January 1994

Combatting Software Piracy: Can Felony Penalties for Copyright Infringement Curtail the Copying of Computer Software?

Greg Short

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation

Available at: http://digitalcommons.law.scu.edu/chtlj/vol10/iss1/7

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
COMBATTING SOFTWARE PIRACY: CAN FELONY PENALTIES FOR COPYRIGHT INFRINGEMENT CURTAIL THE COPYING OF COMPUTER SOFTWARE?

Greg Short

I. INTRODUCTION

By 1990, software piracy in the United States accounted for approximately $2.4 billion in lost income per year for software manufacturers, up from approximately $500 million per year a decade ago. Worldwide, the losses are estimated to have been $10-12 billion in 1990. This dramatic rise in software piracy over the past decade not only created a burgeoning business in pirated software and resulted in dwindling profits for the software industry, but it also prompted renewed efforts by software manufacturers and the federal government to combat the pirating of software. The combination of industry and government efforts culminated in Public Law Number 102-561,

Copyright © 1994 Greg Short.


1. The term "software piracy" has been used to refer to the unauthorized copying and distribution of software programs as well as the unauthorized creation of derivative works based on the software. See Lauren Bruzzone, Comment, Copyright and License Protection for Computer Programs: A Market Oriented Assessment, 11 Pace Law Review 303, 310 n.49 (1991). However, for the purposes of this comment and the recently enacted legislation discussed herein, "software piracy" refers only to the reproduction of software and the subsequent distribution of any copies, not the practice of reverse-engineering or the development of derivative programs.


4. Felonization, supra note 2.

signed into law by President Bush on October 28, 1992.\(^6\) The new legislation, which was the focus of intense lobbying by the Software Publishers Association (SPA),\(^7\) creates felony penalties for software pirates.

This comment first reviews the background of the software piracy problem: analyzing who copies software and why, assessing what is the impact of this pirating on the software industry, and examining past attempts by manufacturers to prevent piracy. Second, it traces the development of the recently enacted legislation. Third, the comment evaluates the reaction to the legislation by software manufacturers and consumers, and further debates the law’s utility as a tool to combat software piracy.

II. SOFTWARE PIRACY

People who copy software can be grouped into three broad categories: organized pirates, individual computer owners/users, and corporate employers/employees. Each category has its own motivation for copying software.\(^8\) Organized pirates copy on a large scale primarily for profit with the software frequently sold through pirate electronic bulletin boards systems (BBSs).\(^9\) Individual computer owners, motivated by a desire to avoid paying for software, generally copy for personal use in the home, school or business from software received from friends or colleagues. Corporate copiers, who some commentators acknowledge are the most unmanageable piracy problem,\(^10\) include individuals in the work-place who copy, with or without management approval, software that may or may not be licensed by the company. Often called “soft-lifting,”\(^11\) employers may condone or ignore employee copying of software, rationalizing it as part of the business or justifying it on the grounds that the company has already

---


\(^7\) Felonization, supra note 2. The SPA is one of the principal trade associations of the personal computer software industry.

\(^8\) For an assessment of the ethics, investment, reputation and detection concerns of these groups and their piracy threat, see generally Daniel T. Brooks, Computer Law Basics (1985).


\(^10\) See, e.g., Amy Cortese, A Felonious Crime: Software Copyright Infringement, InformationWeek, Sept. 14, 1992, at 14, in which Ron Palenski, general counsel for Information Technology Association of America, commented that software piracy is mostly within corporations.

licensed one copy of the software. At other times, employers may have little knowledge about the making of copies, especially if the office computers are not networked or audited.

Organized pirates aside, those in the individual and corporate categories often copy because they do not understand their legal obligations regarding copyrighted software. At other times, those who do understand their obligations copy anyway, either because they believe that there is little chance of being caught, or because they consider it a fringe benefit of their job to make a copy either for their computer at work or at home. For pirates at all levels, the attraction is further enhanced because it is very quick and inexpensive to copy software, requiring only the cost of a blank disk and a few minutes to download the program. If software piracy is inexpensive, easy and difficult to detect, manufacturers, in their drive to make software more readily available, unwittingly contributed to the piracy problem. In the 1970s, most software was custom-made for use on mainframes and marketed through direct sales; the manufacturer maintained a close relationship with the licensee, provided updates to the software when required, and experienced little demand for copies of the specialized software. In contrast, by the 1980s, as corporate and personal ownership and use of microcomputers increased dramatically, generic software for the PC or workstation was available at retail or wholesale outlets; few buyers or users had any relationship with the manufacturer, the software needed little or no support, and there was a wide demand for copies of the programs.

