in Internet Software Piracy Conspiracy (Sept. 30, 2003), *available at* http://www.cyberrime.gov/motterSent.htm.

[142] Press Release, U.S. Department of Justice, Massachusetts Man Pleads Guilty in New Hampshire Software Piracy Conspiracy (Dec. 19, 2003), *available at* http://www.cybercrime.gov/mcVayPlea.htm.

[143] Press Release, U.S. Department of Justice, Background on Operation Cyber Sweep—Examples of Prosecutions (Nov. 20, 2003), *available at* http://www.usdoj.gov:80/opa/pr/2003/November/03_crm_639.htm. The individual defendants are Jordan Zielin of New York, David Foresman of Lombard, Illinois, Kenneth Woods of Warrentown, Virginia, Daniel McVay of North Easton, Massachusetts, and John Neas of Holbrook, Massachusetts. Mark Hayward, *Five Digital Pirates Charged in Raid,* Union Leader (Manchester, N.H.), Nov. 21, 2003, at A20, *available at* http://www.msnbc.com/local/MUL/M340529.asp. Allegedly, Zielen, a Bank of America employee, set up a warez server on the Bank of America network, and Forseman operated a warez server at Verio's data center. *Id.*

[144] 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.

[145] *Id.*

the downloaded software was worth between $40,000 and $70,000.[146] He received four months in prison, four months of home confinement, and a $3,000 fine.[147]

9. Kerry Gonzalez

In June 2003, Kerry Gonzalez, 24, pleaded guilty to criminal copyright infringement. Gonzalez posted an unfinished "work print" copy of the movie *The Hulk* to a movie bootleg website two weeks prior to the movie's opening.[148] Gonzalez received the copy from a friend, who had in turn received the copy from an advertising agency employee.[149] A security tag in the movie, which Gonzalez unsuccessfully tried to remove, allowed the studio to trace the copy to the ad agency and ultimately to Gonzalez.[150]

10. Operation Safehaven

Operation Safehaven[151] was a fifteen month investigation into software privacy. In April 2003, government agents executed over twenty search warrants, leading to the seizure of thousands of CDs and DVDs and various warez servers, including the largest warez site seized in the U.S. to date.[152] Four defendants have pleaded guilty to conspiracy to commit copyright infringement and are awaiting sentencing.[153]

11. Operation Cybernet

Operation Cybernet targeted the individuals operating the

[146] *Id.*

[147] 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.

[148] Press Release, U.S. Department of Justice, N.J. Man Pleads Guilty in Federal Court to Stealing the Movie 'The Hulk' and Posting it on the Internet (June 25, 2003), *available at* http://www.cybercrime.gov/gonzalezPlea.htm.

[149] *Id.*

[150] P.J. Huffstutter, *How Hulk Crushed the Online Pirate*, L.A. Times, June 26, 2003, *available at* http://www.latimes.com/business/la-fi-hulk26jun26224419,1,1391001.story.

[151] Press Release, U.S. Department of Justice, Federal Investigation Leads to Prosecution of Internet Software Pirate (Oct. 2, 2003), *available at* http://www.cybercrime.gov/myersPlea.htm. The individual defendants are: Travis Myers, 29, of Yakima Wash., Terry Katz, 26, of Yorktown Heights, NY, Walter Kapechuk, 55, of Schenectady, NY, and Warren Willsey, 53, of East Berne, NY.

[152] *Id.*

[153] *Id.*

Usenet group alt.2600.warez and other FTP sites and IRC channels.[154] The operation produced its first conviction in December 2003 with the guilty plea of James Remy, a forty-year-old from Washington Township, N.J. who was employed at an East Brunswick graphic design and printing company.[155] Remy admitted to operating a warez server in his home that, from October 26, 2000 through July 24, 2001, was used to download files with a total retail value of $2,242,712.[156] The Department of Justice touted this as "the largest loss nationwide in a criminal copyright infringement case resulting from conviction of a warez site operator who is not part of an organized group. . . ."[157]

D. Commentary About the Prosecutions

As discussed in Section 1(C), the Act targeted individuals like LaMacchia; that is, individuals who used the Internet to distribute infringing software on a commercial scale but without a profit motive. Seven of the nine prosecutions match those objectives and therefore are directly consistent with the Act's intent. Spatafore and Gonzalez did not engage in commercial scale infringement, but their activities closely resemble that of warez traders, and thus they still fit comfortably within the Act's intended scope. Therefore, the prosecutions to date appear generally consistent with Congress' objectives for the Act.[158] Some of the Operation Bandwidth defendants have stipulated only to downloading a single copy of software.[159] While these prosecutions would be troubling in the abstract, in context it is likely that these stipulations were part of a plea bargain to avoid greater liability for RWZ's behavior.

This conclusion contrasts with the widespread predictions of problems that the Act would create. For example, some commentators expressed concern that aggressive prosecutors would

[154] *See* Press Release, U.S. Department of Justice, Man Admits to Distribution of Pirated Movies, Music, Computer Software and Games Worth Over $2.2 Million (Dec. 8, 2003), *available at* http://www.cybercrime.gov/remyPlea.htm.

[155] *See id.*

[156] *Id.*

[157] *Id.* (quoting Assistant U.S. Attorney Christopher J. Christie).

[158] *Cf.* 143 CONG. REC. S12689, S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch) (saying that "[i]f the practical effect of the bill turns out to be draconian, we may have to revisit the issue").

[159] Brad McGourty stipulated to downloading a copy of Microsoft Money, and Charles Yurek stipulated to downloading a copy of Windows XP. OIG May 2003, *supra* note 137, at 21-22.

abuse their discretion to win convictions.[160] One commentator predicted that prosecutors would bring weak felony cases to get quick misdemeanor plea bargains.[161] While prosecutors have been successful in getting defendants to plea bargain,[162] none of the cases appear particularly weak.

Commentators also worried that *de minimis* offenders would be prosecuted.[163] Indeed, Sen. Hatch specifically clarified that the Act should not reach *de minimis* infringements by educators who believe their actions constitute fair use[164] or individuals who merely execute software programs.[165] However, none of the cases are fairly characterized as *de minimis* (other than perhaps the Operation Bandwidth cases described above), and the DOJ is reluctant to pursue such cases, especially when defendants are sympathetic or act without profit motives.[166]

[160] Despite reservations about the Act's breadth, Sen. Hatch supported the Act because he was willing to rely on "the good sense of prosecutors and judges" to identify defendants consistent with the Act's purposes. *Id.*

[161] *See* Andrew Grosso, *The Promise and Problems of the No Electronic Theft Act*, Comm. of the ACM, Feb. 2000, at 23, 26, *available at* http://delivery.acm.org/10.1145/330000/328243/p23-grosso.pdf?key1=328243&key2=878343660-1&coll=GUIDE&dl=GUIDE&CFID=13119240&CFTOKEN=57162232. *Cf.* Henry M. Gladney, *Digital Intellectual Property: Controversial and International Aspects*, 24 COLUM.-VLA J.L. & ARTS 47, 65 (2000) (discussing how defending a felony prosecution under the Act is complex and tedious, thus inducing defendants to plea bargain).

Although not directly echoing this argument, the House Report evidences a desire to give prosecutors extra tools to negotiate plea agreements. *See* H.R. REP. NO. 106-339, at 8 (1997) (explaining that the financial thresholds were set low to allow the DOJ to extract plea bargains from felony defendants). *Cf.* DOJ IP CRIMES MANUAL, *supra* note 56, § III(A) ("Misdemeanor copyright infringement is another option for prosecutors. It can be a useful charge in cases where scale of the crime is difficult to prove with specificity . . . .").

[162] Only two defendants, Christian Morley of PWA and Tony Walker of Fastlane, have gone to trial.

[163] *See* H.R. Rep. No. 105-339, at 8 (1997) (saying that *de minimis* infringers should not be punished, giving the example of a teenager softlifting a software program for a younger sibling); 143 CONG. REC. S12689, S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch) (stating that earlier versions of the Act's "language was so broad that the net could be cast too widely . . . so that minor offenders . . . would be swept in"); Loren, *supra* note 22, at 870 (fearing that prosecutors would interpret the Act as a mandate to pursue small volume copiers).

[164] 143 CONG. REC. S12689, S12689 (daily ed. Nov. 13, 1997).

[165] *Id.* at S12690. Senator Hatch says that, "under a literal reading of the bill, the ordinary purchaser of computer software who loaded the software enough times in the 180-day period to reach the more-than-$1,000 threshold may be a criminal. This is, of course, not the intent of the bill." *Id.*

[166] *See* United States Consolidated Response to Defendants' Pre-Trial Motions, United States v. Rothberg, No. 00-CR-85, 2002 WL 171963, at *9 (N.D. Ill. Feb. 4, 2002) (noting that the government did not prosecute the hundreds of individuals

Similarly, the ACM believed the Act criminalized activities protected by fair use.[167] However, none of the defendants to date could legitimately claim fair use.[168] Furthermore, this concern may never have been legitimate at all.[169] Fair use remains a complete defense to criminal copyright infringement,[170] and some have suggested that any infringement made without commercial advantage or private financial gain is presumptively fair use.[171] Even without that presumption, a good faith but incorrect belief that a use was fair may negate willfulness.[172]

Some commentators expressed concern that the Act would detrimentally affect special communities, specifically universities and juveniles. Regarding universities, the ACM predicted that universities would remove copyrighted works from the Internet to avoid prosecution.[173] In practice, while universities are constantly evaluating ways to minimize their liability for content posted by students and faculty members, the Act does not appear

who only downloaded warez distributed by PWA); *Hearings*, *supra* note 9, at 49 (statement of Kevin DiGregory) ("I am not sure that we—that we want to be in a position to Federally prosecute that particular individual who decides to take that one piece of copyrighted material and send it to a friend or a relative."); *Hearings*, *supra* note 1 (statement of Kevin DiGregory); DOJ IP Crimes Manual, *supra* note 56, § III(E)(4) (advising prosecutors not to pursue technical violations of the Act if the defendant is sympathetic).

[167] *See* Simons, *supra* note 49.

[168] *Cf.* United States v. Slater, 348 F.3d 666, 669 (7th Cir. 2003) (calling a claim that warez trading is fair use "preposterous").

[169] *See* Dan Goodin, *Scientists Want Net Law Veto*, CNET news.com, Nov. 25, 1997, *at* http://news.com.com/2100-1023-205787.html (quoting Professor Pam Samuelson as saying that the assertion about fair use "may be a slight overstatement" and attorney Jonathan Band as saying "[i]f there was fair use before [the Act], there will be after").

[170] NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[A][2]; A. HUGH SCOTT, COMPUTER AND INTELLECTUAL PROPERTY CRIME: FEDERAL AND STATE LAW 271-72 (2001); Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 254 (1999).

[171] *See* DOJ IP Crimes Manual, *supra* note 56, § III(C)(3); Loren, *supra* note 22, at 887; James E. Neuman, *Copyright Violations Face Criminal Exposure*, N.Y.L.J., Oct. 13, 2001, at S3. 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, *see* 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.

[172] *See infra* Section IV(A).

[173] Simons, *supra* note 49; *see also* Goodin, *supra* note 169 (quoting Professor Pam Samuelson as saying, "If there is any question of copyright infringement, institutions will be inclined to avoid the whole problem and take things down, even when years of litigation would have found the use fair.").

to have led to significant efforts by universities to remove content from the Internet.[174] Instead, universities curtailing infringing online activities are more concerned about bandwidth usage[175] or civil liability[176] than criminal liability. Meanwhile, prosecutors have not shown any interest in prosecuting universities, even when NET Act defendants used school computer networks.

Some commentators also believed that the Act would disproportionately impact juveniles based on an assumption that many warez traders were minors.[177] While NET Act defendants have been as young as nineteen, no minors have been prosecuted. In fact, the DOJ will suspend prosecutions when a potential defendant is a juvenile,[178] which may explain the lack of prosecutions. Further, the stereotype that warez traders are primarily juveniles may be a fallacy.[179]

[174] *See* University of Wisconsin-Milwaukee, *New Internet Copyright Legislation Signed*, Fac./Staff Newsl. (Univ. of Wis.-Milwaukee), Jan. 23, 1998, *at* http://www.uwm.edu/News/report/old/jan98/Legal_Affairs.html (stating that the NET Act "does not impact existing UWM policy"). *Cf.* Georgia Harper, Liability for the Wrongful Acts of Publishers (Aug. 31, 2001), *available at* http://www.utsystem.edu/ogc/intellectualproperty/publia.htm (discussing how the University of Texas may be liable for publishing tortious content, but not advising its constituents to stop publishing).

[175] John Faust, Note, *Digital Music: Educational Issues*, 2001 BYU Educ. & L.J. 367, 387 (citing Georgia Harper, *University Liability for Student Infringements* (last updated Sept. 6, 2001), *at* http://www.utsystem.edu/ogc/intelectualproperty/napster.htm) ("Some [universities] have already blocked access for reasons unassociated with legal liability, most notably, because of the bandwidth use associated with searching for and transferring large files.").

[176] *See* Katie Dean, *School Blocks Out File-Trading*, WIRED NEWS, May 2, 2003, *at* http://www.wired.com/news/print/0,1294,58698,00.html (explaining that the New Jersey Institute of Technology blocked all Internet file-sharing to eliminate the risk of being sued by the recording industry and to avoid the hassle of complying with the high volume of legal demand letters); *see also* Scott Carlson, *New Jersey Institute of Technology Prohibits File Sharing on its Campus*, CHRON. HIGHER EDUC., May 1, 2003, *available at* http://chronicle.com/cgi2-bin/printable.cgi?article=http://chronicle.com/free/2003/05/2003050101t.htm. .

[177] *See* Stephanie Brown, *The No Electronic Theft Act: Stop Internet Piracy!*, 9 DEPAUL-LCA J. ART & ENT. LAW & POL'Y 147, 162-63 (1998) (citing Wendy Leibowitz, *Kid Stuff: Judges Having Hard Time with Computer Crime, Sentencing Standards Aren't Clear-Cut*, NAT'L L. J., July 6, 1998, at A1); *see also* Tetzlaff, *supra* note 10, at 107 (saying teenage boys are "archetypal" warez traders).

