Hastings Communications and Entertainment Law Journal

Volume 16 | Number 4 Article 6

1-1-1994

Federal Criminal Remedies for the Theft of Intellectual Property

Kent Walker

Federal Criminal Remedies for the Theft of Intellectual Property

by
KENT WALKER*

Table of Contents

* Kent Walker is an Assistant United States Attorney in San Francisco specializing in the prosecution of high-technology crime. The opinions in this article are his own and do not necessarily represent the positions of the United States Department of Justice or the United States Attorney's Office.

I
Introduction

As we concentrate more and more of the value of our economy into accessible forms of information, we must worry more and more about the dark side of the Information Revolution — theft and abuse of information. The United States has long recognized and tried to protect the value of commodified information (intellectual property), through patents, copyrights, trademarks, and trade secret protection. Traditionally, however, society has relied upon civil remedies to vindicate these interests. Today, a sea-change in public opinion gradually is persuading policy-makers that the theft of *intellectual* property can be as serious as the theft of *tangible* property in an Information Age economy.

II
New Criminal Laws & Penalties

In 1976, Congress made it a misdemeanor to "infringe[ ] a copyright willfully and for purposes of commercial advantage or private financial gain."[1] In 1982, after lobbying by the motion picture and recording industry, Congress enacted legislation making large-scale commercial infringement of movies or records a felony, punishable by up to five years in prison and a $250,000 fine.[2] Most recently, in 1992, Congress made commercial infringement of a copyright involving ten or more copies collectively worth more than $2,500 a felony.[3] While the 1992 amendment initially was designed to deal with the growing problem of large-scale commercial infringement of copyrighted computer software, it was later broadened to cover all types of copyrighted works subject to such infringement.[4]

On a related front, in 1984 Congress made it a felony to traffic in goods or services using a counterfeit trademark.[5] Again, the possible penalties are severe: five years in prison and fines of up to $250,000

1. Copyright Act of 1976, Pub. L. No. 94-553, § 101, 90 Stat. 2541, 2586 (1976) (codified at 17 U.S.C. § 506(a) (1988)).

2. Piracy and Counterfeiting Amendments Act of 1982, Pub. L. No. 97-180, 96 Stat. 91, 92 (1982) (codified at 18 U.S.C. § 2319(b) (Supp. IV 1992)).

3. Act of Oct. 28, 1992, Pub. L. No. 102-561, 106 Stat. 4233 (1992) (codified as amended at 18 U.S.C. § 2319(b) (Supp. IV 1992)).

4. 138 CONG. REC. 7580-81 (June 4, 1992); 138 CONG. REC. H11, 129-30 (Oct. 3, 1992); S. REP. No. 268, 102d Cong., 2d Sess. 2-3 (1992); H.R. REP. No. 997, 102d Cong., 2d Sess. 3572 (1992) *reprinted in* 1992 U.S.C.C.A.N. 3569, 3569-70.

5. Trademark Counterfeiting Act of 1984, Pub. L. No. 98-473, § 1502(a), 98 Stat. 1837, 2178 (codified in 18 U.S.C. § 2320 (1988)).

for individuals and up to $1,000,000 for corporations.[6] Even higher fines are available, up to twice the gross gain to the defendant or twice the gross loss to the victim.[7] In addition to fines and incarceration, both copyright and trademark laws provide for the destruction of the infringing items.[8]

Other federal statutes that impact this area include those prohibiting wire fraud and mail fraud[9] and those prohibiting interstate transportation of stolen property.[10] While federal courts have been reluctant to regard "information" as stolen "property" for purposes of the statute dealing with interstate transportation, recent cases suggest that the issue is still very much open.[11]

Finally, because many counterfeit articles are manufactured abroad and imported into the United States, it is important to recognize that it is a felony to import, receive, or transport goods "knowing the same to have been imported or brought into the United States contrary to law."[12] Commercial importation of unauthorized copies of copyrighted works constitutes an act of copyright infringement and violates the law.[13]

III
New Federal Sentencing Guidelines for High-Technology Crime

Looking at statutory prohibitions and maximum penalties alone can be misleading when ascertaining whether the software pirates and similar infringers will receive serious sentences. In the past, judges have treated white-collar offenders leniently, often letting them off with probation and a warning.[14] The United States Sentencing Guidelines ("Guidelines") promulgated by the United States Sentencing Commission have made a point of ensuring short but certain terms of