One result of this dramatic change in the computing environment has been the exponential growth in software piracy. The SPA estimates that one out of every five PC software programs is now an illegal copy. Software piracy of this scale translates into a reduction in

13. Mark, supra note 3, at 44.
14. Id.
15. See, e.g., Bruzzone, supra note 1, at 311.
17. For a description of the bifurcation of the computer program market, see Bruzzone, supra note 1, at 307-09.
18. Id. at 308-09.
19. Rob Kelly, Corporate Pirates Walk the Plank, INFORMATIONWEEK, Nov. 9, 1992, at 30; see also Patrick G. Marshall, Copying Computer Programs Puts Byte on Software Firms, MINNEAPOLIS STAR TRIB., July 1, 1993, at 16E.

Senator Biden, in his report to the Senate from the Committee on the Judiciary that debated the proposed legislation, contended that studies indicated that "for every authorized copy of a software program in circulation, there is an illegal copy also in circulation." See S. Rep. No. 268, 102d Cong., 2d Sess. 2 (1992).
profits for manufacturers, a reduction in money available for investment and research in new products, and, consequently, more expensive software for the consumer.\textsuperscript{20} In response to this syphoning of their profits, manufacturers have responded with a variety of innovative methods to prevent the pirating of software.

III. EFFORTS TO CURTAIL PIRACY

A. License Protection

Most software in the United States is licensed by the manufacturer or distributor rather than sold out right to the consumer.\textsuperscript{21} Licensing arrangements include formal contracts between manufacturers and licensees, "shrink-wrap" licenses that come with software purchased retail or wholesale, and registration fees for the use of "shareware" downloaded from BBSs. Each license usually refers to a single copy or multiple copies of the software and the license is generally for the use of the copy or copies by the licensee only. By licensing copies of the software, the manufacturer seeks to avoid the "first sale doctrine" of the Copyright Act\textsuperscript{22} and to prevent the licensee from transferring or lending the software to others who may duplicate it and thereby reduce the manufacturer's potential revenue.\textsuperscript{23}

However, it is not an infringement of copyright for the licensee of a software program to copy or adapt that software for either an essential step in using the program or for archival purposes.\textsuperscript{24} Most manufacturers agree that the making of an archival copy by the licensee for disaster recovery purposes does not present a piracy problem, and manufacturers generally give the licensee permission to make ar-

\textsuperscript{20} Mark, supra note 3, at 43-44.

\textsuperscript{21} David A. Rice, Licensing the Use of Computer Program Copies and the Copyright Act First Sale Doctrine, 30 JURIMETRICS J. L. SCI. & TECH. 157, 157 (1990). Note that most licensed software is object code rather than source code. Technically speaking, object code is the machine-readable code that is compiled from the human-readable source code in which the software is developed; more simply, the software developer writes the software program in a programming language that is then run through a compiler to convert the program into the binary code that can be read by the computer. See Bruzzone, supra note 1, at 315. By providing only the object code to the licensee, the manufacturer ensures that the user cannot decipher the software unless it is converted back or, essentially, reverse engineered. See James A. Eidelman & Corol R. Shepherd, Living Among Pirates: Practical Strategies to Protect Computer Software, 65 MICH. B.J. 284, 284-85 (1986).

\textsuperscript{22} 17 U.S.C.S. § 109(a) (1993). This doctrine gives to the owner of a copy of a copyrighted work the right to transfer or dispose of that copy. However, under § 109(c), those rights do not extend to the lease of a copyrighted work. For a broad discussion of the first sale doctrine, see generally Rice, supra note 21.

\textsuperscript{23} David L. Hayes, Shrink-wrap License Agreements: New Light on a Vexing Problem, 7 COMPUTER L. ASSOC. BULL., No. 2 at 5, 5-6 (1992).

chival copies or provide the licensee with extra copies for such purposes.\textsuperscript{25} On the other hand, adapting the software usually requires the source code, but manufacturers rarely distribute this to a licensee.\textsuperscript{26} Alternatively, a licensee can adapt the software through reverse-engineering, but most licensors specifically preclude the licensees the right to reverse-engineer.\textsuperscript{27}

For example, the shrink-wrap license has traditionally been used to protect the manufacturer's interest and to inform the buyer of the limits on the copying of the software sold through retail or wholesale outlets.\textsuperscript{28} The software package exposes the license and a notice informing the buyer that by opening the package the buyer agrees to the terms of the license.\textsuperscript{29} Despite of the doubts raised about the enforceability of shrink-wrap licenses,\textsuperscript{30} manufacturers still use them because they remain an accepted industry standard. Furthermore, in an attempt to counter the argument by consumers that they did not see the shrink-wrap license and did not agree to its terms, some manufacturers reiterate the buyer's acceptance of the license agreement at the logon screen.\textsuperscript{31}

Thus, the main advantages to licensing software lie in the manufacturer's ability to retain title to the software and to restrict the privileges of the licensee.\textsuperscript{32} In addition, licensing gives the manufacturer two potential causes of action if a licensee pirates the software: copyright infringement and/or breach of contract.\textsuperscript{33} However, past attempts to enforce these civil contractual and/or copyright rights have

\textsuperscript{25} The law does not explicitly require that the user be permitted to make the archival copies or that the user should look to the manufacturer as the source of archival copies. See Sterne & Kessler, supra note 12, at 161-62.

