INTELLECTUAL PROPERTY CRIMES

I. INTRODUCTION

Owners of intellectual property are able to protect their rights by pursuing civil remedies. Yet the possibility of civil sanctions alone is insufficient to deter violators who steal trade secrets or infringe on others' trademarks, copyrights, or patents.[1] Indeed, some intellectual property thieves view civil damage actions as

1. Historically, theft of trade secrets has been handled by civil remedies. However, because of increased technological complexity, delays in civil litigation, and advances in computer technology, all of which permit thieves to profit more rapidly from trade secrets, traditional remedies, such as injunctions and civil damages, have become largely ineffective. Furthermore, considering the intangible nature of trade secrets and the fact that thieves are often judgment proof or too sophisticated to pursue, the civil remedy is quite illusory. *See* J. Derek Mason et al., *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets*, 16 No. 3 COMPUTER LAW 14, 15 (1999).

just another cost of doing business. It has been estimated that the theft of intellectual property rights in the United States cost over $300 billion dollars in 1997, with high technology corporations most frequently targeted.[2] A more recent study sponsored by American Society for Industrial Security estimates that in 1999, *Fortune 1000* companies alone lost more than $45 billion from theft of trade secrets.[3]

The lack of deterrence associated with civil mechanisms has led the federal government and most states to enact statutes designed to prevent the theft of intellectual property rights. These are usually broadly-written statutes that encompass the intellectual property at issue in any given case. Other statutes are specifically tailored to the type of intellectual property for which protection is sought. These latter provisions are used with increasing frequency to deter and punish perpetrators.

This article examines several areas of intellectual property law under which criminal prosecutions are brought. Section II covers the theft of trade secrets, while Section III discusses trademark counterfeiting. Section IV addresses copyright infringement. Section V examines the new problems raised by online servers, while Section VI looks at patents and Section VII at art crimes. Finally, Section VIII discusses sentencing for intellectual property crimes.

II. THEFT OF TRADE SECRETS

Prior to the enactment of the Economic Espionage Act, addressed in Part A, no federal criminal statute dealt directly with the theft of intangible trade secrets. Parts B through E of this Section will cover alternative statutes federal prosecutors have used in the past, with limited success, to penalize the misappropriation of trade secrets. These include the National Stolen Property Act, the Trade Secrets Act, the Mail and Wire Fraud statutes, and the Racketeer Influenced and Corrupt Organizations Act. Finally, Part F describes state provisions used to combat trade secret theft.

A. Economic Espionage Act of 1996

In October 1996, discouraged by the failure of civil remedies to prevent trade secret theft, the inability of prosecutors to effectively use other criminal statutes,

---

2. *See* Jack Nelson, *Spies Took $300-Billion Toll on U.S. Firms in '97 Business: FBI Says Espionage is Increasing, with at Least 23 Governments Targeting American Companies*, L.A. TIMES, Jan. 12, 1998, at A1 (noting that numerous foreign governments are "targeting" intellectual property of American firms, especially trade secrets); Sharon Walsh & Robert O'Harrow, Jr., *Trying to Keep a Lock on Company Secrets; Law Enforcement Officials Fear Rise in Computer Crimes, Made Easier by Technological Advances*, WASH. POST, Feb. 17, 1998, at D1 (describing computer espionage aimed at company secrets).

3. American Society for Industrial Security/PricewaterhouseCoopers, TRENDS IN PROPRIETARY INFORMATION LOSS: SURVEY REPORT, 1999 (reporting statistics gathered from a 1998 survey on loss of proprietary information).

and the frequent efforts by foreign governments to obtain trade secrets from American companies, Congress made the theft of trade secrets a federal crime by enacting the Economic Espionage Act ("EEA").[4] The EEA established two criminal offenses under which governments can prosecute trade secret theft. The first offense, "economic espionage" ("§ 1831"), arises only when the theft benefits a foreign government.[5] This carries higher penalties than the second offense, "theft of trade secrets" ("§ 1832"), which is broader and generally concerns all trade secret theft.[6] The "theft of trade secrets" offense, though broader, includes three requirements not necessary for prosecution under the "economic espionage" offense. One is that the benefit intended to be conferred must be economic in nature. In contrast, § 1831 simply requires that the defendant benefit the foreign instrumentality in any manner. Secondly, § 1832 requires that the defendant intended or knew that the offense would injure the owner of the trade secret. This level of scienter is not necessary under § 1831. Finally, § 1832 demands that the stolen information be involved in interstate commerce; this factor is unnecessary under the "economic espionage" section.[7]

1. Definition of Trade Secret

The EEA defines trade secrets to include "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . . ."[8] Although substantially similar to the trade secret definition in the civil Uniform Trade Secrets Act ("UTSA"),[9] the definition in the EEA is broader in an effort to

4. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839); *see* Gerald J. Mossinghoff et al., *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, 79 J. PAT. & TRADEMARK OFF. SOC'Y 191, 191-95 (1997) (discussing reasons for enactment of EEA).