6. 18 U.S.C. § 2320(a) (1988).
7. 18 U.S.C. § 3571(d) (1988).
8. 17 U.S.C. § 506(b) (1988); 18 U.S.C. § 2320(b) (1988).
9. 18 U.S.C. §§ 1341, 1343 (Supp. IV 1992).
10. 18 U.S.C. § 2314 (1988 & Supp. IV 1992).
11. *See* United States v. Brown, 925 F.2d 1301, 1308-09 (10th Cir. 1991) (interstate transfer of stolen computer code not covered by 18 U.S.C. § 2314); *but see* United States v. Riggs, 739 F. Supp. 414, 418-23 (N.D. Ill. 1990) (interstate electronic transfer of stolen computer data covered by § 2314). The United States Supreme Court has recognized confidential corporate information as "property" for purposes of mail and wire fraud prosecution. Carpenter v. United States, 484 U.S. 19, 25-26 (1987).
12. 18 U.S.C. § 545 (1988 & Supp. IV 1992).
13. 17 U.S.C. § 501(a) (Supp. IV 1992); 17 U.S.C. § 602 (1988 & Supp. IV 1992).
14. *See* J. CONKLIN, ILLEGAL BUT NOT CRIMINAL: BUSINESS CRIME IN AMERICA 129 (1977).

imprisonment for white-collar offenders.[15] Accordingly, the Guidelines treat the criminal infringement of copyrights or trademarks (or the unauthorized interception of certain electronic signals, such as satellite television transmissions) much like other types of theft or fraud by making the "retail value" of the infringing items the key determinate of the ultimate sentence.[16] This retail-value approach is crucial, because, as the Guidelines commentary notes, "the value of the infringing items . . . will generally exceed the loss or gain due to the offense."[17]

Thus, a typical first-time infringer, making two thousand copies of a software program with a retail value of $50, faces a base sentence of ten to sixteen months incarceration.[18] Greater monetary losses, more significant roles in the offense, or extensive operations can result in even higher penalties.[19] Thus, at least in theory, federal courts will now treat the illegal *copying* of software as indistinguishable from the illegal *theft* of that software.[20]

IV
New Approaches Among Law Enforcement Agencies

As important as the newly heightened penalties are the changing attitudes of federal and state law enforcement agencies. The Federal Bureau of Investigation ("FBI") has long been reluctant to investigate misdemeanor copyright infringements, particularly in view of the strong civil sanctions available under Title XVII.[21] The conversion of these cases to felonies, reflecting new congressional interest in the area, has helped to focus federal law enforcement on this growing area.[22] Moreover, the FBI's National Economic Security Threat List ("NESTL") reflects a reorientation in the post-Cold War era to focus some of its foreign counter-intelligence resources on the threats to the nation's economic well-being.[23]

15. United States Sentencing Commission, *Guidelines Manual*, ch. 1, Pt. A(4)(d) (Nov. 1993).

16. U.S.S.G. § 2B5.3(b) cmt.

17. U.S.S.G. § 2B5.3 cmt.

18. U.S.S.G. §§ 2B5.3, 2F1.1(b)(1), ch. 5, pt. A.

19. *Id.*

20. The United States Department of Justice has also proposed an entirely new section for the Sentencing Guidelines designed to deal with other forms of computer crime, including unlawful computer hacking that compromises privacy or interferes with the operation of computer systems. 57 Fed. Reg. 62832 (Dec. 31, 1992).

21. S. REP. NO. 268, 102d Cong., 2d Sess. 2 (1992).

22. *See, e.g.*, James Bernstein, *Feds Find Illegal Software in Raid*, NEWSDAY, Oct. 30, 1992, at 51.

23. FBI Headquarters, National Security Division.

This initiative places special emphasis on crimes involving critical technologies, including computer software, computer hardware, telecommunications, and biotechnology.[24] Some of the most egregious piracy of copyrighted and trademarked products occurs abroad, particularly in lesser developed nations that lack a tradition of intellectual property protection. The Software Publishers Association estimated in 1990 that the software industry alone, with domestic revenues of $4.6 billion, lost $2.4 billion to domestic piracy, while worldwide piracy losses were between ten and twelve billion dollars.[25]

Other federal law enforcement agencies, including the United States Customs Service, which is responsible for all import and export violations including importation of counterfeit or infringing goods, and the United States Secret Service, which is responsible for various types of computer crime, especially crime that affects financial institutions, have begun to emphasize high-technology investigations.

Similarly, the Department of Justice has created a Computer Crime Unit ("Unit") dedicated exclusively to the prosecution of high-technology crimes, including copyright and trademark offenses, as well as wire fraud, criminal computer hacking, and use of computer bulletin-boards to exchange child pornography or stolen credit information. This Unit has proposed new sentencing guidelines governing criminal computer hacking, computer intrusions, and theft of private or classified information via computer and telecommunications systems.