[178] *See Hearings*, *supra* note 51 (statement of Kevin DiGregory). *See generally* DOJ IP Crimes Manual, *supra* note 56, § III(E)(4) (describing a prosecutor's limited choices when prosecuting juveniles).

[179] *See* McCandless, *Warez Wars*, *supra* note 10 ("These are not pimply teenagers . . . not one member is younger than 20; Clickety-Clack is the youngest at 23. Most are 30-plus. Champion uploader Digital has been happily married for 22 of his

Finally, some commentators have predicted that copyright owners would take advantage of the longer criminal statute of limitations (five years instead of three) to obtain remedies after the civil statute of limitations expired.[180] So far the prosecutions to date do not evidence such an effort, as most cases appear to have been brought—and often resolved—within a matter of months. Further, with the evidentiary challenges of prosecuting cases involving Internet-based infringement, prosecutors probably will not pursue stale cases.

III

CONSEQUENCES OF THE ACT

Based on the previous section's analysis of the prosecutions to date, one might infer that the Act has been a success. However, the Act has not conformed the behavior of warez traders or had any real effect on piracy generally. Therefore, its relative lack of positive benefit prompts the question as to whether the Act's benefits outweigh its costs.

A. The Act's Effect on Piracy

Piracy rates cannot realistically be measured accurately. For example, to measure the Act's effect on piracy, the proper analysis would compare current piracy rates against what the rate would be without the Act, an obviously impossible inquiry.

Nevertheless, Congress relied on piracy statistics in its deliberations, so it is appropriate to start an efficacy analysis there. Specifically, the House Report cited a statistic that worldwide revenue losses to software piracy were $11 billion in 1996,[181] a statistic repeated by several legislators during the floor debates.[182] This number came from a study conducted by the International Planning and Research Corporation (the "IPRC

46 years . . . . Founding member Abraxas has three kids, one over 18."). The average PWA defendant was thirty-five years old, and the average age of Operation Bandwidth defendants was around thirty-two years old.

[180] *See* Heneghan, *supra* note 44, at 31 n.54; Loren, *supra* note 22, at 848; Neuman, *supra* note 171, at S3.

[181] H.R. REP. NO. 105-339, at 4 (1997).

[182] 143 CONG. REC. S12689, S12692 (daily ed. Nov. 13, 1997) (statement of Sen. Kyl); 143 CONG. REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Cannon); 143 CONG. REC. H9883, H9884 (daily ed. Nov. 4, 1997) (statement of Rep. Coble); 143 CONG. REC. H9883, H9887 (daily ed. Nov. 4, 1997) (statement of Rep. Delahunt).

Study") and commissioned by the Business Software Alliance ("BSA") and the Software and Information Industry Association.[183]

Unfortunately, Congress's reliance on this statistic is indefensible. First, the $11 billion statistic measured worldwide losses, which was irrelevant to assessing a law applying to activity in the United States. The U.S. piracy statistic in the IPRC Study was $2.4 billion,[184] still a large number but eighty percent less than the cited statistic.

Second, the IPRC Study's methodology[185] feigns credibility through complexity that obscures guesswork, subjective judgments, and unreliable data inputs. The IPRC Study computes lost revenues by considering the number of computers shipped into a country, guessing why those computers were purchased, and then guessing the number of business software programs that should have been licensed based on the country's technological maturity and the amount of software licensed in the United States at that stage of maturity. The amount of actual legitimate sales is then estimated using confidential data self-reported by BSA member companies, grossed up to reflect those member companies' percent of the U.S. market and then grossed up again to reflect the U.S. market's percent of the worldwide market.

This methodology is not credible because it uses multiple layers of estimates and uses unreliable data self-reported by member companies. Also, the IPRC Study ignores country-by-country differences in price elasticity for software.[186] Further, the IPRC Study modeled U.S. piracy using U.S. historical numbers as the baseline, creating an inherent circularity in the computation of piracy in the United States.[187]

Third, the IPRC Study reported *business* software losses, and

[183] INT'L PLANNING & RESEARCH CORP., SEVENTH ANNUAL BSA GLOBAL SOFTWARE PIRACY STUDY 6 (2002), *available at* http://www.bsa.org/usa/policyres/admin/2002-06-10.130.pdf [hereinafter IPRC Study]. The Software Publishers Association, which co-sponsored the 1996 IPRC Study, subsequently became the Software and Information Industry Association.

[184] *Id.*

[185] *See id.* at 8-9.

[186] *See id.*

[187] Starting in 2001, the IPRC prepared a state-by-state analysis of piracy which avoids this circularity but raises many of the same methodological questions. *See* Int'l Planning & Research Corp., U.S. Software State Piracy Study (2003).

softlifting was the biggest cause of this.[188] Softlifting means "purchasing a license for software and loading it onto additional computers, thus exceeding the license."[189] Commercial softlifting was already criminalized prior to the Act,[190] so the Act did not really implicate this activity. If Congress thought warez trading was the key problem, Congress should have considered how much revenue was lost to warez trading, but it did not.

Not surprisingly, subsequent versions of the IPRC Study reveal that piracy did not decrease from 1997 (the Act's passage) through 1999 (after the Act had been on the books for a full year). Worldwide revenue losses to software piracy increased from $11.3 billion in 1997 to $12.2 billion in 1999,[191] and software piracy in the United States increased from $2.4 billion in 1997 to $3.2 billion in 1999.[192]

Further, other empirical evidence suggests that piracy covered by the Act has gone up since its passage. A BSA study showed that warez trading sites increased from 100,000 in 1997 to 900,000 in 1999.[193] Another BSA survey from May 2002 showed that more than eighty percent of all Internet users who have downloaded commerical software have downloaded software

188 *See Hearings*, *supra* note 9, at 77 (statement of Greg Wrenn, Senior Corporate Counsel, Adobe Systems, Inc.).

189 *Hearings*, *supra* note 9, at 97 (statement of Sandra A. Sellers).

190 *See* DOJ IP Crimes Manual, *supra* note 56, § III(B)(5) (stating that "reproduction of unauthorized copies of a work for use within a single company is clearly an infringement for financial gain and commercial advantage . . . the purpose of the infringement is to save money by not purchasing additional authorized copies or licenses; the savings constitutes a financial gain for the infringer.").

191 IPRC Study, *supra* note 183, at 7. Note that piracy decreased in the IPRC Study from 1999 to 2001. The IPRC Study cites six factors contributing to a long-term worldwide decrease in software piracy: (1) software companies provide legitimate copies into developing markets faster, (2) software companies provide more user support internationally, (3) software prices have gone down, (4) industry groups have led education and civil enforcement efforts, (5) legitimate licensing practices increasingly support business credibility, and (6) there are more criminalization and government efforts to protect software. *Id.* at 2-3. Also, the IPRC model is very dependent on the number of computer units sold. If the units sold decreased, as often occurs in economic downturns, could that have contributed to the piracy decrease as much or more than any of the cited factors?

192 *Id.* at 6.

193 Stanley A. Miller II, *Software Piracy: When Using a Mouse Makes You Smell Like a Rat*, Milwaukee J. Sentinel, May 30, 2000, at 1M [hereinafter Miller, *Rat*]. BSA's website now claims that there are an estimated two million warez pages. *See* BUS. SOFTWARE ALLIANCE, COPYRIGHT POLICY INITIATIVES TO PROTECT CREATIVE WORKS, *at* http://www.bsa.org/usa/policy/copyright/creative-works.phtml (last visited Nov. 17, 2003).

without paying for it, and twenty-five percent of users who download software *never* pay for it.[194] And assuming peer-to-peer (P2P) file-sharing violates the Act, piracy has taken off since the Act's passage; an estimated fifty-seven million Americans use P2P file-sharing services[195] and forty-two percent of those individuals have burned a music CD rather than purchase it.[196]

While this evidence alone does not prove the Act's lack of efficacy, empirical evidence does not indicate that the Act has curbed infringements. Because multiple factors or considerations can influence piracy rates, there are a variety of hypotheses about why the Act may not effectively curtail copyright infringement.

1. Inadequate Enforcement and Penalties

Some have argued that the DOJ has not adequately enforced the Act,[197] the implicit concern prompting Rep. Coble to hold the Oversight Hearings. However, Rep. Coble should not have been surprised. The House Report indicates that the Congressional Budget Office expected that the Act "would enable DOJ to prosecute *several* additional copyright infringement cases each year."[198] While no prosecutions had been brought prior to the Oversight Hearings, the prosecutions brought since then meet or exceed this projection.

However, enforcement remains unpredictable, so infringers

[194] IPSOS PUBLIC AFFAIRS, QUANTIFYING ONLINE DOWNLOADING OF UNLICENSED SOFTWARE (2002), *at* http://www.bsa.org/usa/policyres/admin/2002-05-29.118.pps [hereinafter Ipsos Survey].

[195] *See* Jon Healey, *Labels May Face Risk in Piracy Suits*, L.A. Times, June 27, 2003, at 3(1) (observing that an estimated four million people are using KaZaA at any one time, collectively making 800 million files available).

[196] Press Release, Ipsos-Reid, File-Sharing and CD Burning Remain Steady in 2002: IPSOS (Feb. 20, 2003), *available at* http://www.ipsos-reid.com/media/dsp_displaypr.prnt.cfm?ID to view=1743.

[197] *See* Kevin M. Kelly, Comment, *The MP3 Challenge: Has Congress Effectively Shielded the Music Recording Industry from Internet Copyright Piracy?*, 18 Temp. Envtl. L. & Tech. J. 163, 189 (2000) ("The lack of prosecutions under the NET Act destroys the deterrent effect of the statute. The Department of Justice must actively seek individuals involved in Internet copyright piracy and prosecute those individuals in a high profile atmosphere. Only then will a true deterrent be created."); *see also* Rep. Howard Coble, *How Should the Government Protect Copyrights in Light of Technology?*, ROLL CALL, Mar. 27, 2000, at 14 ("A criminal statute that is not used by prosecutors and does not carry a credible threat of imprisonment is unlikely to be much of a deterrent, and the experience with the NET Act to date demonstrates the truth of this statement.").

[198] H.R. REP. NO. 105-339, at 6 (1997) (emphasis added).

may not have a meaningful fear of being prosecuted.[199] And some hypothesize that the Act does not sufficiently deter offenders because it lacks adequate penalties, either because the Sentencing Guidelines are too lax[200] or too complicated and unpredictable.[201]

2. *Ignorance of the Act*

The DOJ predicted that a few well-publicized prosecutions would have a strong deterrent effect.[202] But despite the publicity given to those prosecutions, the Act may not be well known.[203] Even warez traders, who generally know that their activities are illegal,[204] may not understand the legal consequences of their actions.[205]

[199] *See* Team Report, *supra* note 60, at 12 ("While the NET Act focuses only on the [swiftness of punishment], discussions with industry representatives made clear that the uncertainty of any punishment also plays a significant role in the widespread failure of deterrence."); *see also* Jim Wagner, *The Hunt for Warez*, Internetnews.com, Apr. 19, 2002, at 1, *at* http://www.internetnews.com/dev-news/article.php/10 1012961 (quoting Bob Kruger, BSA's Vice President of Enforcement, as saying, "Why do people continue to break the law? . . . For one, they don't think they'll get caught. . . ."). *But see* Tom R. Tyler, *Compliance with Intellectual Property Laws: A Psychological Perspective*, 29 N.Y.U. J. INT'L L. & POL. 219, 220-22 (Fall 1996-Winter 1997) (arguing that criminal deterrence only works when the probability of getting caught and punished clears a minimum threshold which criminal laws rarely reach; but even then, certainty of punishment plays only a small role in legal compliance).

[200] *See* Bernstein, *Net Zero*, *supra* note 76.

[201] *See* Neuman, *supra* note 171, at S3 ("The sentencing process [is] fraught with unpredictability and complexity.").

[202] *See Hearing*, *supra* note 51 (statement of Kevin DiGregory).

[203] *See* Gladney, *supra* note 161, at 64-66. Gladney cites a non-scientific survey he conducted showing widespread ignorance of the law. *Id.* at 63 n.65.

[204] *See* Statement of Facts, United States v. Pattanayek at 2 (E.D. Va. 2002) (No. 02-118-A) ("Defendant knew that his participation in [DrinkOrDie] and RTS was illegal, and he was aware of past federal prosecutions against similar groups."); Tetzlaff, *supra* note 10, at 115 (quoting a warez trader as saying, "We KNOW what we are doing is wrong"); Granade, *Warez*, *supra* note 8 (quoting an abandonware webmaster as saying, "I knew it was illegal."); Marc Saltzman, *Flashbacks for Free: the Skinny on Abandonware*, Gamespot.com, *at* http://gamespot.com/gamespot/ features/pc/abandonware/index.html (last visited Nov. 17, 2003).

[205] *See generally* Shahram A. Shayesteh, *High-Speed Chase on the Information Superhighway: The Evolution of Criminal Liability for Internet Piracy*, 33 Loy. L.A. L. Rev. 183, 217-18 (1999) (discussing warez traders' misunderstandings about the efficacy of disclaimers and fair use).

As a typical example of warez traders' bravado and naiveté, consider the boast of NXSonic, a warez site operator, who says that warez site operators have "talked with lawyers and know the boundaries" and therefore have concluded no criminal liability attaches so long as "sites do not have actual software on the sites." Wagner, *supra* note 199, at 2. However, the DOJ claims that merely linking to infringing

3. Socialization

As individuals become increasingly required to make copies to function in our society, they become socialized to ignore copyright law.[206] This socialization becomes reinforced with low incidents of enforcement,[207] the quasi-anonymity inherent in being one of millions of people committing infringement every day,[208] and the perceived inequity between high software prices and low manufacturing and distribution costs.[209] Thus, piracy may in-

software can be criminal. *See* DOJ IP CRIMES MANUAL, *supra* note 56, § III(E)(5) (discussing the theories under which linking can be prosecuted); *accord* David Goldstone and Michael O'Leary, *Novel Criminal Copyright Infringement Issues Related to the Internet*, U.S. ATTORNEYS' BULL., May 2001, at 33, 38, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usab4903.pdf.