5. 18 U.S.C. § 1831 (1994 & Supp. IV 1998) (delineating what constitutes economic espionage).

6. 18 U.S.C. § 1832 (1994 & Supp. IV 1998) (delineating what constitutes theft of trade secrets). The EEA provides for a maximum term of imprisonment of fifteen years if the criminal act was done with the intent to benefit a foreign government and ten years in all other cases. The maximum fine that may be imposed upon an organization is $10 million if the intent of the organization was to benefit a foreign government. In all other cases, the maximum fine imposed on an organization is $5 million. 18 U.S.C. §§ 1831-1832 (Supp. IV 1998).

7. United States v. Hsu, 155 F.3d 189, 195-96 (3d Cir. 1998) (discussing limitations contained in § 1332 that are not found in § 1331).

8. 18 U.S.C. § 1839 (1994 & Supp. IV 1998) (listing definitions of terms used in Chapter 90—Protection of Trade Secrets). Even if the original owner never loses custody over his property, the EEA recognizes the loss of value to that owner. *See generally* COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, FEDERAL PROSECUTION OF VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS (COPYRIGHTS, TRADEMARKS AND TRADE SECRETS) 73 (1997) [hereinafter "FEDERAL PROSECUTION MANUAL"] (describing the elements of the EEA, and other possible charges for the theft of trade secrets), *available at* http://www.usdoj.gov/criminal/cybercrime/intell_prop_rts/toc.htm.

9. UNIF. TRADE SECRETS ACT §§ 1-12, 14 U.L.A. 437 (1990) [hereinafter "UTSA"] (describing civil penalties for theft of trade secrets).

modernize the law and "keep pace with growing technology, especially in the computer and information storage sectors."[10]

In order to protect property that is considered a trade secret, the owner of the property must take reasonable measures to keep it secret.[11] Additionally, the economic value of the information must be derived from the public's lack of knowledge or inability to readily access the information through proper means.[12] This provision imposes a higher standard of self-protection on the owner of a trade secret than on owners of other types of property.[13]

2. Tangibility

The EEA represents the first time federal legislation has specifically protected intangible property without additional requirements, such as a use of mail or a wire transmission. This protection of intangible property stems from the EEA's broad definition of trade secrets to include "all forms and types of . . . information . . . whether tangible or intangible, and whether or how stored . . . ."[14] The Act therefore covers information stolen in electronic form or merely memorized.[15]

However, the EEA's legislative history indicates the provision covering memorized information was not intended to include general knowledge and skill learned on a job when an employee leaves one company and moves to another in the same or a similar field.[16]

---

10. Mossinghoff, *supra* note 4, at 197. The EEA trade secret definition is broader in that it expands the number of trade secrets listed, expressly protects intangible information, and protects information in any form regardless of how it is stored. *See* Arthur J. Schwab & David J. Porter, *Federal Prosecution of Trade Secrets: Understanding the Economic Espionage Act of 1996*, 10 No. 4 J. PROPRIETARY RTS. 2, 3-4 (1998) (describing the EEA's expansion of the UTSA's list of representative trade secrets); *see also* J. Derek Mason et al., *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets*, 16 No. 3 COMPUTER LAW. 14, 14-16 (1999) (discussing the history and provisions of the Economic Espionage).

11. 18 U.S.C. § 1839(3)(A) (1994 & Supp. IV 1998) (defining trade secret). This is similar to the UTSA which obligates owners to take "efforts which are reasonable under the circumstances to maintain its secrecy." UTSA § 1 (1996).