The United States Attorney's Office for the Northern District of California, which includes Silicon Valley as well as many of the biotechnology and software industries of Northern California, has announced a high-technology crime initiative targeting such crimes. The Office has also begun working with state and local law enforcement to investigate and prosecute strong-arm robberies of computer chips, which are often, ounce-for-ounce, more valuable than heroin.

V
Recent Criminal Prosecutions

Grand juries have returned a number of indictments as a result of the new enforcement priorities. On July 7, 1993, a federal grand jury sitting in San Francisco returned a nine-count indictment against a corporation that was systematically copying and distributing more than twenty thousand copies of copyrighted and trademarked

24. *Id.*
25. SOFTWARE PUBLISHERS ASS'N, SOFTWARE PIRACY 6 (Nov. 1, 1992).

MicroSoft MS-DOS and Windows software and manuals.[26] The indictment represented not only the first charges in the nation under the new felony copyright statute[27] but also included charges that the defendants had laundered their profits through overseas accounts, giving the government the right to seize and forfeit their assets.[28]

In San Jose, a separate grand jury recently handed down the first indictment charging criminal infringement of copyrighted CD-ROM software.[29] An earlier case resulted in the first jail sentences for software copyright infringers.[30] In the telecommunications arena, various individual and corporate defendants were convicted for their roles in selling cable television equipment designed to intercept television programming without authorization.[31] Current grand jury investigations include the illegal export of restricted technology and the theft of computer technology.

VI
Limits to Criminal Prosecution of Information Theft

There remain, of course, limits to the reach of criminal prosecution for the theft of information. There is no federal law prohibiting trade secret theft, often the most valuable and sensitive property of many high-tech firms. Some states have laws that cover the theft of trade secrets,[32] but the penalties for state offenses are typically lower than those for similar federal offenses.[33] Moreover, there are difficulties with such prosecutions, including establishing that the trade secret was in fact secret (typically determined by the measures taken to safeguard it) and that it had commercial value (a subjective question often open to dispute).

Moreover, unlike laws prohibiting copyright infringement, there are no criminal penalties for patent infringement. This perhaps reflects the difficulty of proving that a patent infringement included the appropriate *mens rea*, given the possibility of independent creation

26. United States v. Prosys, Inc., No. CR-93-0348-RHS (N.D. Cal. 1993).

27. *Indictments Under New Software Piracy Law Issued*, BOSTON GLOBE, July 8, 1993, at 37.

28. *Prosys*, No. CR-93-0348-RHS.

29. United States v. C-88 Corp., Int'l, No. CR-93-20133-RMW (N.D. Cal. 1993).

30. United States v. Lee, No. CR-92-0456-SBA (N.D. Cal. 1992).

31. United States v. Neplokh, No. CR-92-0546-MAG (FSL) (N.D. Cal. 1993).

32. *See, e.g.*, CAL. PENAL CODE § 499(c) (West 1988) (providing for fine up to five thousand dollars and/or imprisonment up to one year).

33. *See, e.g.*, 18 U.S.C. § 1343 (1988 & Supp. 1993) (providing for fine up to one thousand dollars and/or imprisonment up to five years).

and the arcane nature of the patent prosecution process conducted by the United States Patent Office.

Furthermore, while a criminal proceeding is typically much faster and results in stronger penalties than a civil suit, there are some drawbacks associated with a criminal prosecution. A victim company will necessarily have less control over proceedings instituted by the government than it would have over civil litigation. While criminal discovery is typically far more limited than civil discovery (avoiding, for example, depositions, interrogatories, and requests for production except on narrow grounds), the case may attract publicity to a company's problem with piracy. Finally, while the federal Victim's Rights and Restitution Act[34] entitles a victim company to restitution for the full amount of its losses, such restitution may be less than what is available under the statutory damages provisions of civil copyright law[35] or the Lanham Act.[36]

VII
The Elements of Criminal Copyright Infringement

Because criminal copyright infringement charges have the most general application to this area, it is useful to review the surprisingly straightforward elements of a criminal copyright infringement prosecution. As with a civil infringement action, a criminal copyright action requires proof that the defendant infringed a valid copyright.[37] This includes proof of the existence of the copyright, either through a certificate of registration from the Register of Copyrights or testimony from the author regarding the work's originality and date of fixation in a tangible medium.[38]

The most common types of infringement subject to criminal prosecution involve reproduction or distribution of a copyrighted item in violation of 17 U.S.C. § 106(1) and (3).[39] The prosecution need not prove that the infringing work is identical to the original work in all

34. 42 U.S.C. §§ 10601 et seq. (1988 & Supp. IV 1992).