[206] *See* Tyler, *supra* note 199, at 224 ("[t]he predominant strategy is to create a legal entitlement and then seek to enforce that entitlement with a threat. The result is widespread noncompliance with the law."); Wagner, *supra* note 199, at 1 (citing Bob Kruger, BSA's Vice President of Enforcement, as saying that people continue to break the law because "they think it's no big deal"). *See generally* Eric Schlchter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet*, 12 BERKELEY TECH. L.J. 15, 34-38 (1997) (discussing how users become socialized to accept copyright infringement), *available at* http://www.law.berkeley.edu/journals/btlj/articles/vol12/Schlachter/html/reader.html.

[207] *See Hearing*, *supra* note 51, at 7 (statement of Batur Oktay, Corporate Counsel, Adobe Systems, Inc.) ("Left unprosecuted, these types of websites—which are brazen about their own illegality—send the message that Internet pirates can operate with impunity, that there is no effective enforcement, that intellectual property protection on the Internet is unavailable."), *available at* http://www.house.gov/judiciary/okta0512.htm; Heneghan, *supra* note 44, at 45 (stating that "the practice of targeting a few visible scapegoats only serves to diminish people's respect for the law"); Jason Hoppin, *The Crackdown on IP Crime*, THE RECORDER, Dec. 3, 2001 (quoting a criminal defense attorney as saying that selective enforcement of criminal copyright cases breed contempt for the law), *available at* http://www.law. com/regionals/ca/stories/edt1203a.shtml.

[208] *See* Tyler, *supra* note 199, at 223 ("Little actual risk accrues to people who free ride on the efforts of others by copying articles, CDs or tapes. Hence, the structural opportunities for free riding are high in this area, making effective deterrence difficult."); Jefferson Graham, *Students Put Their Own Spin on Downloading Music*, USA Today, Apr. 10, 2003, *available at* http://www.usatoday.com/tech/ news/techpolicy/2003-04-10-music-share_x.htm (quoting a file-sharing student as saying that he still downloads music, despite publicized lawsuits against other students, because "[t]he record labels will never be able to stop downloading. It's too widespread."); Stephen Granade, *Beelzebub Interview*, BRASSLANTERN.COM, *at* http://brasslantern.org/community/interviews/beelzebub.html (last visited Nov. 18, 2003) (quoting a warez trader as saying that "[t]here's no way that the BSA et al could hope to prosecute every single individual who has ever downloaded a piece of illegal software from the internet. It clearly would not be economically viable . . . .") [hereinafter Granade, *Beelzebub*].

[209] *See* IPSOS Survey, *supra* note 194 (stating that eighty percent of Internet users feel that "it makes no sense for software companies to charge consumers . . . hundreds of dollars per user license for programs that cost them only a few pennies

crease because users become accustomed to routinely committing infringement and feel moral ambiguity about the justness of copyright law.

4. Imprecise Targeting

A final hypothesis is that the Act does not accomplish its goals because its provisions are not precise enough to change the behavior of the targeted infringer groups. To better analyze how the Act affects potential infringers, it is helpful to categorize infringers into different subgroups, as explored in the next section.

B. Classes of Pirates

During the 1997 Subcommittee Hearings, representatives of the Software Publishers Association and BSA discussed several types of software piracy: softlifting, counterfeiting, unauthorized loading of software onto hard drives by computer manufacturers and dealers, unauthorized software renting, and hacking/warez trading.[210] It remains unclear why so much hearing time was spent on these various types of infringers,[211] when all but the hacking/warez trading type were criminalized prior to the Act.

Even the hearing's brief discussion about hacking/warez trading was filled with imprecision. For example, the Software Publishers Association representative defined this group as a "type of pirate, the consummate 'hacker' or 'warez' aficionado."[212] Her reference actually covers three heterogeneous groups, each of whom warrant more discussion:

to reproduce"). Although this sentiment is felt strongest towards the software industry, many consumers have similarly strong feelings that the recording industry is morally unjust. *See* Amy Harmon, *Recording Industry Goes After Students Over Music Sharing*, N.Y. Times, Apr. 23, 2003, at A1 (discussing student hostility towards the music industry), *available at* http://query.nytimes.com/gst/abstract.html?res=F1081EFD355E0C708EDDAD0894DB404482.

[210] *Hearings*, *supra* note 9, at 97 (statement of Sandra A. Sellers). *See generally* Business Software Alliance, Types of Piracy, *at* http://www.bsa.org/ usa/antipiracy/Types-of-Piracy.cfm (last visited Nov. 18, 2003). While this list describes only software infringement, other infringer subgroups include fans/enthusiasts (i.e., an individual who builds a fan website), archivists/historians, critics, and P2P file-sharers who download MP3 files for personal enjoyment.

[211] For example, the Software Publishers Association's representative focused her presentation at the 1997 Subcommittee Hearing on softlifting by United States government agencies. *Hearings*, *supra* note 9, at 87-91 (statement of Sandra Sellers). Even the legislators were confused by the seeming irrelevance of this digression. *See id.* (statement of Rep. Cannon) (confirming with Ms. Sellers that the Act did not address her government softlifting concerns).

[212] *Hearings*, *supra* note 9, at 99 (statement of Sandra A. Sellers).

Commercial Pirates. Commercial pirates infringe copyrighted works for profit.[213] This subgroup includes counterfeiters, manufacturers and dealers who load unauthorized software onto hard drives, and software renters. Because by definition they commit commercial infringement, their behavior was criminalized prior to the Act.[214]

Crackers. Intrusive crackers obtain unauthorized access to private Internet spaces, such as private areas to download copyrighted material.[215] The Act does not specifically address this group, although intrusive cracking is covered by other criminal laws, such as the Computer Fraud and Abuse Act,[216] the Electronic Communications Privacy Act,[217] and numerous state antitrespass or computer crimes laws.[218]

Circumvention crackers defeat mechanisms installed by copyright owners to limit copying or use of the copyrighted work.[219] As discussed below, circumvention cracking is an integral part of the warez community, but neither the Act nor the 1997 Subcommittee Hearings addressed it. Congress subsequently criminalized circumvention cracking in the DMCA.[220]

Warez Traders. As mentioned previously, warez traders are enthusiasts who trade or distribute warez as an avocation. But even this description lumps together several subgroups:

- Warez distributors are organized groups that prepare and distribute warez for non-commercial reasons. To handle a high volume and rapid turnaround times, group members often

213 *See* David M. Hornik, *Combating Software Piracy: The Softlifting Problem*, 7 HARV. J.L. & TECH. 377, 378 (1994).

214 *See* 17 U.S.C. § 506(a)(1) (2000).

215 *Crack*, Webopedia.com (last visited Nov. 18, 2003), *at* http://www.webopedia.com/term/c/crack.html.

216 18 U.S.C. § 1030 (2000), *available at* http://www4.law.cornell.edu/uscode/ 18/1030.html.

217 18 U.S.C. § 2701 (2000), *available at* http://www4.law.cornell.edu/uscode/ 18/2701.html.

218 *See, e.g.*, 3 Ian C. Ballon, E-COMMERCE AND INTERNET LAW § 51.09 (2001).

219 *See* Omar J. Pahati, *Digital Pirates and the "Warez" Wars*, AlterNet.org, Jan. 24, 2002, *at* http://www.alternet.org/story.html?StoryID=12283 ("[G]angs, usually made up of software developers and technologists, work to reverse the protections built into software products, enabling others to distribute the products free of charge. Make no mistake—these gangs are not your rogue technophiles from the MS-DOS days, but a large, highly organized movement interested in 'cracking' every piece of software that sees the light of day.").

220 17 U.S.C. § 1201 (2000), *available at* http://www4.law.cornell.edu/uscode/ 17/1201.html.

specialize in a particular skill.[221] First, a supplier (often a software vendor insider) delivers a new software program to a "drop site," a computer where other group members can access it. Second, a group member "cracks" the software by removing or circumventing any copyright protection mechanisms. Third, other group members test the cracked software to make sure it still works and then "pack" the software by dividing it into easy-to-distribute packets. Finally, the cracked software is delivered to another drop site, from which members disseminate it throughout the Internet. Warez prepared by these distribution groups often contain an information file (".nfo file") which, among other things, describes which group claims credit for the distribution.[222]

- Warez collectors are individuals who collect warez. They want to build the biggest or most impressive collection of warez,[223] and they display their collections as a way to win peer approval.
- Warez downloaders are individuals who download warez for some reason other than collection, such as to evaluate or actually use the warez. Often warez downloaders are enthusiasts looking for the newest and coolest software.[224] Some warez downloaders also like getting something for

[221] *See* DOJ Warez Organizations, *supra* note 123. *See generally* Lemos, *supra* note 125; Adam L. Penenberg, *Where Do You Want to Pirate Today?*, FORBES, Aug. 8, 1997, *available at* http://www.forbes.com/1997/08/08/column.html; *The Truth About Piracy*, *at* http://www.defacto2.net/web.pages/gameover.1 (last visited Nov. 18, 2003) [hereinafter Truth Article].

[222] *See* McCandless, *Warez Wars*, *supra* note 10.

[223] *See* Team Report, *supra* note 60, at 16 (explaining that "some persons collect 'trophy' copies of software or video games simply to 'prove they can do it' and to add to their collection"); McCandless, *Warez Wars*, *supra* note 10 ("The more high-end and toolbar-tastic the app, the better"; quoting a warez collector as saying, "You end up collecting programs you don't need and never use. Just so you can say, 'I've got this or I've got that.' Or 'My version of Photoshop is higher than yours.'"); *id*. (explaining that collectors "feel unfulfilled unless they've swelled their coffers by at least one application a day . . . .' It's an obsessive game. We see it every day—people begging for something to 'finish their collection.'"); Granade, *Beelzebub*, *supra* note 208 (describing "warez hoarders" who "accumulate a collection of the most expensive software packages obtainable" which can be "worn like a badge to reflect a person's skill as a warez hunter").

[224] Stephen Poole, *PC Pirates*, CNET GameSpot.com, at 5 (on file with the Oregon Law Review) (quoting a warez downloader as saying "I love getting my hands on some new game that everyone has been hyping and giving it a run, or having someone say to me, 'Man, did you see that game? It looks real cool—I can't want till it comes out,' and being able to reply 'Yeah, I have it, but it's not that great.'"). *Cf.* Tetzlaff, *supra* note 10, at 107 (explaining that "the getting and the having mean more than the using"); Granade, *Beelzebub*, *supra* note 208 ("The thrill of the chase is just as important as achieving the goal of finding what you are searching for.").

nothing.[225] In contrast, many distributors and collectors never use the warez they have.[226]

- Abandonware traders are individuals who trade out-of-print software or games.[227] Some abandonware traders characterize themselves as archivists or historians;[228] others are just enthusiasts. Abandonware traders often seek to distance themselves from normal warez traders[229] because they believe their actions do not deprive a copyright owner of economic value.[230] However, from a legal standpoint, abandonware traders should be treated the same as warez traders under the Act.[231]

C. What Motivates Warez Traders?

Understanding the psychology and motivation of warez traders can help assess the likelihood that the Act will properly conform their behavior.

1. Ego

Fundamentally, almost all warez traders are motivated by ego. For warez distributors, "[t]he whole point . . . is to get the pirate

225 *See* Granade, *Warez*, *supra* note 8, at 2.

226 *See* Tetzlaff, *supra* note 10, at 104 (explaining that "warez enthusiasts generally acquire large libraries of software, most of which they have no desire or ability to ever use"); McCandless, *Warez Wars*, *supra* note 10; David Pogue, *Some Warez over the Rainbow*, MACWORLD, Oct. 14, 1997, at 3, *available at http://* preferhman.net/texts/underground/hacking/MACWORLD%20AGREEZ!!!.txt (explaining that "most warezers don't even use what they download" and quoting an industry representative as saying that "[t]hese kids have huge 3GB hard drives full of compressed software they can't even use, high-end stuff they don't have the manuals for").

227 *See* Granade, *Warez*, *supra* note 8, at 5. *See generally* Saltzman, *supra* note 204.

228 *See* Greg Costikyan, *New Front in the Copyright Wars: Out-of-Print Computer Games*, N.Y. TIMES, May 18, 2000, *available at* http://www.nytimes.com/library/tech/00/05/circuits/articles/18aban.html; Granade, *Warez*, *supra* note 8, at 6 (quoting an abandonware webmaster as saying, "Without abandonware sites, these games will be lost. I don't want them to be lost."); Saltzman, *supra* note 204 (saying abandonware site operators "do it out of love for oldies, and they think of themselves more as game historians than criminals").

229 *See* Granade, *Warez*, *supra* note 8 (suggesting that abandonware enthusiasts view warez traders as anarchists).

230 *See* Costikyan, *supra* note 228 (explaining that "publishers provide no legal way for gamers to get older games; the market is too small to justify the effort. So gamers feel justified in making vintage games available, despite the legal risks.").

231 However, abandonware traders may have a better basis to claim fair use because, by definition, their activities do not affect the work's market.

program released and distributed before any other group."[232] 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.[233] Fast distributions of impressive software evidences the individual or group's collection, cracking, and distribution skills,[234] contributing to a reputation for speed or quality cracking.[235]

To the participants, warez distribution and collection is a game or a competition.[236] Warez traders seek to win fame and respect by playing the game better than their peers.

2. *Thrill of the Illicit*

Many warez traders derive a thrill from doing something il-

[232] Jason Farnon, *Evolution of a Warez D00d*, *at* http://www.flashback. se/archive/AWA-001.TXT (last visited Nov. 11, 2003).

[233] *See* McCandless, *Warez Wars*, *supra* note 10 ("The ultimate bartering tools are zero-day warez. . . . The prizes for good zero-day warez vary; you may get instant download status on a particular server, logins and passwords for exclusive FTP sites, or admission to the ranks of a powerful cartel like the Inner Circle.").