\textsuperscript{26} See Eidelman & Shepherd supra note 21, at 285.

\textsuperscript{27} Rice, supra note 21, at 157-58. Note that making a copy of a licensed program for the purposes of reverse engineering is considered fair use; see, e.g., Sega Enter. Ltd. v. Accolade, Inc., 977 F.2d 1510, 24 U.S.P.Q.2d (BNA) 1561, 1578 (9th Cir. 1992); Atari Games Corp. v. Nintendo of Am., Inc., 975 F.2d 832, 24 U.S.P.Q.2d 1015, 1023 (Fed. Cir. 1992).

\textsuperscript{28} Sterne & Kessler, supra note 12, at 165-66.

\textsuperscript{29} The shrink-wrap package may also contain a registration card for the licensee to return to the manufacturer acknowledging agreement to the license terms, but few of these are returned. Id. at 164-65. For a sample of a shrink-wrap license, see, Eidelman & Shepherd, supra note 21, at 291.

\textsuperscript{30} For an analysis of the Vault Corp. v. Quaid Software Ltd., 847 F.2d 255 (5th Cir. 1988), and Step-Saver Data Sys., Inc. v. Wyse Tech., No. 88-7961, 1989 U.S. Dist. LEXIS 11320 (E.D. Penn. Sept. 26, 1989), cases, and their impact upon the protection of computer software, see Hayes, supra note 23, at 6-10.

\textsuperscript{31} Eidelman & Shepherd, supra note 21, at 288.

\textsuperscript{32} Id. at 287.

\textsuperscript{33} Id.
not always been successful in combating software piracy. Indeed, the image of software protection through licensing has become a fragmented one consisting of overlapping theories of intellectual property law and contract law, and the recent lobbying for reforms to the Copyright Act was prompted by software manufacturers convinced that existing protection was insufficient to prevent piracy.

B. Hardware and Software Protection

Originally, many software manufacturers looked to hardware protection as a barrier to duplication of their software, such as copy-protected disks or devices attached to the computer which prevented copying of the disk. The Association of Data Processing Service Organizations (ADAPSO) introduced a “lock, ring and key” approach in the early 1980s, but this was soon abandoned by most manufacturers because it was too costly to implement and maintain.

Hardware protection also threatened consumer good will. Many customers were offended that they were considered potential pirates, while others complained about delays when forced to contact the manufacturer for a replacement disk or to make an archival copy of the software. In addition, hardware protection devices quickly spawned innovators who decoded or bypassed the various locks. Instead, a modern approach is to employ software protection, such as licensee IDs embedded in the software that display every time the program is run. These have the added advantage of assisting manufacturers to trace the source of pirated copies.

C. Distribution Arrangements

Other efforts to curtail software piracy have focused on the packaging of the software. These efforts include the printing of warnings of the penalties for infringement of the license and copyright, and the

34. For example, recent court decisions have cast doubt about the validity and enforceability of shrink-wrap licenses (see Hayes supra note 23, at 6-10) and created concern about what software features are copyrightable. For a discussion of copyright protection of computer software, see generally Evan Finkel, Copyright Protection for Computer Software in the Nineties, 7 SANTA CLARA COMPUTER & HIGH TECH. LJ. 201 (1991); for a discussion of the copyrightability of the “look and feel” of software in the U.S., see generally Daniel A.D. Hunter, Protecting the Look and Feel of Computer Software In the United States and Australia, 7 SANTA CLARA COMPUTER & HIGH TECH. LJ. 95 (1991).
35. Mark, supra note 3, at 44-45.
36. Id. at 45.
37. Id.
38. Id.
40. Id.
insertion of a hologram that identifies the software as an original manufacturer copy. Nevertheless, forged holograms have been found inserted into packages containing pirated copies. A more standard approach to curtailing software piracy through distribution arrangements has been for manufacturers to deny support and upgrade facilities to users of software unless the user can point to a license agreement, produce a registration card from a shrink-wrap purchase, or agree to pay a license fee.

D. Software Copying Policies

Educating consumers about the potential liability for copying software was a major thrust of ADAPSO's anti-pirate strategy in the 1980s. Companies sought to implement internal corporate policies on legitimate software copying in the work place, thereby hoping to reduce or eliminate unauthorized copying at the office and to minimize the corporations' exposure to liability for their employees' actions. ADAPSO even drafted a five point software copying policy entitled "Thou Shall Not Dupe" and distributed the proposal throughout the industry.