12. 18 U.S.C. § 1839(3)(B) (1994 & Supp. IV 1998); *see* Michael G. Radigan, *Safeguarding Against Economic Espionage*, 221 N.Y. L.J. 88 (May 10, 1999) (discussing the legal framework for protection of trade secrets and recommending preventative measures for protecting corporate assets from theft). This requirement is broader than the U.T.S.A.'s corresponding provision. The U.T.S.A. requires the person misappropriating the trade secret be the one who will benefit economically from its disclosure or use. Mason, *supra* note 10, at 16.

13. *See* FEDERAL PROSECUTION MANUAL, *supra* note 8, at 75.

14. 18 U.S.C. § 1839(3) (1994 & Supp. IV 1998).

15. *See* James H. A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 189-90 (1997) (arguing that mere memorization and use of general experience gained should not be a basis for civil liability against former employees).

16. H.R. Rep. No.104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026 [hereinafter "EEA HOUSE REPORT"] (reporting legislative history of the EEA).

3. Intent and Method of Misappropriation

Under § 1831, the perpetrator must intend or know that the "offense will benefit any foreign government, foreign instrumentality, or foreign agent."[17]

When trade secret theft does not benefit a foreign government, provisions of § 1832 apply. Under the EEA, "theft of trade secrets" requires specific intent and methods of misappropriation. Section 1832 states broadly that any unauthorized possession of a trade secret with intent to injure another violates the Act.[18]

The EEA intent requirements include "knowingly" intending "to convert a trade secret," while "knowing that the offense will . . . injure any owner of that trade secret."[19] Consequently, the scope of the EEA is somewhat more limited than its civil counterpart, the UTSA, which does not require that the "defendant be aware of the trade secret."[20] However, § 1832 does not require that the defendant be aware of the trade secret under its attempt and conspiracy provisions.[21]

At the same time, the EEA's definition of "theft" of a trade secret is broader than the UTSA's, which defines "theft" as misappropriation by improper means.[22] In contrast, the EEA defines three categories of theft: (1) stealing or obtaining by

---

17. 18 U.S.C. § 1831(a) (1994 & Supp. IV 1998) (delineating what constitutes economic espionage).

18. Section 1832 states in relevant part:

> [w]hoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy . . . .

18 U.S.C. § 1832(a) (1994 & Supp. IV 1998). The five clauses of §§ 1831(a) and 1832(a) are the same and are presumably disjunctive so that violation of any one clause is sufficient to violate the statute. 18 U.S.C. §§ 1831(a), 1832(a) (Supp. IV 1998). Section 1832 contains three limitations not found in § 1831: (1) defendant must intend to convert a trade secret to the economic benefit of someone other than the owner; (2) defendant must intend or know the threat will injure the owner of the trade secret; and (3) the trade secret must be "related to or included in a product that is produced for or placed in interstate or foreign commerce." United States v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998) (holding that impossibility is not a defense to attempted trade secret theft, even where no actual trade secret is used in an investigation of an EEA violation).

19. 18 U.S.C. § 1832(a) (1994 & Supp. IV 1998) (delineating what constitutes theft of a trade secret).

20. UTSA, 14 U.L.A. 437 (1990).

21. *Hsu*, 155 F.3d at 198 ("attempt and conspiracy . . . do not require proof of the existence of an actual trade secret.").

22. *See* Pooley, *supra* note 15, at 192 & n.91 (defining misappropriation under the UTSA).

deception, (2) copying, destroying, or conveying, and (3) mere receipt of stolen information.[23]

4. Applicability to Conduct Abroad

Another expansive provision of the EEA is § 1837, which allows the government to prosecute conduct that occurs overseas if the party involved in the activity is bound by U.S. federal law or if an "act in furtherance of the offense was committed in the United States."[24] The first provision in § 1837 extends the jurisdictional reach of the federal government to penalize the actions of U.S. citizens and corporations abroad, even when there is no other connection with the United States.[25] The second provision enables the federal government to pursue trade secret theft outside of the country as long as some part of the activity, such as a phone call, was connected to the United States.[26]

At the same time, § 1833 narrows the scope of the act by providing two exceptions relating to law enforcement and other governmental activities.[27] The first exception allows the government to continue an otherwise lawful "investigative, protective, or intelligence activity."[28] The second exception permits the reporting of suspected criminal activity to law enforcement.[29]

5. Prosecutions Under the EEA

As the EEA is a relatively new law, the government has only begun to prosecute violators. Some commentators have attributed the slow enforcement to the tension between criminal law and the generally civil nature and history of intellectual property protection.[30] Commentators also speculate that the government will wait

---

23. 18 U.S.C. § 1832(a)(3) (1994 & Supp. IV 1998) (applying the act to anyone who knowingly "receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization"); *see* Pooley, *supra* note 15, at 192 (stating that EEA provisions are in some respects significantly broader than other civil trade secret laws).