[234] *See id.* (stating that to Warez distributors, "sticker prices mean[ ] nothing—except inasmuch as more expensive programs are harder to crack, and that makes them the most desirable, spectacular trophies of all. . . . The more the manufacturers harden a product, with tricky serial numbers and anticopy systems, the more fun it becomes to break."); McCandless, *Warez World*, TELEPOLIS (July 26, 2001), *at* http://www.heise.de/tp/english/inhalt/te/9170/1.html (quoting warez cracker TAG as saying "[software manufacturers] really don't want their stuff copied which makes it all the more tasty for someone with a reputation to keep up.") [hereinafter McCandless, *Warez World*].

[235] *See* McCandless, *Warez Wars*, *supra* note 10 ("NFO files do more than brag or supply installation instructions; they testify that the ware is a bona fide release, guaranteed to work. And this is more than just posturing; a group's reputation is paramount. Each release is painstakingly beta-tested. These are their products now, their labors of love. . . . Nobody wants to be accused of being 'unprofessional.'"); Customs Fact Sheet, *supra* note 127 ("Earning an online reputation as the fastest to steal, 'crack,' and release high-quality pirated software over the Internet is the most important to them.").

[236] *See* McCandless, *Warez Wars*, *supra* note 10 (warez trading is "a game, a pissing contest; a bunch of dicks and a ruler."); McCandless, *Warez World*, *supra* note 234 (quoting warez trader Diamond as saying "We are in it for the same reason some people try to do 200 foot jumps on a bike. It's all about saying we are cool and showing off."); Penenberg, *supra* note 221 ("Like winning a pinball tournament or turning over the scoreboard on *Missile Command*. It's about ego and ephemeral glory, about being 'the man'. . . ."); Truth Article, *supra* note 221 ("One of the [warez] scene's main motives that drive people to make this their hobby, almost their lives, is ego and competition. Competing groups push the members in the group to try to be #1 in the scene.").

licit.[237] According to one warez site operator, "deep down everyone is a little scared [of criminal prosecution] but that is also what keeps us going."[238]

3. *"Software Should Be Free"*

Almost all warez traders believe software should be free, and they view themselves as benefactors for the oppressed, like a cyber–Robin Hood.[239] Specifically, many warez traders view software manufacturers as oppressive and the software industry as the enemy.[240] With the "software should be free" philosophy,[241] many warez traders bitterly oppose commercial pirates who, like software manufacturers, commit the sin of charging for what should be free.[242]

[237] *See* Wagner, *supra* note 199, at 2; Tetzlaff, *supra* note 10, at 108 ("The thing that makes [warez trading] exciting is the forbidden quality of its prizes, the values and restrictions that come from outside the computer in the 'real' world of stores and cops and federal legislation.").

[238] *Id.* (quoting warez site operator NXSonic).

[239] *See* Tetzlaff, *supra* note 10, at 114 (quoting a warez trader as saying "[i]t is the role of pirated software to . . . make the technology and information that will determine the future available to everyone."); Miller, *Rat*, *supra* note 193, at 1M (saying that warez traders view "setting up a warez Web site is a noble thing to do" and quoting warez trader HippieGuy as saying, "It's like Robin Hood. Taking from the rich and giving to the poor."); Customs Fact Sheet, *supra* note 127.

[240] *See* McCandless, *Warez World*, *supra* note 234 (warez trading is "an act of bloodless digital terrorism. It's 'Fuck you, Microsoft.'"); McCandless, *Warez Wars*, *supra* note 10 ("In warez world, the software companies are the criminals"); Granade, *Beelzebub*, *supra* note 208 (quoting a warez site operator as saying "warez will live on forever in one form or another until something is done to redress the problems of high prices and bug ridden, section [sic] rate software."); Granade, *Warez*, *supra* note 8 ("Some people view warez use as a form of protest against software companies, a way to avoid what they see as exploitative pricing policies.").

[241] *See* Miller, *Rat*, *supra* note 193, at 1M ("Software pirates . . . said that all software should be free . . . . 'Software companies make plenty of money off businesses. The everyday guy should be able to use any program for free.'"); Wagner, *supra* note 199, at 2 (quoting a warez site operator as saying "people [trade warez] because we are tired of paying outrageous prices for software"). However, some warez traders say they support paying for software when the perceived value is commensurate with its price. *See* McCandless, *Warez Wars*, *supra* note 10 (quoting a warez distributor as saying "We do advocate buying your own software if you really like it and use it heavily.").

[242] *See* Tetzlaff, *supra* note 10, at 104 ("the practice of charging any form of actual money is frowned upon by most members of the warez scene."); Lee Gomes, *Software Makers Turn Small-Time Pirates into Political Prisoners*, WALL STREET J., Nov. 11, 2002, at B1 ("Selling any of the programs is anathematic."); McCandless, *Warez Wars*, *supra* note 10 (quoting several warez distributors who say they do not seek money, including one warez distributor saying, "We're not in it for the money. I would never sell something I got from warez."); Granade, *Beelzebub*, *supra* note 208 ("a pirate profits by acquiring software by whatever means and selling it on for

Historically, warez traders had a norm that to download warez, you must return something.[243] However, as the community's self-perception as cyber–Robin Hoods matures, some warez "traders" distribute warez freely, without any expectations in return.[244]

4. Sense of Community

Finally, warez trading permits traders to participate in a community and form friendships.[245] Many warez traders are social misfits in the physical world, but online they find kindred spirits.[246] As one warez trader said, "[w]arez d00dz want to belong. They have been shunned by everyone, and thus turn to cyberspace for acceptance."[247]

their own personal gain, but this, simply put is not the warez way; it goes completely against the scene's ethic of free software."); Truth Article, *supra* note 221 ("Some people sell copies of the latest software for profit; the [warez] scene for one simple fact also scorns this.").

[243] *See* Tetzlaff, *supra* note 10, at 106 ("The server operator makes the contents of his collection available for all to see. He asks that anyone who wishes to obtain some of these files first transmit to him some useful file he does not yet have. . . . This isn't just a matter of greed on the administrator's part, it also reflects a group ethic. If you would take, so also must you give."); McCandless, *Warez Wars*, *supra* note 10 ("On the freewheeling IRC chat forums, 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").

[244] *See* Granade, *Beelzebub*, *supra* note 208 (quoting a warez site operator as saying, "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, all you have to do is ask nicely or loiter in the right places.").

[245] *See id.* ("[The warez scene] is a club like any other, full of enthusiasts who share thoughts, ideas and friendships over a virtual medium. . . . Searching for warez gives you the chance to interact and form friendships with people from all over the globe, which otherwise you would not have the opportunity to do."); Former DrinkOrDie Member Chris Tresco Answers, Slashdot.com, Oct. 4, 2002, *at* http://interviews.slashdot.org/interviews/02/10/04/144217.shtml?tid=123 (discussing how a warez trader tried to quit his group several times, "but imagine a bunch of guys/gals sitting around talking all day and suddenly you stop showing up . . . You start to miss that type of interaction."); McCandless, *Warez World*, *supra* note 234 (quoting warez trader Diamond as saying, "You also make a lot of friends in the scene and that's the best part for me.").

[246] *See* Farnon, *supra* note 232 ("Warez d00dz get along so well because they can relate to each other so damn well."); Penenberg, *supra* note 221 (quoting a warez trader as saying, "If they can't make it in real life, they get into warez to try and be cool."). *Cf.* McCandless, *Warez Wars*, *supra* note 10 (discussing how warez traders posted obituaries for traders who had been busted, saying things like "We feel for ya!").

[247] Farnon, *supra* note 232.

D. Implications of Warez Traders' Motivations

The Act implicitly assumes that warez traders are rational actors who, like any others, will curtail behavior in response to threatened punishment. Indeed, building on that assumption, a number of commentators have argued that only criminal punishment will motivate warez traders,[248] and some have complained that the Act's penalties are too lenient to truly motivate.[249]

But it is wrong to assume that warez traders respond to this threat system so directly.[250] Warez traders do have standards and codes of ethics,[251] but they are indifferent to rules they do not believe in.[252] It is unrealistic to expect that they will conform to externally-imposed rules. More likely, criminal sanctions may only stroke warez traders' egos by increasing the impressiveness of their actions; the greater the punishment, the bigger the

[248] *See Hearings*, *supra* note 9, at 20 (statement of Marybeth Peters, Register of Copyrights) (stating that for individuals acting without a profit motive, "civil remedies are less likely to serve as an effective deterrent. Therefore, criminal sanctions are needed to deter these individuals from causing serious harm to the value of copyrighted works."), *available at* http://commdocs.house.gov/committees/judiciary/hju48724.000/hju48724 0.htm [hereinafter Peters Testimony]; Bernstein, *Net Zero*, *supra* note 76, at 58-59 ("There is no other way to deter online criminal infringement acts other than jail time.").

[249] *See* Karen J. Bernstein, *The No Electronic Theft Act: The Music Industry's New Instrument in the Fight Against Internet Piracy*, 7 UCLA ENT. L. REV. 325, 326 (2000) (stating that "the only way to fend off the non-profit Internet pirate is by increasing prison sentences for Internet pirates through the NET Act."); Andrea L. Foster, *Lawmakers Demand That Colleges Crack Down on Illegal File Sharing*, CHRON. HIGHER EDUC., Feb. 27, 2003, *available at* http://chronicle.com/cgi2-bin/printable.cgi?article=http://chronicle.com/free/2003/02/2003022701t.htm. *But see* Tyler, *supra* note 199 (arguing that increased sanctions play little role in motivating legal compliance).

[250] *See* Tyler, *supra* note 199, at 234 (stating that "reliance upon threats of punishment to enforce intellectual property laws is a strategy that is likely to be ineffective.").

[251] *See* McCandless, *Warez Wars*, *supra* note 10 (describing the warez traders' "commandments" as "[g]ood manners, good use of bandwidth, and good warez. Give unto others as you would have them give unto you."). Other "cardinal sins" include distributing virus-infected files, posting a "me too" comment, posting partial releases, posting a release in a single file instead of smaller pieces, and posting the URLs of secret FTP sites. McCandless, *Warez World*, *supra* note 234. Warez groups have also established standard protocols for the acceptable size and format of warez releases, Poole, *supra* note 224, at 10, and the release of "iso" files, http://www.defacto2.net/web.pages/iso.1/ (last visited Oct. 11, 2003).

[252] *See* Tetzlaff, *supra* note 10, at 115 (quoting a warez trader as saying "We KNOW what we are doing is wrong, yet we continue not because we have a need for the software we use, but because we want it."). Also consider the perspectives of a warez trader: "It's just that the moral impact of stealing doesn't hit us. We feel no remorse, usually." Truth Article, *supra* note 221.

thrill.[253] If so, Congress's efforts may counterproductively encourage, not inhibit, warez trading.

Criminalizing warez trading may also reinforce the warez traders' Robin Hood self-perception as do-gooders fighting unjust laws. As the laws become more stringent, warez traders may believe them increasingly unjust, in turn increasing the self-perceived moral justification for their actions.

Criminal sanctions also deepen warez traders' social bonds to each other. In an "us vs. them" world (where the "them" is software companies, the government, or any form of authority), warez traders already perceive themselves as outcasts. Criminalization further reinforces their status as outlaws having more in common with each other than with the rest of society. Once socialized into this community, warez traders have trouble leaving it because it becomes the only place where they feel like they belong.

Thus, the Act may very well fail at its core objective of deterring warez traders. Quite possibly, the Act may be counterproductively encouraging warez trading.

E. The Act's Coverage Overlaps With Other Factors Inhibiting Piracy

Finally, the Act's efficacy is weakened because other laws and systems duplicitously overlap with the Act and may have greater impact on infringers' behavior than the Act. Most obviously, copyright owners can sue infringers, which can be very effective at shutting down infringers. Some government officials believe infringers who are indifferent to money damages (because they are judgment-proof) cannot be motivated by civil lawsuits,[254] but copyright owners can shut down these infringers through injunctions.

Just the mere possibility of being sued can deter infringers.

[253] Tetzlaff, *supra* note 10, at 108 ("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.").

[254] 143 CONG. REC. S12689, S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch) ("For persons with few assets, civil liability is not an adequate deterrent."); Declan McCullagh, *DOJ to Swappers: Law's Not on Your Side*, CNET NEWS.COM, Aug. 20, 2002, *at* http://news.com.com/2100-1023-954591.html (citing a DOJ official as saying that civil infringement actions do not adequately intimidate judgment-proof file-sharers) [hereinafter, McCullagh, *Swappers*].

Certainly average Americans are highly swayed by the threat.[255] Thus, the record industry's recent lawsuit against P2P file-sharers has affected both file-sharing activity and Americans' psychology about file-sharing.[256] Even blasé warez traders can be influenced by the threat of a lawsuit.[257] For example, in 1999 the BSA civilly sued twenty-five individuals for trading warez in chat rooms, after which BSA enforcement official Bob Kruger claimed to "have seen an immediate impact on piracy in IRC channels as a result of the lawsuit."[258] Solely on the basis that civil remedies are highly effective at curbing infringement, some have questioned the need for the Act at all.[259]

[255] Graham, *supra* note 208 (citing how students on at least fifteen campuses pulled down file-sharing services in response to the recording industry's lawsuits against students operating mini-Napsters); Harmon, *supra* note 209, at A1 (describing two students who took down their mini-Napster systems after four other students got sued, including a University of Maryland student who took down his system within an hour of hearing the news because "I don't think I was doing anything wrong . . . . But who wants to face a $98 billion debt for the rest of their lives? I was scared."); Stanley A. Miller II & Dan Egan, *College Students Bond Over File-Swapping Suit*, MILWAUKEE J. SENTINEL, May 4, 2003, at A1 (quoting a Michigan Tech official as saying, "The cease-and-desist notice is enough of a wake-up call."), *available at* http://www.jsonline.com/news/gen/may03/138411.asp?; Winstein, *supra* note 123 (citing a confident music archive site operator who removed Metallica songs from his site after Metallica threatened civil suit against Napster users).