While such a policy may not completely insulate a corporate employer from liability for copying done by its employees, under the doctrine of respondeat superior, it has been argued that corporate directors and counsels are under a duty to adopt such policies. In contrast, one reviewer of such policies suggests that the onus for limiting piracy in the software market lies with improved publisher services

41. Mark Clifford, Pirate's Lair: Taiwan's Software Copiers Perfect the Hologram, FAR EASTERN ECON. REV., Oct. 8, 1992, at 79.
42. A novel approach has been pursued by McAfee & Associates, a Santa Clara, California, firm, whose motto has been "Steal our Software." McAfee distributes its software, mainly anti-viral programs, as shareware on BBSs, and includes a requirement that corporations using the software must license it. However, McAfee also relies on individuals to download the programs, and share them with their colleagues at the office, who will in turn make more copies of the program, without licensing the software. McAfee then contacts the company, informs them that they have unlicensed copies of its software and requests a license fee for the use of the software in order for the company to avoid any infringement liability. At other times, an audit by a company of its network will reveal unlicensed copies of the programs, and the company will contact McAfee for a license. In other words, McAfee relies on user honesty and/or the fear of litigation to secure licenses from those corporations who have pirated, perhaps unwittingly, its software. See Laurie D. Weeks, McAfee, Maker of Anti-viral Software, Plans Offering to Build on Its Success, WALL ST. J., Sept. 21, 1992, at A5D.
43. Sterne & Kessler, supra note 12, at 170-01.
44. Id. at 171-73.
45. Cangialosi, supra note 9, at 291.
46. Sterne & Kessler, supra note 12, at 171-72.
and better licensing agreements, rather than on software copying policies, because “corporate users would be more willing to respect the requirement that each copy of a program be legitimately purchased if the manufacturers tailor their products and services to the particular needs of the corporations.”

IV. INEFFECTIVENESS OF ANTI-PIRACY EFFORTS

By the late 1980s, the perception was that these contractual, technical and educational efforts were insufficient to stem the tide of software piracy. Despite preliminary concerns of expense and potential customer alienation, the software manufacturers, headed by ADAPSO, SPA and the Business Software Association (BSA), began to utilize litigation more readily as a means to combat piracy.

ADAPSO’s first suits for software copying were filed in the mid-1980s and targeted high profile corporations whose employees were known to be copying software. While the goal was to expose and publicize the copying problem, most suits were settled. The SPA’s first suit was filed in 1988. Since that time the SPA has organized a group of attorneys nationwide who by 1992 had filed over 300 copyright infringement lawsuits for software copying, with the cost of the enforcement program supported by contributions from SPA’s membership.

Sometime referred to as the “Software Police,” the SPA’s approach is to identify suspect companies and obtain court orders allowing the them to search the offices and seize any non-licensed copies of software. Tips about companies with pirated software invariably come from disgruntled or former employees calling the SPA’s hotline, or from unsuspecting users of pirated software calling the manufacturer’s customer support number. Prior to the recent

49. Id. at 49.
50. Sterne & Kessler, supra note 12, at 169.
51. Id.
53. Software Police, supra note 11.
54. Kostal, supra note 52. The SPA has over 1000 members, including IBM, Apple and Microsoft.
55. Software Police, supra note 11.
56. Kostal, supra note 52.
57. Software Police, supra note 11. The SPA gets approximately 100 calls a week on its hotline, while the BSA gets over 250 calls per day on numerous international hotlines. See Karen Kaplan, Industry Groups Unleash “Software Cops” to Fight Piracy, ARIZONA REP., Aug. 16, 1993, at B1.
58. Sterne & Kessler, supra note 12, at 169.
amendments to the Copyright Act, the SPA could force companies to destroy all illegal copies and collect fines for each copyright violation. However, their strategy was to settle with a company once it purchased legitimate copies of the software.

BSA, founded in 1988, is an association of some of the largest personal computer software publishers in the United States, including Digital Research, Lotus Development Corporation, Microsoft Corporation and Word Perfect Corporation. BSA has targeted international pirates in a strategy similar to SPA, but it focuses on bringing criminal charges and putting pressure on local legislators and enforcement officials. For example, in April 1990, BSA brought 20 suits against software pirates in Spain, but later that year announced an amnesty period to allow those companies to request a license and an out-of-court settlement. About half of BSA’s suits are against corporations, and although BSA has yet to raid any corporations in the United States, BSA has begun targeting BBSs based in the United States and abroad that distribute pirated software.