24. 18 U.S.C. § 1837 (1994 & Supp. IV 1998) (describing the applicability of the EEA to conduct outside the United States).

25. 18 U.S.C. § 1837(1) (1994 & Supp. IV 1998) (extending the EEA's jurisdictional reach to citizens, permanent residents, or organization organized under laws of the United States).

26. 18 U.S.C. § 1837(2) (1994 & Supp. IV 1998) (extending the EEA's jurisdictional reach to crimes where "some act in furtherance of the offense was committed in the United States").

27. Section 1833 states:

> [t]his chapter does not prohibit—(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or (2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if has lawful authority with respect to that violation.

18 U.S.C. § 1833 (1994 & Supp. IV 1998).

28. EEA HOUSE REPORT, *supra* note 16, at 14.

29. *Id.*

30. *See* Gerald J. Mossinghoff et al., *The Economic Espionage Act: A Prosecution Update*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 360, 366 (1998) (reporting criminal actions and convictions under the EEA).

for cases where "the blatancy of the theft and the potential ease of conviction" are obvious.[31] Others attribute the conservative use of the EEA as a result of Congress's concern about stifling competition.[32]

The government has brought at least eleven criminal actions under the EEA.[33] All are fairly straightforward, stemming from FBI stings, and were filed under § 1832.[34] Cases filed under the EEA include the theft of trade secrets involving a cancer-fighting drug, Taxol,[35] PPG Industries' glass-making process,[36] Intel computers,[37] a veterinary test kit owned by Idexx Laboratories of Maine,[38] a breast cancer treatment called Taximofen,[39] designs for a controlling mechanism for a coal-mining machine manufactured by Joy Mining Machinery Inc.,[40] and a proprietary software program developed by Deloitte-Touche.[41] The EEA has also been used to prosecute the attempted theft of Hoffman La Roche's Hepatitis C monitoring kit,[42] future razor systems from the Gillette Company,[43] and the attempted sale of marketing plans and subscription lists to a rival newspaper.[44]

---

31. Victoria Slind-Flor, *New Spy Act to Boost White-Collar Defense Biz: Enhanced Enforcement of Trade Secret Theft Expected*, NAT'L L.J., July 28, 1997, at A1; *see also* Mossinghoff, *supra* note 30, at 367 (opining government desire to "work out the 'bugs' in new law" with lesser offenders before pursuing more serious cases).

32. *See* Joel M. Androphy et al., *Criminal Prosecutions of Trade Secret Theft: The Emergence of the Economic Espionage Act*, 38-Aug. HOUS. LAW. 16, 17 (2000) (describing the EEA as an emerging tool to protect trade secrets in the age of technological advances).

33. The FBI investigated approximately 800 EEA cases in 1998. *See* Mason, *supra* note 1, at 18 (citing *Too Much Trust: Are trade secrets safe with suppliers?*, INDUSTRY WEEK, Nov. 2, 1998, at 27).

34. *See* Mossinghoff, *supra* note 30, at 366-67. Although some current cases involve foreign companies and nationals, there have been no cases under § 1831 involving the theft of trade secrets to benefit foreign governments, instrumentalities, or agents.

35. United States v. Hsu, 155 F.3d 189, 191-92 (3d Cir. 1998); *see* United States v. Hsu, 40 F. Supp. 2d 623, 627-28 (E.D. Pa. 1999) (holding on remand that the EEA is not unconstitutionally vague as applied to defendant, and did not implicate defendant's first amendment right to free speech). *But see* Robin D. Ryan, *The Criminalization of Trade Secret Theft Under the Economic Espionage Act of 1996: An Evaluation of United States v. Hsu*, 25 U. DAYTON L. REV. 243, 244-45 (2000) (arguing that, despite the district court's decision, the EEA conflicts with the constitutional requirement that statutes define the crime with sufficient clarity).

36. *See* Slind-Flor, *supra* note 31, at A1 (noting that the PPG case was one of the first two prosecutions under the Act).