Ultimately, to obtain real deterrence of civil infringers, copyright owners may have no alternative to civil enforcements. This may explain the record industry's massive campaign targeting individuals who offer substantial amounts of music through P2P file-sharing networks. *See* John Borland, *RIAA Sues 261 File Swappers*, CNET NEWS.COM, Sept. 8, 2003, *at* http://news.com.com/2100-1023-3-5072564.html?.

[256] *RIAA Chief Says Piracy Lawsuits Have Changed Public Awareness*, 67 BNA PAT., TRADEMARK, & COPYRIGHT J. 130 (2003).

[257] *See* Gomes, *supra* note 242, at B1 (PWA's Robin Rothberg claimed he would have stopped trading based on a civil infringement action); Granade, *Beelzebub*, *supra* note 208 (quoting a warez site operator saying that he "would be only too willing to co-operate with [prosecutors or plaintiffs] in taking down the site before any legal proceedings took place" and that he hopes that prosecutors or copyright plaintiffs would contact him "before making any rash decisions"); Mark Moor, *Stealing It Softly—The Pirate Mr X*, HERALD SUN, June 4, 2003, *at* http://heraldsun.news.com.au/printpage/0,5481,6536520,00.html (describing a warez collector who plans to stop because of increased enforcement efforts).

[258] *Warez Chatters Busted: Piracy*, Wired News, Nov. 17, 1999, *at* http://www.wired.com/news/print/0,1294.32616,00.html.

[259] On this basis, several commentators have questioned the need for the Act. *See* Heneghan, *supra* note 36, at 44; David Loundy, *The Good, Bad, Ugly of Copyright Law Rewrites*, CHICAGO DAILY L. BULL., Jan. 8, 1998, at 5, *available at* http://www.loundy.com/CDLB/1998-Copyright.html (arguing that the LaMacchia loophole should have been closed through civil enforcement actions, not new legislation); Declan McCullagh, *The Copyright Conundrum*, CNET NEWS.COM, Oct. 14, 2002, *at* http://news.com.com/2010-1071-961818.html ("Before the NET Act became law,

Of course, having a strong civil liability scheme may not be enough. In some cases, criminal laws provide a useful or even necessary complement. Criminal penalties (especially jail time) can have strong deterrent effects, and the power to initiate a criminal prosecution can make enforcement easier by creating the ability to obtain search warrants[260] and bring cross-border enforcement actions.[261] And, to the extent infringements create social externalities, the government may be the optimal plaintiff to bear the enforcement costs. But even if those reasons are sufficient to warrant criminal coverage for infringement, other criminal laws overlap with the Act,[262] particularly with respect to large-scale warez trading:

- Large scale warez distributors like PWA, Fastlane, and DrinkOrDie improperly use third-party computer servers in a manner that likely violates the Computer Fraud and Abuse Act[263] and possibly analogous state computer crimes laws.
- When Intel employees exchanged company owned computer hardware for the right to access the PWA warez library, they likely committed theft or analogous crimes.
- In 1998, anti-circumvention laws[264] criminalized circum vention cracking, which most large-scale warez distributors systematically do.
- Distribution of pre release software or other corporate proprietary information could violate the Economic Espio nage Act.[265]

copyright holders already had the power to sue suspected infringers in civil court, and if the NET Act were to be repealed, they would retain that right.") [hereinafter McCullagh, *Conundrum*]. *See generally* Geraldine Szott Moohr, *The Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory*, 83 B.U. L. REV. 731, 752 (discussing idea that criminal sanctions should be a last resort, but legislators often act without considering the efficacy of civil legislation).

260 *Cf.* Hoppin, *supra* note 207 (citing how search warrants allowed an intellectual property plaintiff to get materials that would not have been feasibly obtained through discovery).

261 *See* McCullagh, *Swappers*, *supra* note 254 (quoting the DOJ's John Malcolm as saying that the government can enforce copyrights better than private plaintiffs because the government can conduct multi-jurisdictional and international investigations).

262 *See* William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505 (2001) (discussing that federal criminal laws routinely overlap). *See generally* DOJ IP CRIMES MANUAL, *supra* note 56, § III(A) (describing other criminal laws that protect copyrighted material beyond 17 U.S.C. § 506 (2000)).

263 18 U.S.C. § 1030 (2000), *available at* http://www4.law.cornell.edu/uscode/ 18/ 1030.html.

264 17 U.S.C. § 1201 (2000), *available at* http://www4.law.cornell.edu/uscode/ 17/ 1201.html.

265 *See* 18 U.S.C. §§ 1831-1839 (2000), *available at* http://www4.law.cornell.edu/

- Attaching .nfo files to warez could violate the DMCA provision protecting the integrity of copyright management information.[266]

In addition to civil copyright infringement and other criminal laws, other private actors regulate infringement covered by the Act. Internet access providers often proactively shut down systematic infringers before the copyright owner or government is even aware of the problem.[267] Universities are also playing an active role in mitigating infringement, promptly cooperating with takedown notices from copyright owners[268] and subjecting student infringers to the university's disciplinary system.[269] In addi-

uscode/18/pIch90.html. The Economic Espionage Act has been used to prosecute at least one misappropriator who acted without commercial advantage or private financial gain. *See* U.S. Department of Justice, Press Release, L.A. Man Pleads Guilty to Theft of Trade Secrets for Stealing Information to DirecTV 'Smart Card' (Apr. 28, 2003) (discussing the prosecution of Igor Serebryany, a student who stole DirecTV anti-piracy technology trade secrets from the law firm he worked at and posted them to hacker websites), *available at* http://www.usdoj.gov/criminal/cybercrime/serebryanyPlea.htm.

[266] *See* 17 U.S.C. § 1202(a) (2000), *available at* http://www4.law.cornell.edu/uscode/17/1202.html.

[267] *See* Tetzlaff, *supra* note 10, at 112 ("A warez pirate is much more likely to get in trouble with his ISP than with the SPA itself. In fact, this is how most pirates get shut down."). For example, University of Oregon network administrators caught and shut down Jeffrey Levy based on his high bandwidth usage. Andy Patrizio, *DOJ Cracks Down on MP3 Pirate*, WIRED NEWS, Aug. 23, 1999, *at* http://www.wired.com/news/politics/0,1283,21391,00.html.

[268] *See* Scott Carlson, *Recording Industry Sues 4 Students for Allegedly Trading Songs Within College Networks*, CHRON. HIGHER EDUC., Apr. 4, 2003 (discussing how schools like Michigan Tech and Princeton routinely cooperate with the recording industry), *available at* http://chronicle.com/free/2003/04/2003040401t.htm; Letter from Curtis J. Tompkins, President, Michigan Technological University, to Cary Sherman, President, Recording Industry Association of America (Apr. 4, 2003) (describing all of the steps Michigan Tech has taken to cooperate with the RIAA), *available at* http://www.admin.mtu.edu/urel/news/media_relations/95/.

[269] *See* John Borland, *Navy Disciplines Students for Downloading*, CNET NEWS.COM, Apr. 15, 2003, *at* http://news.com.com/2100-1025-996990.html (discussing how the Naval Academy disciplined eighty-five students for illegal file-sharing); Justine Maki, *University Cracks Down on File Sharing*, DIGITAL COLLEGIAN (Penn State), Apr. 21, 2003, *at* http://www.collegian.psu.edu/archive/2003/04/04-21-03tdc/04-21-03dnews-04.asp (discussing how 220 Penn State students were referred to Judicial Affairs because of file-sharing); Miller & Egan, *supra* note 255 (quoting a Michigan Tech official as saying that there was a zero recidivism rate for students prosecuted for file-sharing through the University disciplinary system).

Even the mere threat of discipline under a university system can be effective at conforming student behavior. *See* Adam VanOsdol, *Students Forced to Delete Music*, INDIANA DAILY STUDENT, Jan. 30, 2003, *at http://www.idsnews.com/story.php?id=14352* (quoting a file-sharing student who received a university letter instructing her to delete the files or she would be referred to the judicial board: "I was very,

tion, copyright owners also use technological protections to curb infringement.[270]

IV

WHAT EXACTLY DOES THE ACT CRIMINALIZE?

Section III discussed the Act's efficacy. Section IV now considers the other half of the equation—what social costs does the Act create?

A. Criminalization of Everyday Activities

It is generally undesirable policy to make every American a criminal. Even copyright owner industry groups agree that Congress should not "accidentally tak[e] a large percentage of the American people, either small business or citizens, into the gray

very scared. I thought I was going to jail. . . . I erased everything I had and deleted the program.").

[270] *See* Andrew Ross Sorkin, *Software Bullet is Sought to Kill Musical Piracy*, N.Y. TIMES, May 4, 2003, at A1 (discussing such technological techniques as "spoofing," redirection, "freeze," "silence" and "interdiction"); *see also* Brian Krebs, *Online Piracy Spurs High-Tech Arms Race*, WASH. POST, June 26, 2003 (discussing other technological efforts), *available at http://www.washingtonpost.com/ac2/wp-dyn/A34439-2003Jun26*.

The recording industry has used instant message technology to scare file-sharers and automated scripts to notify Internet access providers of alleged file-sharers. *See* John Borland, *RIAA to File Swappers: Let's Chat*, CNET NEWS.COM, Apr. 29, 2003, *at* http://news.com.com/2102-1025_3-998825.html. One such instant message read:

> COPYRIGHT INFRINGEMENT WARNING: It appears that you are offering copyrighted music to others from your computer. Distributing or downloading copyrighted music on the Internet without permission from the copyright owner is ILLEGAL. It hurts songwriters who create and musicians who perform the music you love, and all the other people who bring you music.
>
> When you break the law, you risk legal penalties. There is a simple way to avoid that risk: DON'T STEAL MUSIC, either by offering it to others to copy or downloading it on a 'file-sharing' system like this.
>
> When you offer music on these systems, you are not anonymous and you can easily be identified. You also may have unlocked and exposed your computer and your private files to anyone on the Internet. Don't take these chances. Disable the share feature or uninstall your 'file-sharing' software.
>
> This warning comes from artists, songwriters, musicians, music publishers, record labels and hundreds of thousands of people who work at creating and distributing the music you enjoy. We are unable to receive direct replies to this message.

Joris Evers, *Recording Industry Warns File Swappers Via IM*, MACCENTRAL.COM, Apr. 30, 2003, *at* http://maccentral.macworld.com/news/2003/04/30/riaawarning/.

area of criminal law."[271] Yet, the Act appears to do just that.

The everyday activities potentially covered by the Act are breathtaking in scope and ubiquity. Our digital society requires us to make copies—lots of copies—to function productively,[272] and all of those copies infringe if they involve third-party copyrighted works. Thus, the Act makes every file uploaded to the Internet or email forwarded to a friend the potential basis of criminal prosecution. The process of committing little acts of infringement is endemic in our lives, and all of those are, in theory, subject to scrutiny should we ever be prosecuted.[273]

But perhaps the most problematic everyday infringing activity is P2P file-sharing. As discussed above, fifty-seven million Americans use P2P file-sharing services, and the P2P file-sharing software programs KaZaA and Morpheus—the market leaders after Napster's shutdown—have collectively been downloaded over 360 million times.[274]

Yet, P2P file-sharers likely violate the Act. Some users download enough files to clear the Act's financial thresholds. But even lower-activity users automatically store files in a shared directory where other users can download the files, and some users altruistically choose to share infringing files.[275] In either of those cases, any actual downloads made could also count toward the financial threshold. If enough files are uploaded or downloaded, the user may clear the criminal financial thresholds.

[271] *Hearings on S. 893 Before the Subcomm. on Intellectual Prop. and Judicial Admin. of the House Comm. on the Judiciary* (1992) (statement of the Vice President and General Counsel, Computer and Communications Industry Association); *see* United States v. LaMacchia, 871 F. Supp. 535, 544 (D. Mass. 1994) ("It is not clear that making criminals of a large number of consumers of computer software is a result that even the software industry would consider desirable.") (footnote omitted), *available at* http://www.loundy.com/CASES/US_v_LaMacchia.html.

[272] *See* John Leland, *Beyond File-Sharing; a Nation of Copiers*, N.Y. TIMES, Sept. 14, 2003, § 9, at 1.

[273] *See* Nimmer on Copyright, *supra* note 7, § 15.01[A][2] (noting the frequency with which ordinary Americans have to make decisions under the Act).

[274] CNET DOWNLOAD.COM, *at* http://download.com.com/3101-2001-0-1.html (last visited Oct. 15, 2003); *see* Fred von Lohmann, *New Music Rules Are Needed*, DAILY PRINCETONIAN, Apr. 14, 2003 ("More Americans have used file-sharing software than voted for the President."), *available at* http://www.dailyprincetonian. com/archives/2003/04/14/opinion/7930.shtml.

[275] For a discussion about the sociological factors behind P2P file-sharing, *see generally* Lior Jacob Strahilevitz, Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks (John M. Olin Law & Economics Working Paper, 2d Series No. 162, 2002), *available at* http://www.law.uchicago.edu/Lawecon/WkngPprs_151-175/162.ls.file-swapping.pdf.

Alternatively, irrespective of a user's quantity of downloads or uploads, every file-sharer may be criminally infringing due to the expanded definition of "financial gain," which could apply to the sharer's receipt of other copyrighted works through the file-sharing system.[276]

There is little debate that P2P file-sharing could be criminal,[277] and Congress certainly has made it clear that it wants P2P file-sharing prosecuted. In Summer 2002, nineteen members of Congress, led by Sen. Joseph Biden, wrote to U.S. Attorney General John Ashcroft requesting that the DOJ make a priority of using criminal copyright laws to curtail infringement via P2P networks.[278] The letter specifically requested that the DOJ prosecute P2P network operators "who intentionally facilitate mass piracy" and individuals who "intentionally allow mass copying from their computer" over P2P networks.[279] In response, the DOJ pledged to bring criminal prosecutions against individual file-sharers, but no timetable has been set.[280]

[276] *See* McCullagh, *Conundrum*, *supra* note 259 (arguing P2P file-sharing is punishable under the Act because trades are made with an expectation of receipt of value); Declan McCullagh, *Perspective: The New Jailbird Jingle*, CNET NEWS.COM, Jan. 27, 2003, *at* http://news.com.com/2010-1071-982121.html [hereinafter McCullagh, *Jingle*]. *Cf.* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1015 (9th Cir. 2001) (finding that, based partially on the amended definition of financial gain, P2P file-sharing was "commercial" for purposes of a fair use analysis), *available at* http://www.law.cornell.edu/copyright/cases/239 F3d 1004.htm.