This movement away from prevention and education toward the pursuit of pirates in the courts reflected both the exasperation of software manufacturers with traditional techniques for curtailling software piracy and a commitment to more strong-arm tactics. At the same time, representatives of the software manufacturers lobbied Congress for stiffer laws to deal with pirates by arguing that existing penalties and remedies for copyright infringement were insufficient to deter software pirates, that federal prosecutors and law enforcement agencies were reluctant to pursue cases that only resulted in misdemeanor convictions, and that discovery procedures for civil complaints were often inadequate to garner sufficient evidence to

59. See, e.g., Kaplan, supra note 57.
60. See, e.g., Kostal, supra note 52.
62. Id.
63. Kelly, supra note 19.
64. Id.
66. In response, many corporations who have been targets of the manufacturers pursuit have attacked these operations as witch hunts. Kaplan, supra note 57.
67. See, e.g., Felonization, supra note 2.
68. Id.; see also S. Rep. No. 268, supra note 19, at 2 (comparing the current disinclination of prosecutors to prosecute software piracy cases with a similar situation that existed with sound recordings before Congress changed the copyright laws to help deter piracy in that industry).
successfully sue the pirates.\textsuperscript{69} This lobby for stricter penalties was represented in Congress by Senator Orrin Hatch (Republican, Utah) and Representative William J. Hughes (Democrat, New Jersey).

\textbf{V. DEVELOPMENT OF FELONY LEGISLATION}

\textbf{A. Proposed Law}

Under section 506(a) of the Copyright Act, criminal infringement of a copyright is punishable according to the provisions of section 2319 of Title 18.\textsuperscript{70} Section 2319 originally provided felony penalties of up to 5 years in prison and/or fines of up to $250,000 for infringing copyrighted motion pictures, sound recordings or other audiovisual works (depending upon the number of copies made of each type of copyrighted work), but infringement of other copyrighted works was only a misdemeanor punishable by up to a year in prison and/or a $25,000 fine.\textsuperscript{71} In April 1991, Senator Hatch introduced Senate Bill 893 (S. 893) to add computer programs to the list of copyrighted works that can trigger criminal penalties for copyright infringement under § 2319.\textsuperscript{72}

\textbf{B. Legislative History}

The Senate Judiciary Committee referred the bill to its Subcommittee on Patents, Copyrights and Trademarks, which approved the bill for consideration by the full Committee on July 25, 1991.\textsuperscript{73} The Judiciary Committee unanimously approved S. 893 on August 1, 1991.\textsuperscript{74} The full Senate passed the bill on June 4, 1992,\textsuperscript{75} and the bill then moved to the House.

\textsuperscript{69} House Panel Considers Stricter Criminal Penalties for Software Infringement, Pat. Trademark \& Copyright L. Daily (BNA) (Aug. 28, 1992) [hereinafter House Considers Penalties].

\textsuperscript{70} "Criminal Infringement. Any person who infringes a copyright willfully and for purposes of commercial advantage or private financial gain shall be punished as provided in section 2319 of title 18." 17 U.S.C. § 506(a) (1988).


\textsuperscript{72} S. 893, 102d Cong., 2d Sess. (1992). The bill's purpose was to "amend Title 18 of the United States Code to increase the penalties for violations of copyrights in computer software. Under current law, piracy of computer software is a misdemeanor offense. This bill will elevate the offense to a felony." S. Rep. No. 268, supra note 19, at 2. Note that the bill's provisions were also included as part of the omnibus crime package. H.R. Rep. No. 997, 102d Cong., 2d Sess. 2 (1992), reprinted in 1992 U.S.C.C.A.N. 3569, 3570.

\textsuperscript{73} S. Rep. No. 268, supra note 19.


\textsuperscript{75} House Passes Bill on Criminal Penalties for Copyright Infringement, 44 Pat. Trademark \& Copyright J. (BNA) No. 1100, at 601 (Oct. 8, 1992) [hereinafter House Passes Bill].
The House Judiciary Committee referred the bill to its Subcommittee on Intellectual Property and Judicial Administration on June 11, 1992, which held hearings on the bill on August 12, 1992. On September 10, 1992, the Subcommittee approved a modified version of the bill that extended the proposed felony provisions for software infringement to infringement of all types of copyrighted works and standardized the number and value of infringing copies of the various works required for criminal liability.

This amended version was passed by the full House on October 3, 1992, and returned to the Senate for approval. On October 8, 1992, the Senate unanimously agreed to the amendments, and the bill was sent to the President. President Bush signed the bill into law on October 28, 1992.

C. Amended Law

Under the newly adopted legislation, a person who "willfully and for purposes of commercial advantage or financial gain" reproduces or distributes within a 180-day period at least 10 copies of one or more copyrighted software programs that have a retail value of at least $2,500, faces imprisonment of up to five years and a fine of $250,000 for a first offense, and up to 10 years imprisonment for a second offense.