37. United States v. Pringle, Criminal No. 98-M-37 (filed E.D. Tex. 1998) (discussing alleged theft of Intel computers); United States v. Hallstead, Criminal No. 98-CR-00041 (filed E.D. Tex. 1998) (same).

38. United States v. Camp et al., Criminal No. 98-CR-00048 (filed E.D. Me. 1998).

39. Slind-Flor, *supra* note 31, at A1.

40. United States v. Fulton, Criminal No. 98-CR-00054 (filed N.D. Ga. 1998).

41. *See* United States v. Trujillo-Cohen, Criminal No. CR-H-97-251 (filed S.D. Tex. 1997) (charging defendant with knowing conversion of proprietary software program by selling it for her personal benefit). The employee pled guilty to one count under the EEA and one count of mail fraud. She was sentenced to forty-eight months in prison for each count and was ordered to pay $337,000 in full immediately. *See* Mossinghoff, *supra* note 30, at 366 (noting that *Trujillo-Cohen* appears to be the first case that cites no other criminal statutes other than the EEA in the indictment).

42. United States v. Pei, Criminal No. 98-M-04090 (filed D.N.J. 1998).

43. *See* Mossinghoff, *supra* note 30, at 365-66 (discussing Gillette employee's attempts to sell trade secrets to competitors).

44. *See id.* at 366 (discussing arrest of circulation managers after allegedly offering to sell marketing plans and subscription lists to rival newspaper).

Lastly, in April 1999, a Taiwanese businessman and his daughter were convicted of conspiracy to steal trade secrets and attempted theft of trade secrets under the EEA, in connection with the theft of trade secrets from the Avery Dennison Corporation relating to formulations for self-adhesive products, initially valued at $50-$60 million.[45]

6. *Defenses*

Defenses to the EEA include: (1) independent development; (2) reverse engineering; (3) and lack of secrecy. All of the defenses are available in civil misappropriation cases, though not statutorily specified in the EEA.[46]

B. National Stolen Property Act

The National Stolen Property Act ("NSPA")[47] provides criminal sanctions for any person who "transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud . . . ."[48] Federal courts have held that under certain circumstances the NSPA is applicable

45. *See* United States v. Yang, 74 F. Supp. 2d 724 (N.D. Ohio 1999) (denying defendant's motion for a new trial after conviction under the EEA); *see also* Mossinghoff, *supra* note 30, at 365 (discussing the *Yang* arrests resulting from FBI sting operation); Daniel Eisenberg, *Eyeing the Competition*, TIME, Mar. 22, 1999, at 58 (discussing lawsuits, including that against the Yangs, filed under the EEA).

46. *See* 142 CONG. REC. S12,212-13 (daily ed. Oct. 2, 1996) (statement of Sens. Spector and Kohl) (asserting (1) that parallel development of a trade secret cannot constitute a violation of the EEA, (2) that reverse engineering of a product to which access has been lawfully gained cannot constitute a violation of the EEA, and (3) that where an owner fails to safeguard his trade secret, no one can be rightfully accused of misappropriating it). *See Generally* Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235 , 294-95 (1999) (describing defenses to and sanctions for intellectual property crimes); Dennis J. Kelly & Paul R. Mastrocola, *The Economic Espionage Act of 1996*, 26 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 181, 187 (2000) (noting that the EEA's legislative history shows that Congress did not intend "parallel development" or "reverse engineering" to be crimes).

47. 18 U.S.C. § 2314 (1994). The NSPA was intended "to fight the 'roving criminal' whose access to automobiles made it easy to move stolen property across state lines . . . frustrating local law enforcement." Keith D. Krakaur & Robert C. Juman, *Two New Federal Offenses Help Battle Corporate Espionage*, 4 NO. 2 BUS. CRIMES BULL.: COMPLIANCE & LITIG. 7, 7 (1997).

48. 18 U.S.C. § 2314 (1994). Section 2314 provides criminal sanctions to any person who:

> having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person or persons to travel in, or to be transported in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of $5,000 or more . . . .