[277] This position has been taken by, among others, an aide to Rep. Cornyn and RIAA chief Hilary Rosen. *See* Declan McCullagh, *Share "True Crime," Do the Time*, CNET NEWS.COM, Nov. 12, 2003, at http://www.news.com.com/2100-1026-5106684.html (quoting a Cornyn aide); Declan McCullagh, *Congress Targets P2P Piracy on Campus*, CNET NEWS.COM, Feb. 26, 2003, *at* http://news.com.com/2102-1028-986143.html (quoting Hilary Rosen). Other commentators who have concluded that P2P file-sharing violates the Act include Aaron M. Bailey, Comment, *A Nation of Felons?: Napster, the NET Act, and the Criminal Prosecution of File-Sharing*, 50 AM. U. L. REV. 473, 531 (2000), *available at* http://www. wcl.american.edu/journal/lawrev/50/bailey.pdf, and Shayesteh, *supra* note 205, at 218 n.237. *Cf.* Gomes, *supra* note 242, at B1 ("Someone trading software on post-Napster services like Kazaa could, if they have enough software on their machine, be treated just like Mr. Rothberg."). *But see* McCullagh, *Jingle*, *supra* note 276 (quoting Prof. Jessica Litman as saying that automated storage of files in a shared directory may not constitute willfulness).

[278] Letter from Senator Joseph Biden et al. to U.S. Attorney General John Ashcroft (July 25, 2002), *available at* http://www.politechbot.com/docs/congress.p2p.letter.081002.pdf; *see* Declan McCullagh, *File-Swapping Foes Exert P2P Pressure*, CNET NEWS.COM, Aug. 13, 2002, *at* http://news.com.com/2100-1023-949533.html.

[279] Biden, *supra* note 278.

[280] McCullagh, *Swappers*, *supra* note 254 (quoting John Malcolm, Deputy Assistant Attorney General). In March 2003, Mr. Malcolm reiterated the commitment to

In the interim, Congress expresses continued frustration about P2P file-sharing. In February 2003, at a hearing of the House Judiciary Committee's Subcommittee on Courts, the Internet and Intellectual Property, some Subcommittee members, including Rep. Waters and Rep. Weiner, reinforced their view that P2P file-sharing is illegal.[281] Subcommittee members also blasted universities for not doing more to catch and penalize students engaged in P2P file-sharing and for failing to turn over violators to the government for prosecution.[282]

Even more recently, in July 2003, Rep. Conyers introduced the Author, Consumer, and Computer Owner Protection and Security (ACCOPS) Act of 2003,[283] which would remove any doubt about whether P2P file-sharing is illegal by criminalizing willful infringement through P2P file-sharing where a user makes even one file available for sharing. Congress's point could not be clearer: it hates P2P file-sharing and wants it stopped.

Despite Congress's exhortations, no P2P file-sharer has been prosecuted yet. More generally, there are a number of reasons why prosecutors may choose not to prosecute average Americans for everyday and common activities: the activity could be fair use, the activity may not clear the financial thresholds, evidence may be too difficult to collect, or the infringement may not be committed "willfully."[284]

Specifically, the willfulness standard plays a critical role in distinguishing between legal and criminal activity[285] and thus war-

prosecute P2P file-sharers. *See International Copyright Piracy: A Growing Problem with Links to Organized Crime and Terrorism: Hearing Before the Subcomm. on Courts, the Internet and Intellectual Prop. of the House Comm. on the Judiciary*, 108th Cong. 103 (2003) (statement of John Malcolm), *available at* http://commdocs.house.gov/committees/judiciary/hju85643.000/hju85643_0f. htm. In August 2003, Mr. Malcolm yet again reiterated a desire to prosecute P2P file-sharers but observed that it was hard to meet the thresholds and obtain the right evidence. *See* Jon Healey, *Man Pleads Guilty to Web Music Bootlegging*, L.A. TIMES, Aug. 22, 2003, at C1.

[281] *See* Declan McCullagh, *Congress Targets P2P Piracy on Campus*, CNET NEWS.COM, Feb. 26, 2003, *at* http://news.com.com/2102-1028-986143.html.

[282] *See* Foster, *supra* note 249.

[283] *See generally* http://www.eff.org/IP/P2P/CONYER_069.PDF.

[284] *See generally* Brown, *supra* note 177, at 153-64.

[285] *See* DOJ IP Crimes Manual, *supra* note 56, § III(E)(5) ("A key question in these developing criminal cases under these circumstances is evidence of willfulness."); NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[A][2] ("[T]he only bar against an overzealous prosecutor criminalizing nearly every copyright infringement case lies in the other prerequisite to criminal liability: willfulness."); Coblenz, *supra* note 170, at 250 ("Willfulness [is] the only significant difference between criminal and civil infringement."); Loren, *supra* note 22, at 846 (explaining that the willful-

rants more discussion. The U.S. Supreme Court has characterized willfulness as "'a word of many meanings' whose construction is often dependent on the context in which it appears."[286] Yet, Congress did not define willfulness in the Act.

This omission was not an oversight. The word's definition was discussed extensively in the legislative history, and some legislators wanted to define it explicitly.[287] Rep. Goodlatte proposed, but later withdrew, an amendment to the Act defining willfulness as requiring "*intent* to violate another person's copyright."[288] The House Report explains that Goodlatte's definition was opposed because the definition's reference to "intent" might change the current understanding of willfulness and "the majority view on the matter is that 'willful' conduct necessitates 'intent.'"[289]

But, intent of *what*? The House Report's comment obscures the central issue. Instead, the House Report says merely that the Act "will *not* change the current interpretation of the word as developed by case law and as applied by the Department of Justice."[290] In floor debates, Sen. Leahy repeated those words and continued, "nor does [the Act] change the definition of 'willful' as it is used elsewhere in the Copyright Act."[291]

Accepting these statements at face value,[292] this legislative his-

ness requirement is the only practical requirement distinguishing civil and criminal copyright infringement).

286 Bryan v. United States, 524 U.S. 184, 204 (1998) (quoting Spies v. United States, 317 U.S. 492 (1943)).

287 *See* H.R. Rep. No. 105-339, at 10 (1997); *see also* Letter from the American Association of Law Libraries et al. to Honorable Henry J. Hyde, Chairman, House Judiciary Committee (Oct. 3, 1997) (urging the Act should include the phrase "intent to violate another's copyright"), *available at* http://www.ll.georgetown.edu/aallwash/lt100397.html.

288 H. REP. NO. 105-339, at 10 (1997).

289 *Id.*

290 *Id.*

291 143 Cong. Rec. S12,689, S12,690 (daily ed. Nov. 13, 1997). This statement is ambiguous because arguably it tries to reference how the term is used in the civil copyright context. For discussion about differences in the word's usage in civil and criminal copyright contexts, see Ting Ting Wu, *The New Criminal Copyright Sanctions: A Toothless Tiger?*, 39 IDEA 527 (1999), *available at* http://www.idea.pierce law.edu/articles/39/39_4/16.Wu.pdf.

292 This qualifier is necessary because at least two legislators expressly said they were overturning case law pertaining to willfulness. Reps. Coble and Goodlatte said that the Act rejects cases holding that evidence of reproduction and distribution of copyrighted works, by itself, can establish willfulness. 143 CONG. REC. H9883, H9884 (statement of Rep. Coble); *accord* 143 CONG. REC. H9883, H9886 (statement of Rep. Goodlatte). Elsewhere, Rep. Coble said that "minority case law from the

tory still does not clarify matters because, as discussed below, the existing case law was inconsistent.[293] Further, where the legislators did explain their views on the word, the articulations were also inconsistent and suggest a split of opinion between the House and Senate.[294]

In the Senate discussions, Sen. Hatch articulated a traditional definition of willfulness as "the intent to violate a known legal duty."[295] In contrast, in the House discussions, Rep. Coble articulated a more lax definition of willfulness:

> It should be emphasized that proof of the defendant's state of mind is not required. The Government should not be required to prove that the defendant was familiar with the criminal copyright statute or violated it intentionally. Particularly in cases of clear infringement, the *willfulness standard should be satisfied if there is adequate proof that the defendant acted with reckless disregard of the rights of the copyright holder*. In such circumstances, a proclaimed ignorance of the law should not allow the infringer to escape conviction. Willfulness is often established by circumstantial evidence, and may be inferred from the facts and circumstances of each case.[296]

The willfulness definition has not gotten any clearer since the Act's passage. The academic commentary remains confused about the implications of the willfulness standard,[297] and while

Second and Ninth Circuits which facilitated criminal prosecution of infringement in the absence of some evidence of deliberate intent cannot be invoked by authorities" prosecuting NET Act cases. Coble, *supra* note 37, at 302.

[293] *See* Susan W. Brenner, *Defining Cybercrime: A Review of State and Federal Law*, *in* CyberCrime: The Investigation, Prosecution and Defense of a Computer-Related Crime 11, 23-24 (Ralph D. Clifford ed., 2001); *infra* notes 300-01 and accompanying text.

[294] *See* DOJ IP Crimes Manual, *supra* note 56, at § III(B)(3) (discussing the differing perspectives on willfulness from the legislators).

[295] 143 Cong. Rec. S12,689, S12,689 (daily ed. Nov. 13, 1997). Senator Hatch continues: "As Chairman of the Judiciary Committee, that is the interpretation that I give to this term. Otherwise, I would have objected and not allowed this bill to pass by unanimous consent." *Id.* This standard was also supported by the Business Software Association, *Hearings*, *supra* note 9, at 85 (statement of Brad Smith, Associate General Counsel, Microsoft) (stating that "under criminal law a willful act requires that it be intentionally done with knowledge that it was prohibited by law."), and the Register of Copyrights, *id.* at 31 (statement of Marybeth Peters).

[296] 143 Cong. Rec. H9883, H9884 (daily ed. Nov. 4, 1997) (emphasis added); *accord* 143 CONG. REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte); 143 CONG. REC. H9883, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Frank) (approving Rep. Goodlatte's statement).

[297] *Compare* Note, *The Criminalization of Copyright Infringement in the Digital Era*, 112 HARV. L. REV. 1705, 1716 (1999) (arguing that the NET Act codified the "intent to infringe" definition) [hereinafter Harvard Note] *with* Bailey, *supra* note

many cases have interpreted the term willfulness in a civil infringement context, relatively few cases have done so in criminal copyright cases.[298] As a consequence, the case law continues to create "uncertainty in an area already filled with vagueness, gray areas, and doctrines with no bright line rules."[299]

Almost everyone agrees that there is a majority and minority view with respect to willfulness in the criminal copyright infringement context. The majority view 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.[300] The minority view is that willfulness requires the government to prove only that the defendant had the intent to copy.[301]

For purposes of understanding how the Act impacts our everyday activities, the difference between the views is critical. Under the majority view, defenses to willfulness include the infringer's ignorance of the law,[302] an infringer's subjective good-faith belief

277, at 493 n.129 ("The legislative history of the NET Act appears to indicate that criminal infringement is meant to be a strict liability crime."). Both extreme positions are questionable; but Bailey's position is more so. *See* H.R. REP. NO. 105-339, at 10 (1997) (citing with approval the DOJ's distinction between criminal copyright infringement and civil copyright infringement because the latter is a strict liability tort—meaning, by implication, that criminal copyright infringement is not).

[298] Loren, *supra* note 22, at 876.

[299] *Id.* at 879.

[300] SCOTT, *supra* note 170, at 277 (citing United States v. Moran, 757 F. Supp. 1046 (D. Neb. 1991)); *accord* Randy Gidseg et al., *Intellectual Property Crimes*, 36 AM. CRIM. L. REV. 835, 854 (1999); Heneghan, *supra* note 44, at 34; Megan K. Maher & Jon Michael Thompson, *Intellectual Property Crimes*, 39 AM. CRIM. L. REV. 763, 788 (2002); Wu, *supra* note 291, at 547-48. Nimmer characterizes this as the "better" view. NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[A][2].

[301] SCOTT, *supra* note 170, at 277; *accord* Gidseg et al., *supra* note 300, at 854 (characterizing this doctrine as applicable only in the Second and Ninth Circuits); Loren, *supra* note 22, at 877. Scott characterizes the minority view as "doubtful" and says the language added by the Act to 17 U.S.C. § 506(a)(2) ("evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement") further casts doubts on this view's viability. SCOTT, *supra* note 170, at 277. Nimmer says that this added language precludes any prosecutions based on simple proof of conduct violating the Copyright Act. NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[B][2]. Loren says the minority cases "are not nearly as definite as commentators have made them out to be" and suggests that, in even those cases, prosecutors need to show that the defendants knew that the law prohibited their copying. Loren, *supra* note 22, at 877.

[302] SCOTT, *supra* note 170, at 278; Loren, *supra* note 22, at 869; Wu, *supra* note 291, at 549-51.

that the use was fair,[303] and the infringer's subjective good-faith belief that the infringing work was not actually infringing, because the new work was not substantially similar to the preexisting work or a defense such as the First Sale doctrine applied.[304]

If ignorance of the law is a defense, then many otherwise infringing activities would escape punishment. Only in rare cases can prosecutors overcome that defense.[305] Similarly, a defense that the infringer had a good faith belief that the use was fair would significantly narrow the Act's scope. With the fair use defense's inherent unpredictability and inconsistency, defendants can legitimately believe that most de minimis infringements committed during everyday activity constitute fair use. However, case law has already said that P2P file-sharing[306] and warez trading[307] are not fair use, so defendants may lack a good faith belief in those situations.