VI. LEGISLATIVE DEBATES

In his speech to the Senate advocating the adoption of the House’s amended version of the bill, Senator Hatch described the proposed law as "designed to help the computer software industry combat the growing problems of large-scale commercial piracy." However, despite the contentions by the legislation’s drafters and supporters that only organized pirates were the target of the new law, other commentators continue to argue that the majority of software piracy occurs in the corporate setting. In fact, as described earlier, it is the corporations who are frequently the target of the software manufacturer efforts to combat software piracy. This contradiction raises the question of whether the law is simply focused on derailing large-scale software

78. House Passes Bill, supra note 75.
79. Id.
82. Hatch, supra note 2, at S17,958.
83. Cortese, supra note 10.
piracy, or whether it can be used to target corporate pirates or even individual pirates.

Some early comments about the new law's potential reach raised concerns about whether the law could be used against companies with multiple unlicensed copies of a program,84 companies employing reverse-engineering techniques,85 individuals making copies for their friends,86 system operators of BBSs that provide pirate copies, or, possibly, even users of those BBSs.87 In evaluating these concerns, the Congressional committees focused on two main issues that are necessary to trigger criminal penalties for software piracy: 1) the threshold requirements for the number and value of copies, and 2) the mens rea requirement.

A. Mens Rea Requirement

Some of the concerns raised by the new felony legislation stemmed from the lack of definition for the terms “willful,” “commercial advantage,” and “private financial gain” when determining criminal copyright infringement. Although section 506(a) has been part of the Copyright Act since 1976 and “willful” has been in the copyright law since 1897, the term has never been defined in the Act.88 This inadequacy of definition was seen by both opponents and proponents of the new legislation as making it possible, at least theoretically, for criminal liability to be imposed on corporate or individual copiers of software in addition to organized pirates.89

In an attempt to flush out the mens rea requirement for the crime, Senator Hatch, in his speech to the Senate advocating adoption of the new legislation, stressed that “unless done for the express purpose of obtaining commercial advantage or private financial gain, copying of copyrighted material is not a crime” under the new law.90 Although this comment did little more than restate the requirements of the law, Representative Brooks, in his speech to the House on October 3, 1992, before the bill went to the House vote, stated:

85. House Considers Penalties, supra note 69.
86. Id.
87. Messmer, supra note 65. Ilene Rosenthal, director of litigation for the SPA, hinted that the SPA’s approach of targeting only BBS operators might change to include users. See Marshall, supra note 19.
89. House Considers Penalties, supra note 69; Willet, supra note 84; O’Connor, supra note 84.
90. Hatch, supra note 2, at S17,959.
The requirement of a mens rea for criminal copyright infringement serves the important purpose of drawing a sharp distinction with civil copyright infringement... For an infringement to be deemed a criminal violation... a specific mens rea must be proved. Even if civil liability has been established, without the requisite mens rea it does not matter how many unauthorized copies... have been made or distributed: No criminal violation has occurred.91

Still, despite criticism about the lack of definition, the standards required to prove criminal infringement of copyright have been well articulated by the courts.92 Generally, as applies to § 506(a), "willful" infringement requires that the act be voluntary, with knowledge that it was prohibited by law, and with the intent of violating the law.93 Furthermore, as emphasized, "the copying must be undertaken to make money, and even incidental financial benefits" are insufficient where the "achievement of those benefits were not the motivation behind the copying."94 In other words, infringements must be undertaken for profit, although it is not necessary for the infringer to receive actual commercial advantage or private financial gain.95 Therefore, concern that innocent copying of software could be criminally prosecuted is unnecessary because the government can only bring a criminal action for willful infringement.96

Nonetheless, in an effort to calm concern about distinguishing criminal from civil infringement, the House Subcommittee on Intellectual Property and Judicial Administration attempted to add a definition of "willful" infringement to S. 893, but this was rejected by the House Judiciary Committee.97 While applauding this move, which placed continued reliance on the courts’ interpretation of the willful element of the offense, Senator Hatch added that he was sure Congress would be willing to define the term better in the future—perhaps hinting that Congress would be prepared to amend the law in order to define its reach more clearly if the current terminology proves unmanageable in the courts.98

92. See generally, 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT, § 15.01 (1993).
93. Id. § 15.01, at 15-8 & n.13.
94. Hatch, supra note 2 at S17,959.
95. Nimmer, supra note 92, § 15.01, at 15-8. See also United States v. Moore, 604 F.2d 1228, 1235 (9th Cir. 1979).
97. Hatch, supra note 2, at S17,959.
98. Id.
99. Another example of the concern over the language of the bill came during the hearings before the House Subcommittee when Rep. Hughes asked whether specific language excluding reverse engineering should be added to the bill. Industry representatives and attorneys argued
B. **Threshold Requirements**