35. 17 U.S.C. §§ 504-505 (1988 & Supp. IV 1992).

36. 15 U.S.C. §§ 1051 et seq.

37. 17 U.S.C. § 106 (1988).

38. A copyright infringement action, whether civil or criminal, may be brought only with respect to works registered with the Register of Copyrights. *See* 17 U.S.C. § 411 (1988 & Supp. IV 1992). The requirements for registration include attaching copyright notices to all publicly distributed copies and depositing copies with the Library of Congress. 17 U.S.C. §§ 401-12 (1988 & Supp. IV 1992).

39. For copyright violations involving computer programs, the government must also prove that the copies were not legally made for archival purposes or as a necessary part of the use of the program. *See* 17 U.S.C. § 117 (1988 & Supp. IV 1992).

respects.[40] Rather, the government may prove infringement by demonstrating "substantial similarity" of the original work and the infringing work.[41] Criminal prosecutions differ most dramatically from civil infringement actions in requiring the government to prove that a defendant acted "willfully and for purposes of commercial advantage or private financial gain."[42] A defendant need not have profited from the infringement, as long as he or she intended to make a profit.[43]

Finally, as in civil infringement actions, criminal prosecutors must recognize the possibility of a defense that the infringing item was properly acquired (the "first sale" doctrine).[44] Although some courts have held that the government must prove the absence of a first sale,[45] the better view, which is supported by the legislative history of the statute, is that a claim of "first sale" is an affirmative defense in both civil and criminal actions.[46] Of course, because the first sale doctrine permits only display and resale of the purchased items,[47] it does not apply to charges of reproducing copyrighted works.

VIII
How to Convince Law Enforcement to Investigate & Prosecute a Case

From the perspective of someone who has had a copyright or trademark infringed, or who has been defrauded of intellectual or other high-tech property through mail or wire fraud, or who has lost information to a criminal computer hacker, the most pressing question is how to convince law enforcement agencies to investigate and prosecute the case. Federal prosecution is often particularly attractive. Not only do federal offenses generally carry stiffer sentences, but federal investigating agencies often have greater resources available, including the ability to pursue suspects nationally or internationally. Moreover, cases typically move more rapidly through the federal system than through crowded state court dockets.

40. *See* United States v. O'Reilly, 794 F.2d 613, 615 (11th Cir. 1986).

41. Hoehling v. Universal City Studios, Inc., 618 F.2d 972, 977 (2d Cir. 1980), *cert. denied*, 449 U.S. 841 (1980).

42. 17 U.S.C. § 506(a) (1988).

43. *See, e.g.*, United States v. Cross, 816 F.2d 297, 301 (7th Cir. 1987); United States v. Shabazz, 724 F.2d 1536, 1539 (11th Cir. 1984).

44. 17 U.S.C. § 109(a) (1988).

45. *See, e.g.*, United States v. Sachs, 801 F.2d 839, 842 (6th Cir. 1986).

46. *See* United States v. Larracuente, 952 F.2d 672, 673-74 (2d Cir. 1992); H.R. REP. No. 1476, 94th Cong., 2d Sess. 1 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5694-95.

47. 17 U.S.C. § 109(a) and (c) (1988).

What makes a given case attractive to federal prosecutors and law enforcement agents? Certainly the amount of the loss can be a significant factor. Because it is often difficult to measure the amount of foregone revenues that an infringement costs the true owner of goods, typically loss is measured by the value of the infringing or counterfeit goods. In addition to the amount of loss, prosecutors may also look at how blatant the piracy is, including whether the suspects had a license to produce the product, and whether they continued production greatly in excess of authorized quantities or after the license had expired.

Prosecutors may also consider the adequacy of civil remedies. If an infringer has deep pockets and is not likely to flee a lawsuit, the substantial civil penalties available may suffice. On the other hand, if an infringer runs a fly-by-night operation with few ties to the community and little money to pay a judgment or has infringed the copyrights of a variety of victims, it may seem more appropriate for the government to file criminal charges to vindicate the rights of the victims.

Finally, a case with novel or interesting facts often appeals to law enforcement entities hoping to deter other potential infringers in the community.

IX
Conclusion

Victims of high-technology and intellectual property crimes should consider the option of pressing criminal charges against those who would steal their stock in trade. Increasingly, federal and state law enforcement agencies are encouraging such referrals and are developing the statutory authority, the resources, and the expertise needed to investigate and prosecute these crimes. Ultimately, however, the chances for a successful criminal prosecution depend on the cooperation of the victim.