Thus, under the majority view, the Act only criminalizes commercial-scale infringers who have no hope of claiming ignorance of the law or fair use. Indeed, some commentators criticize the majority view for this very reason.[308] However, whether one agrees or disagrees with the policy implications of the majority view, there is some chance that the majority view will not apply in a particular case. In those cases, the minority view should apply, and defenses like ignorance of the law and a good faith but erroneous belief in fair use may not be available.

This ambiguity forces rational, informed actors to stay clearly

303 NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[A][2]; Loren, *supra* note 22, at 869, 887; Wu, *supra* note 291, at 549-51.

304 NIMMER ON COPYRIGHT, *supra* note 7, § 15.01[A][2]; Loren, *supra* note 22, at 869; Wu, *supra* note 291, at 548-49. The First Sale doctrine permits a person possessing an authorized copy of a copyrighted work to sell or dispose of that copy without violating the copyright owner's exclusive right to distribute. *See* 17 U.S.C. § 109(a) (2000).

305 *See* DOJ IP Crimes Manual, *supra* note 56, § III(B)(3) (discussing ways to overcome a defense of ignorance of the law).

306 *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1017 (9th Cir. 2001), *available at* http://www.law.cornell.edu/copyright/cases/239 F3d_1004.htm.

307 United States v. Slater, 348 F.3d 666, 669 (7th Cir. 2003).

308 *See* Wu, *supra* note 291, at 538; *see also* Heneghan, *supra* note 44, at 36 ("If a person can claim 'fair use' and escape criminal penalties, then the law has no teeth since alleged infringers will invariably assert this defense."); Lauren Yamamoto, Note, *Copyright Protection and Internet Fan Sites: Entertainment Industry Finds Solace in Traditional Copyright Law*, 20 LOY. L.A. ENT. L.J. 95, 118 (2000) (stating that the willfulness standard "emasculates" the Act), *available at* http://elr.lls.edu/ issues/ v20-issue1/yamamoto.pdf.

away from criminal behavior,[309] necessarily curtailing some legal and socially desirable activity.[310] Nimmer provides a good example of such consequences.[311] Dennis Erlich, a critic of the Church of Scientology, electronically disseminated copyrighted works owned by the Church as part of ridiculing those works. While some cases treat such infringing ridicule as fair use,[312] Erlich lost his case.[313] Under the minority view, the Act could make Erlich criminally liable for his infringement.[314] With criminal exposure for infringing ridicule, this type of social commentary will necessarily be chilled. By potentially creating strict limits on what forms of ridicule are permissible, the Act has a significant social cost.

At minimum, a clear willfulness definition would expedite decision-making. While Congress failed to provide that, the Act did say that "evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement."[315] Unfortunately, this language does not help courts select between the majority and minority definitions, for the same reasons that the House Report's statement "willfulness requires intent" says nothing. For now, we can only hope that prosecutors continue to select cases with the majority view in mind and that enough people remain uninformed about the law so that they do not actually curtail beneficial activities. Ultimately, the courts may need to do what Congress failed to do and clearly define willfulness in the criminal copyright infringe-

309 *See* Loren, *supra* note 22, at 894 ("An interpretation of the willfulness requirement of criminal infringement that does not require proof of knowledge of the legal duties in the Copyright Act will thwart the underlying, constitutionally mandated goal of copyright law by making individuals more reluctant to engage in activities that may, in fact, be permitted by the [Copyright Act].").

310 *See* Moohr, *supra* note 259, at 760-61; Harvard Note, *supra* note 297, at 1706 ("By overdeterring private users, increased criminal penalties for copyright infringement will inhibit the free flow of information and thus impose costs that outweigh the benefits from discouraging piracy."). *See generally* Reno v. ACLU, 521 U.S. 844, 872 (1997) (discussing the detrimental impact of criminal laws on socially beneficial activity on the Internet), *available at* http://supct.law.cornell.edu/ supct/html/96-511.ZS.html.

311 *Hearings*, *supra* note 9, at 155-56 (statement of David Nimmer).

312 *E.g.*, Belmore v. City Pages, Inc., 880 F. Supp. 675, 678 (D. Minn. 1995).

313 Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1250 (N.D. Cal. 1995).

314 *Hearings*, *supra* note 9, at 156 (statement of David Nimmer).

315 17 U.S.C. § 506(a)(2) (2000), *available at* http://www4.law.cornell.edu/uscode/17/506.html.

ment context.[316]

B. Criminalization of Facilitators

The Act's coverage also leaves open the degree to which "facilitation" is criminalized. This ambiguity can be traced to the Act's inception, because arguably LaMacchia did not commit copyright infringement at all. While LaMacchia created and maintained Cynosure, which others used to commit copyright infringement, the government did not allege that LaMacchia uploaded or downloaded any copyrighted material himself.[317] While the Act should apply easily to Cynosure users for the files those users personally uploaded and downloaded, it is less clear why LaMacchia's facilitation role should be criminalized.

Unfortunately, Congress did not specifically address why LaMacchia's actions were criminal or how the statute distinguishes between infringers and facilitators. As with the willfulness definition, when this issue was raised to Congress,[318] a number of legislators made strong remarks that they did not want the Act to cover Internet access providers,[319] and Nimmer even proposed language to correct this deficiency.[320]

However, Congress ultimately acknowledged this issue only

316 *Cf.* Loren, *supra* note 22, at 885 ("The importance of a clear understanding of the contours of the willfulness standard for determining whether the government has carried its burden of showing that the infringing conduct was criminal cannot be overstated.").

317 *See supra* note 15 and accompanying text.

318 *See*, *e.g.*, *Hearings*, *supra* note 9, at 148-56 (statement of David Nimmer).

319 *See*, *e.g.*, 143 CONG. REC. S12689, S12690 (daily ed. Nov. 13, 1997) (statement of Sen. Leahy) (stating that libraries and other Internet access providers were not covered by the Act because they lack willfulness); *Hearings*, *supra* note 9, at 7, 50, 163 (statement of Rep. Frank).

320 At the Subcommittee Hearings, Nimmer proposed an alternative standard for criminal infringement: "Whoever places copyrighted, commercially-marketed material on a computer system with the intent that it be accessible by the public without the consent of the owner of the copyright shall be punished as provided [by law.]" *Hearings*, *supra* note 9, at 150 (statement of David Nimmer). This standard would have provided much-needed clarity on both the facilitator/infringer distinction and willfulness issues. Nimmer argued that this language would still have criminalized LaMacchia's behavior, *id.*, although if LaMacchia did not actually place any items on Cynosure, he could be punished under Nimmer's proposed language only under an accomplice or conspiracy theory based on his encouragement and integral participation in the warez operation. Because he felt Nimmer's proposal overly immunized service providers, Rep. Frank emphatically rejected it, characterizing it as "a very grudging fix" with "huge loopholes" and "an opening negotiating position" that was "not a good use of everybody's time." *Hearings*, *supra* note 9, at 161 (statement of Rep. Frank).

through the weak clarifying language regarding willfulness discussed above.[321] How does this language distinguish Internet access providers from LaMacchia? In other words, exactly what did LaMacchia do beyond operating a website that reproduced and distributed copyrighted works?

Two facts might distinguish LaMacchia from Internet access providers. First, LaMacchia encouraged infringement because he allegedly requested his users to upload specific software to Cynosure, and second, he knew Cynosure users would exchange pirated software and wanted them to do so.[322] While superficially these differences may distinguish LaMacchia from an Internet access provider who passively transmits packets across its network, these factors do little to distinguish other types of online service providers like web hosts that host infringing content or directories or search engines that link to infringing content.[323]

Indeed, any individual or entity who commits contributory civil infringement probably has criminal willfulness under either the majority or minority view.[324] Contributory civil copyright infringement occurs when an individual with "knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[325] Certainly anyone who meets

321 *See* 143 CONG. REC. H9883, H9884 (daily ed. Nov. 4, 1997) (statement of Rep. Coble) (saying the language means that the Act excludes third parties who electronically reproduce or distribute works on behalf of a third party); 143 CONG. REC. H9883, H9885-86 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte) (believing that this language removed Internet access providers from the Act); *see also* Courtney Macavinta, *Congress Approves Copyright Bill*, CNET NEWS.COM, Nov. 18, 1997, *at* http://news.com.com/2100-1023-205520.html ("[T]he language of the final bill makes it clear that ISPs and online services will not be held as 'willfully infringing' just by doing their job, which is routing data across their servers.") (quoting David McClure, Executive Director, Association of Online Professionals).

322 *See* 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. For example, LaMacchia posted the following text on Cynosure: "If anyone has this stuff, I'd appreciate it. Sim City 2000, Excel 5.0 (Windoze), WordPerfect 6.0 (Windoze)." *Id.* He also provided instructions about how to upload files and encouraged uploading. *Id.*

323 At the 1997 Subcommittee Hearing, most of this discussion regarding facilitator liability focused on "passive carriers" like Internet access providers and did not explore other forms of facilitation. *Hearings*, *supra* note 9, at 50-54, 64-65.

324 *See* DOJ IP Crimes Manual, *supra* note 56 § III(E)(2) (in the case of Internet infringement, the prosecutor has to prove that the defendant "maintained some form of knowing control over the content and maintenance of the subject Web site"—in other words, contributorily infringed).

325 Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

this standard will satisfy the minority view, but the combination of scienter and involvement should satisfy the majority view as well. In the DMCA, Congress putatively provided some facilitators a safe harbor from civil liability for user-caused infringement,[326] but this safe harbor has proved largely illusory because it does not appear to apply when an online service provider meets the standard for contributory copyright liability.[327] So, anyone who contributes to civil copyright infringement may also be a criminal infringer (assuming, if applicable, the financial thresholds are met).

Specifically, to the extent the provider otherwise meets the definition of contributory infringement, any of the following activities could lead to criminal prosecution: allowing artists to upload MP3 files for others to enjoy,[328] providing access to USENET newsgroups where some postings contain infringing content,[329] establishing web links to infringing content (either directly or by allowing a user to do so),[330] operating P2P file-sharing services,[331] allowing users to conduct auctions of infringing

[326] 17 U.S.C. § 512(a), (c), (d) and (e) (2000), *available at* http://www4.law.cornell.edu/uscode/17/512.html.

[327] 17 U.S.C. § 512(c)(1)(A); 17 U.S.C. § 512(d)(1), *available at* http://www4.law.cornell.edu/uscode/17/512.html; *see* Jennifer Bretan, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43 (2003).

[328] *See* Playboy Enter., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 2d 503 (N.D. Ohio 1997); *Cf.* Los Angeles Times v. Free Republic, 2000 U.S. Dist. LEXIS 5669 (C.D. Cal. 2000) (denying a fair use defense on the part of a website that allowed users to post news stories for comment and criticism), *available at* http://www.law.uh.edu/faculty/cjoyce/copyright/release10/LosAngT.html.

[329] *See* ALS Scan, Inc. v. RemarQ Cmties., Inc., 239 F.3d 619 (4th Cir. 2001) (finding contributory liability in this context), *available at* http://www.lclark.edu/~loren/cyberlaw01/alscan.pdf.

[330] *See Hearings*, *supra* note 9, at 65 (statement of Marybeth Peters) ("Clearly you would aid and abet if you had a site that said 'Top ten pirated sites' and led everybody to them."); DOJ IP Crimes Manual, *supra* note 56, § III(E)(5) (discussing theories of how to prosecute for linking to infringing content); Goldstone & O'Leary, *supra* note 205, at 38-39 (discussing how criminal liability for facilitation might attach on an aiding-and-abetting theory to individuals who link to infringing content if the individual encourages infringement, evidences intent to infringe or has an illicit relationship with the linked-to site); Shayesteh, *supra* note 205, at 214 (arguing that linking to warez should create contributory liability).

[331] *See* Bailey, *supra* note 277, at 496-97 and 511 (arguing that P2P file-sharing service Napster could be liable for conspiracy or aiding and abetting). Cases holding P2P file-sharing services contributorily liable include A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), *available at* http://www.law.cornell. edu/copyright/cases/239_F3d_1004.htm and *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), *available at* http://www.ca7.uscourts.gov/op3.fwx?submit1=showop&caseno=02-4125.PDF. *See supra* notes 278-83 and accompanying text (discussing

items,[332] operating swap meets,[333] and operating a marketing network for web sites that host infringing content.[334]

Obviously, many of these activities are primarily undertaken commercially, so the risk of criminal liability in those cases did not change due to the Act. But should anyone want to undertake these activities non-commercially, especially to promote social causes that cannot support a commercial endeavor or are not permitted by commercial operations, the risks of criminal infringement could overwhelm the desire to do so. In this respect, the failure to more clearly delineate between infringers and facilitators once again can curtail socially beneficial activities.

V

DEFINING THE PROPER SCOPE OF CRIMINAL COPYRIGHT INFRINGEMENT

The previous Section discussed some practical harms created by poor statute drafting. More conceptually, the shoplifting analogy underlying the Act creates a scope problem.[335] This analogy treats every infringing copy as creating a criminally cognizable loss[336] even though such treatment overstates copyright owners' lost revenues and copyright owners' expenses not actually realized.[337] In turn, by overstating copyright owners' harms, the boundaries of criminal copyright law are extended too far.

The analogy overstates copyright owners' lost revenues be-

Congress' demands to prosecute these infringers). *But see* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 2003 U.S. Dist. LEXIS 6994 (C.D. Cal. 2003) (rejecting contributory liability on the part of a P2P file-sharing software vendor), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/030425 order_on_motions.pdf.

[332] *See* Bob Liu, *'Safe Harbor' Case Mired in Confusion*, INTERNETNEWS.COM, May 15, 2003, *at* http://boston.internet.com/news/print.php/2206911 (discussing a case holding Amazon.com liable for contributory infringement for an infringing DVD made available for sale through its auction tools). *But see* Hendricks v. Amazon.com, Inc., No. CV 02-08443 TJH (C.D. Cal. Dec. 8, 2003).