Another main cause for concern lies in the low threshold requirement of "10 copies" with a "retail value" of "$2,500" that can trigger criminal liability. The legislative history indicates that the "retail value" is to be determined by the retail price of the software at its time of release, or, for a non-retail program, by the harm to the copyright holder (assessed as the greater of the replacement cost or the true cost of the production of the software).\(^{100}\) In clarifying this calculation, Senator Hatch noted that these figures are to be determined by the value of the software in the legitimate retail market, not in the "thieves' criminal market."\(^{101}\) However, although the legislation requires "at least 10 copies" of one or more copyrighted works, Senator Hatch pointed out that "criminal liability attaches if fewer than 10 works are copied if the retail value of the works exceeds $2,500," but imprisonment in such a case cannot exceed one year.\(^{102}\)

Thus, it will be important to see how the courts evaluate the sufficiency of the evidence required to prove criminal liability once the required intent has been shown. For example, with business or personal software programs often costing more than $250, it is possible that a half-dozen or more copies of a program could bring the copier under the reach of the felony legislation, if the mens rea requirement is met. However, the courts have been careful when finding criminal liability for pirating other copyright works. In *United States v. Cross*,\(^{103}\) the court found willful intent to infringe for private financial gain, but found insufficient evidence of the exact number of copies of the infringing videocassettes then required to trigger criminal liability. The felony convictions were vacated.

The suggestion that fewer than 10 copies are required to trigger felony penalties could be interpreted as an attempt by Congress to avoid the rejection of an action by the courts, similar to that in *Cross*, when all the requirements for felony software infringement have been met except the exact threshold number of copies. Nonetheless, Representative Brooks took care to point out that the threshold requirements were not intended to produce a broad net within which to catch all types of copiers:

---

\(^{100}\) See *Hatch*, supra note 2, at S17,958.

\(^{101}\) Id. at S17,959.

\(^{102}\) Id. (emphasis added).

\(^{103}\) 816 F.2d 297, 301 (7th Cir. 1987).
First, it excludes from felony prosecution children making copies for friends as well as other incidental copying of copyrighted works having a relatively low value. Second, the requirements of reproducing or distributing at least 10 copies within a 180 day period removes the possibility that the increased penalties can be used as a tool of harassment in business disputes over reverse engineering.104

VII. TARGETING THE PIRATES

A. Commercial Pirates

According to the SPA, "the new law passed by Congress . . . targets professional software pirates who make many copies of software and resell them at low prices; illegal bulletin board operators who distribute pirated software; and PC dealers who offer 'free' but illegal software to hardware purchasers."105 This claim is supported by recent activity by SPA, BSA and federal criminal agencies. In what was considered to be the first action under the new legislation, the Secret Service in December 1992, raided the dormitory rooms of two Texas Tech University students who were alleged to have traded pirated software on the Internet computer network using the University's computers.106 In another investigation in Texas, the Federal Bureau of Investigation was working with the SPA to target computer stores in Houston that gave or sold pirated software to buyers of hardware.107 Meanwhile, the BSA, with the support of federal law enforcement agencies, was actively pursuing BBSs that sold pirated software.108

Perhaps the most publicized event was the announcement of the first criminal indictments under the new law in June and July 1993.109 In one case, the federal grand jury in San Francisco charged a company and two executives with copyright infringement for distributing some 20,000 copies of Microsoft software, as well as with laundering over $500,000 in illicit profits.110 In another case, a computer hard-
ware company and two executives were indicted after selling thousands of copies of Microsoft software to federal and state agents.\textsuperscript{111}

These activities suggest that not only is the new law operating as intended, but also that law enforcement agencies are more willing to pursue copyright infringement. This latter fact was endorsed by the new United States Attorney for the Northern District of California, Michael Yamaguchi, who said that he wants to bring more software piracy and copyright infringement suits.\textsuperscript{112} On the other hand, the recent indictments handed down by his office were criticized as being gift-wrapped by Microsoft investigators and, as such, reflect a worrisome hand-in-glove relationship between Microsoft and the District Attorney's office.\textsuperscript{113} Ironically, Microsoft complained that the government was not tough enough on the pirates, leaving behind too many machines for duplicating software when they raided the premises.\textsuperscript{114}

\textbf{B. Corporations}

Despite the Congressional protestations to the contrary, it is too early to determine whether large-scale pirates will be the only targets of the new law. In contrast to SPA's claims about the legislation's target, the SPA has overwhelmingly targeted corporations in its civil actions against software pirates—approximately 95\% of its cases last year.\textsuperscript{115} Indeed, the SPA's typical investigation centers on a company with 20 to 30 PCs, but the SPA has sued companies with as few as five PCs.\textsuperscript{116}