[333] *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), *available at* http://www.law.cornell.edu/copyright/cases/76_F3d_259.htm.

[334] *See* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

[335] See Moohr, *supra* note 259, at 756-57.

[336] ARIEL KATZ, A NETWORK EFFECTS PERSPECTIVE ON SOFTWARE PIRACY 44 (University of Toronto Faculty of Law, Law and Economics Research Paper No. 03-01, 2003), *available at* http://papers.ssrn.com/sol3/delivery.cfm/SSRN_ID386141_code030310570.pdf?abstractid=386141 ("[T]he governing paradigm of copyright law . . . assumes that every unauthorized copy of a protected work harms the copyright holder . . . .").

[337] Team Report, *supra* note 60, at 15-16.

cause more copies are treated as a criminal loss than are actually lost. This overcounting occurs because individuals have heterogeneous reservation prices for copyrighted works, so some individuals may procure a cheap infringing copy (where the cost is below their reservation price) but would not have procured a more expensive copy (where the cost exceeds their reservation price).[338] In those cases, not every copy substitutes for the original; some may be evaluation copies, trophies, or never used at all.

This phenomenon is most obvious in cases where infringing copies can be procured for free. In those cases, the infringing work's "cost" (zero) is below everyone's reservation price, and thus more copies are made than would have occurred at a higher price.[339] Theoretically, a copyright owner's actual loss could be accurately calculated by recreating a demand curve and excluding all copies procured by infringers whose reservation price was below the retail value. Without such calculations, treating each copy as a loss to copyright owners overstates the true demand for the work.

The analogy also overstates lost revenues because some copyright owners may implicitly want infringement to occur. Specifically, software vendors may tolerate piracy either as a way to price discriminate against individuals with heterogeneous reservation prices or to create barriers to entry by locking in users (network effects).[340] If so, the Act may counterproductively criminalize behavior that software vendors desire and encourage.

The shoplifting analogy also ignores expenses a copyright owner did not incur. Shoplifting protects retailers from the expropriation of rivalrous goods, where a retailer is deprived of the good and the money spent to procure it. In contrast, copyrighted works are non-rivalrous, so infringement by copying does not de-

[338] *See generally* Stuart P. Green, *Plagiarism, Norms, and the Limits of Theft Law: Some Observations on the Use of Criminal Sanctions in Enforcing Intellectual Property Rights*, 54 HASTINGS L. J. 167 (2002) (discussing the problems of criminalizing the theft of intangibles).

[339] Certainly in the case of warez traders, the reservation price of most of the items they download or collect is zero. *See* Tetzlaff, *supra* note 10, at 109 ("With the exception of a few games, there is probably nothing in [a warez trader's] collection that he would buy if he couldn't obtain it for free.").

[340] *See*, *e.g.*, Katz, *supra* note 336; Stan Liebowitz, *Policing Pirates in the Networked Age*, POLICY ANALYSIS, May 15, 2002, at 4 (discussing theories), *available at* http://www.cato.org/pubs/pas/pa438.pdf.

prive a retailer (or anyone else) any direct out-of-pocket costs.[341]

By overstating the harm suffered by the copyright owner, the Act extends the criminal borders to situations where the law treats the infringement as causing criminal harm, even though no actual harm has occurred to the copyright owner. As we saw with the consequences of an imprecise definition of willfulness, this focus on technical, not substantive, harm puts otherwise socially-permissible activities in jeopardy.

The broad definition of "loss" prompts a more fundamental inquiry. Because we cannot determine with precision when real loss occurs, at what point should loss suffered by a copyright owner be recognized as criminal harm?

Specifically, once Congress internalized the shoplifting paradigm, Congress had to decide how much "loss" warrants criminal punishment. The answer: $1,000 of copyrighted works in a six-month period. There are no minimum number of infringing copies and no need to show connections between disparate acts of infringement.[342] Thus, the Act equally criminalizes individuals who willfully infringe a single work worth more than $1 million and individuals who, in aggregate, willfully infringe $5.56 per day doing normal daily activities.

In today's digital society, this financial threshold is uncomfortably easy to reach. Consider an individual who downloads a few MP3 files every day using a P2P file-sharing software, softlifts a couple of software programs for telecommuting purposes, and forwards by email an article or two a day to friends. Each individual incident of infringement may be trivial, but in 180 days the aggregate consequence of these activities could easily pass the $1,000 threshold.[343] If so, willfulness and prosecutorial discretion are the only things that keep this individual out of jail—even if

[341] *Cf.* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 450 n.33 (1984) (rejecting an argument that copyright infringement can be analogized to the theft of a physical item), *available* at http://www.eff.org/Legal/Cases/sony_v_universal_decision.html.

[342] *See* H.R. Rep. 102-997, at 6 (1992) (discussing the desire to aggregate different copyrighted works in the same prosecution).

[343] Bailey illustrates how a P2P file-sharer using a high-speed connection could reach the financial threshold after three hours of downloading. *See* Bailey, *supra* note 277, at 519-20. Duncan Frissell illustrates how a P2P file-sharer could reach the financial threshold by averaging nine music downloads per day. Posting of Declan McCullagh, declan@well.com, to politech@politechbot.com (July 25, 2001, 20:28:14), *at* http://politechbot.com/p-02305.html.

none of these activities cause the copyright owner any actual economic loss.

So how did this threshold—$1,000 in 180 days—get set so low? The DOJ expressed reservations about the broad sweep of a low dollar threshold,[344] as did the Register of Copyrights, who advocated that criminal liability should require "substantial economic harm."[345] Recall that LaMacchia had been accused of infringing over *$1 million* of software in a little over a month.[346] If the goal was to make sure prosecutors could bust LaMacchia, how did Congress go from LaMacchia's $1,000,000 in one month to the Act's $1,000 in 180 days?

As initially introduced in the House, the first draft of the Act proposed a felony standard of $5,000 and a misdemeanor standard of $0 (that is, every willful infringement was a misdemeanor).[347] The House Report implies that, after the 1997 Subcommittee Hearing, a back-room deal was struck to address concerns that the proposed misdemeanor standard overly criminalized de minimis activities.[348] To avoid that, the misdemeanor standard rose to $1,000 and the felony standard remained at $2,500 (the threshold prior to the Act) instead of the proposed $5,000.[349]

It might seem odd that the Act initially proposed an initial financial threshold of $0 for misdemeanors, but it should not. Because the shoplifting analogy treats every copy as criminally-cognizable harm, why should copyright owners lose a penny? The $0 proposed threshold was the inevitable implication of the shoplifting analogy.

However, the $1,000 "compromise" appears to be wholly arbitrary and not particularly effective. Congress did not cite any supporting evidence to show how the financial threshold provides any meaningful safe harbor for de minimis infringement. From the prosecutor's perspective, proving $1,000 of infringement beyond a reasonable doubt may create significant eviden-

[344] *Hearings*, *supra* note 9, at 45 (statement of Kevin DiGregory).

[345] *Id.* at 30 (statement of Marybeth Peters). Peters proposed a financial threshold of $5,000 in 180 days. *Id.*

[346] *See* 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.

[347] H.R. 2265, 105th Cong. (1997).

[348] H.R. REP. NO. 105-339, at 8 (1997).

[349] *Id.*

tiary and proof problems that, in practice, limit the defendants who can realistically be pursued. But from a defendant's perspective who wants to avoid any risk of criminal infringement and who has full information about all of the infringements he or she has committed, the standard of $5.56 of infringement per day has the practical consequence of criminalizing aggregated de minimis infringements.

To solve this problem, the financial threshold could be raised,[350] or the financial threshold could be met only through a single coordinated set of activities (such as all downloads made from a warez site operated by the defendant) instead of disparate unrelated activities. Alternatively, the time horizon for aggregating infringements could be reduced, say to one week instead of six months, increasing the minimum daily infringement to $142.

One other simple solution should be considered: eliminating 17 U.S.C. § 506(a)(2) entirely. If Congress wants to criminalize systematic warez trading, it has already successfully done so by redefining "financial gain" to include bartering.[351] This definition has already successfully contributed to some warez trader convictions[352] and should successfully apply to most or all large-scale warez trading cases. Meanwhile, the financial gain definition, even as redefined, does not expose most daily activities to infringement for daily activities, which rarely are done with any expectations of value in return. Thus, the simple deletion of 17 U.S.C. § 506(a)(2)—effectively undoing the shoplifting analogy—still preserves Congress's true objectives without unnecessarily broad criminal boundaries.

350 Heneghan proposes a financial threshold of at least $100,000. Heneghan, *supra* note 44, at 34.

351 *See* 17 U.S.C. § 101 (West 2001 & Supp. 2003), *available at* http://www4.law.cornell.edu/uscode/17/101.html; Fois, *supra* note 35; 143 CONG. REC. S12689, S12690 (daily ed. Nov. 13, 1997) (statement of Sen. Leahy) (expecting the revised definition to cover bartering for or trading pirated software). Sen. Hatch explained that "[t]he intent of the change is to hold criminally liable those who do not receive or expect to receive money but who receive tangible value," but does not include "enhancement of reputation" or tangential value (such as a job promotion). 143 CONG. REC. S12689, S12690 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch).

Interestingly, the DOJ has taken the position that, even prior to the Act, it could prosecute warez traders based on a theory that bartering constituted financial gain. 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).

352 *See*, *e.g.*, United States v. Slater, 2003 WL 22519692 (7th Cir. 2003); Statement of Facts, United States v. Tresco, No. 02-CR-132-A, at 8 (E.D. Va. 2002).

CONCLUSION

It is tempting to dismiss the No Electronic Theft Act as one of those laws in which the copyright owners got additional economic protectionism[353] but to little consequence. With the small number and relative appropriateness of prosecutions to date, one might conclude that the Act is not a big deal.

Unfortunately, the Act's procedural history provides little comfort.[354] Congress's consideration of the Act does not evidence any understanding about who the Act was trying to regulate, what motivated these individuals, how the Act would shape those motivations, what mechanisms already tried to motivate those individuals, and the efficacy of the alternative mechanisms.[355]

Substantively, the Act fares little better. The Act has not demonstrably reduced piracy, nor should it realistically be expected to. Congress does not really draft laws with an eye toward maximum efficacy[356] and the Act sweeps in more than just reprehensible conduct, making it seem unjust and thus unsupportable.[357] Meanwhile, the Act's ambiguity and overinclusiveness curb legitimate copying, both copying necessary to handle our daily duties and copying that is part of a vibrant social discourse.

While these detrimental impacts have been limited by broad ignorance about the law's scope, the law imposes a social cost to those aware of it, and that cost escalates each time Congress

353 *See* Katz, *supra* note 336, at 45 ("[A]iding such copyright holders with additional funds spent on enforcement of copyright law by government agencies (through criminal proceedings, for example) is merely an additional subsidy for copyright holders with no positive influence on the general welfare . . . .").

354 *See* Tyler, *supra* note 199, at 233 ("In the area of intellectual property . . . people need to believe that the rules established serve reasonable social purposes and are not simply efforts to create profits for special interest groups, such as large corporations.").

355 *Cf.* Douglas N. Husak, *Limitations on Criminalization and the General Part of Criminal Law*, *in* CRIMINAL LAW THEORY: DOCTRINES OF THE GENERAL PART 36 (Stephen Shute & A.P. Simester eds., 2002) (suggesting that no criminal law should be enacted unless the law is better than other alternatives).

356 *See* Stuntz, *supra* note 262, at 508 (suggesting that Congress does not care about the normative implications of new criminal laws it passes); *id.* at 549 ("Crime definition usually carries low political returns; it is hardly a surprise that legislators spend relatively little time on it.").

357 *See* I. Trotter Hardy, *Criminal Copyright Infringment*, 11 WM. & MARY BILL RTS. J. 305 (2002); Tyler, *supra* note 199 (arguing that people comply with laws they believe are moral and legitimate, and thus laws that are discordant with widespread views of morality have little chance of success); *accord* Husak, *supra* note 355, at 43. *See generally* Moohr, *supra* note 259, at 767-74.

noisily demands the punishment of average Americans. As just one of many such exhortations, in March 2003, Rep. Carter said:

> I think that it would be a good idea to go out and actually bust a couple of these college kids. And you know, if you want to see college kids duck and run, you let them read in the paper that somebody got about a 33 month sentence in the Federal penitentiary for downloading copyrighted material . . . .[358]

These types of demands, a perverse desire in Congress to see average Americans suffer the consequences of an unprincipled criminal law, make the Act a big deal.

Meanwhile, Congress is adrift in its efforts to develop a sensible policy about criminalizing copyright infringement.[359] Recent Congressional proposals to expand criminal copyright law and its enforcement[360] reflect a shotgun approach, a desperate attempt to find some way to make Americans change their behavior. But ad hoc proposals to increasingly put average Americans under tighter criminal controls are not the answer. The answer is to provide Americans with laws they can respect because they fairly distinguish between true criminals and the average American. And on that front, Congress has much more work to do.

[358] *Hearing*, *supra* note 280, at 104 (statement of Rep. John R. Carter). *But cf.* 143 CONG. REC. S12689, S12689 (daily ed. Nov. 13, 1997) (statement of Sen. Hatch) (saying that if overzealous prosecutors go after college pranksters, he hoped judges would be lenient).

[359] Lisa Friedman, *Web Pirates Plunder On*, DAILY NEWS OF L.A., June 23, 2003, at N1. *See generally* Stuntz, *supra* note 262.

[360] Piracy Deterrence and Education Act of 2003, H.R. 2517, 108th Cong. (proposing stronger education and enforcement efforts of the law), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2517ih.txt.pdf; Author, Consumer and Computer Owner Protection and Security (ACCOPS) Act of 2003, H.R. 2752, 108th Cong. (proposing, among other things, to criminalize the willful uploading of a single infringing work), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h2752ih.txt.pdf; Artists' Rights and Theft Protection Act of 2003, S.1932, 108th Cong. § 4 (among other provisions, proposing to make the placement of a single copy of a pre-release copyrighted work (such as a pre-release version of a movie) in a P2P file-sharing software's share directory a felony).