This focus occurs because the SPA relies in part on calls to its hotline for information on corporate pirates and recently there have been few reports on large companies, a trend the SPA attributes to most corporations having instituted software copying policies or utilized software managers to control the software on the network.\textsuperscript{117} For those corporations that have not instituted such policies, the possibility of criminal liability for software copying is very real. Generally, a corporation is liable for the criminal conduct of its agents, including

\begin{itemize}
\item \textsuperscript{111} Jim Doyle & Don Clark, \textit{Firms Pirated Software, U.S. Says}, S.F. CHRON., July 8, 1993, at A13.
\item \textsuperscript{113} Howard Mintz, \textit{Too Close For Comfort}, RECORDER, Aug. 9, 1993, at 1.
\item \textsuperscript{114} \textit{Id}.
\item \textsuperscript{115} \textit{Anti-Piracy Hotline, supra note 105}.
\item \textsuperscript{116} \textit{Hard Line on Software Piracy, CHICAGO TRIB.}, Apr. 25, 1993, at E11.
\item \textsuperscript{117} \textit{Id}.
\end{itemize}
officers and employees, committed in the scope of their employment and on behalf of the corporation.\textsuperscript{118}

For example, would the test for criminal infringement be met if a corporation's officers, for the purpose of avoiding further expenses in the coming quarter, condoned its employees making a dozen copies of a $300 licensed software program, of which only 2 are permissible for archival or operative purposes? Arguably, the corporation has reproduced 10 illegal copies having a retail value of $3,000 within 90 days, and acted knowingly in violation of its license agreement with the intent to profit from the act. Under Senator Hatch's reading of the new law, perhaps even 9 illegal copies worth only $2,700 would be sufficient.

The legislative history of the new law provides no clear direction for such a scenario because, surprisingly, the issue of \textit{respondeat superior} was not raised at the committee hearings.\textsuperscript{119} However, it is not unreasonable to assume that the law could be used by the software manufacturers to threaten corporations whose possession of illegal copies, both in actual number and retail value, are near or above the threshold levels, even if litigation is not ultimately pursued. Indeed, considering the success of software manufacturers in civil actions for software piracy,\textsuperscript{120} corporations would do well to heed the SPA's attempts to help companies stay within the new law by offering them free network audit kits, software management programs and videos explaining copyright law.\textsuperscript{121}

C. Individuals

In presenting the proposed legislation for final approval before the senate, Senator Hatch stated that "this criminal statute is not designed to reach instances of permissible, private home copying,"\textsuperscript{122} but he did not say what such copying entailed or whether the law could reach instances of impermissible home copying. For example, if an individual makes 10 copies of a $300 program and sells them to his friends, it is unclear whether this activity would pass the test for criminal infringement. While observers consider that any incidental

\begin{flushleft}
\textsuperscript{119} The legislative history did make it clear, however, that the law would not encompass legitimate commercial disputes over software copying. See \textit{S. Rep. No. 268}, supra note 19, at 3.
\textsuperscript{120} The SPA levied $3.9 Million in fines and penalties in 1992. \textit{Anti-Piracy Hotline}, \textit{supra} note 105.
\textsuperscript{121} \textit{Hard Line on Software Piracy}, \textit{supra} note 116.
\textsuperscript{122} Hatch, \textit{supra} note 2, at S17,958.
\end{flushleft}
activity is unlikely to be considered felonious piracy, the potential reach of the law does not meld with the claim that the law is only for large-scale pirates.

Although prosecution of individual pirates would not seem profitable for software manufacturers, the SPA is addressing the individual pirate issue. In an attempt to raise awareness of the law in younger people, the SPA has produced a rap video entitled “Don’t Copy That Floppy” for distribution to schools around the country.

VIII. CONCLUSION

Software manufacturers are now armed with both civil and criminal legislation and are voicing an aggressive attitude toward software pirates of all levels, particularly large-scale pirates. Although the reach and effectiveness of the new felony legislation for combatting software piracy will only become clear as pirates at any and every level are prosecuted, the law’s impact maybe felt more quickly than expected. The SPA reported on the eve of the legislation’s passage that losses due to software piracy had dropped by half since 1990 to $1.2 billion in 1991, a trend that may be attributed in part to the publicity surrounding the development of the felony legislation.

Despite this success and the recent activity under the new law directed at large-scale pirates, software copying within corporations remains, arguably, the most prolific and unmanageable piracy problem, but corporations are not, ostensibly, a target of the new felony legislation. Therefore, the law is likely to be only partially successful at combatting software piracy unless manufacturers can either convince the courts that the new law reaches into the corporate environment, or flex enough political muscle to ensure future amendments to the copyright law that give a clear mandate for felony penalties against corporate pirates.

123. House Considers Penalties, supra note 69.
125. Kelly, supra, note 19. The reduction in software piracy appears to have been short-lived. In 1992, worldwide losses to U.S. companies from illegally copied software were estimated at $11 billion, of which $1.9 billion was lost in the U.S. Software Firms Lost $11 Billion Due to Illegal Copying, Group Says, Pat. Trademark & Copyright L. Daily (BNA) (June 3, 1993).