18 U.S.C. § 2314 (1994).

to the theft of tangible property containing trade secrets,[49] even though the NSPA was not designed or intended to apply to trade secret theft.[50]

1. Transported in Interstate or Foreign Commerce

To fall within the scope of the NSPA, allegedly stolen trade secrets must be transported or transferred in interstate or foreign commerce.[51] This requirement exists because Congress enacted the statute under the authority of the commerce clause. The purpose of the statute was to combat theft across state and foreign boundaries, previously not actionable by individual state and foreign governments.[52] The prosecution must also prove that the stolen item was physically transported.[53] It is not enough for the prosecution to establish the presence of a stolen trade secret in a state or country other than its original location.[54]

2. Goods, Wares or Merchandise

Goods, wares or merchandise have been defined broadly as "such personal property or chattels as are ordinarily a subject of commerce."[55] Courts have also

---

49. *See* United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (ruling that theft of sample of synthetic casting material used in repairing broken bones falls under NSPA even though a major portion of its value comes from an intangible component); United States v. Bottone, 365 F.2d 389, 393-94 (2d Cir. 1966) (holding NSPA applicable to theft copies, made by thieves, of documents containing trade secrets); United States v. Seagraves, 265 F.2d 876, 880 (3d Cir. 1959) (finding that theft of geophysical maps identifying possible oil deposits falls under NSPA).

50. *See* Spencer Simon, *The Economic Espionage Act of 1996*, 13 BERKELEY TECH L.J. 305, 306 (1998) (explaining the history of the National Stolen Property Act).

51. 18 U.S.C. 2314 (1994) (criminalizing transportation of stolen goods in interstate or foreign commerce); *see* Van Dorn Co. v. Howington, 623 F. Supp. 1548, 1558 (N.D. Ohio 1985) (holding insufficient a claim under the National Stolen Property Act that did not allege interstate transportation of the stolen property).

52. *See* Peter J. G. Toren, *The Prosecution of Trade Secret Thefts Under Federal Law*, 22 PEPP. L. REV. 59, 67-68 (1994) (describing the rationale underlying the enactment of the National Stolen Property Act).

53. United States v. Brown, 925 F.2d 1301, 1309 (10th Cir. 1991) (dismissing indictment for lack of proof that computer program was physically removed from plaintiff's place of business).

54. *See* Abbott v. United States, 239 F.2d 310, 312 (5th Cir. 1956) (requiring government to prove "[w]ho carried it, or how, or who caused it to be transported"); *see also Bottone*, 365 F.2d at 393-94 (finding NSPA covers stolen photocopies transported in interstate commerce); *Howington*, 623 F. Supp. at 1558 (holding that plaintiff must allege transportation with particularity rather than "merely stat[ing] that a trade secret was appropriated in violation of the statutes").

55. United States v. Seagraves, 265 F.2d 876, 880 (3d Cir. 1959) (citing definition in BLACK'S LAW DICTIONARY 823 (4th ed. 1951)). In *Seagraves*, the stolen trade secrets were geophysical and geological maps produced by Gulf Oil and copied with its equipment onto its paper. The court distinguished the instant case from others by noting that the trade secrets stolen were "the permanent form into which was cast the advice and assistance for which the defendants were consulted." *Id.* at 880. Evidence showed that maps of this type were frequently sold. In addition, expert testimony established the value of some of the individual maps at well over $5,000. *Id.* Other courts have interpreted goods, wares or merchandise similarly. *See Brown*, 925 F.2d at 1308-09 (concluding that goods, wares, or merchandise must be transported in physical form to qualify as stolen trade secrets under NSPA); United States v. Greenwald, 479 F.2d 320, 322 (6th Cir. 1973) (finding documents containing chemical formulation to be goods, wares, or merchandise given the established and viable, albeit limited, market in

held that trade secrets must be stolen while in a tangible form or in conjunction with tangible goods.[56] A violation cannot be established if, for example, a thief merely memorizes a secret formula and then writes it down after crossing a state or foreign boundary.[57]

3. Minimum Value of $5,000

The intent of the NSPA is to address only the theft of items having substantial market value.[58] Courts have taken a variety of approaches in determining the "value" of trade secrets. Some courts have looked for an actual market for the products embodying the stolen trade secrets to determine their value.[59] Absent a market, courts have looked for "any reasonable method" of valuation.[60] Another alternative is using the black market price.[61]

4. Stolen, Converted, or Taken by Fraud

Finally, the NSPA requires a physical theft; the "goods, wares, [or] merchandise" must be physically "stolen, converted or taken by fraud."[62]

5. Knowledge that Items Were Stolen

Possession of stolen trade secrets by a defendant is not sufficient to place a

---

chemical formulations and that established market among chemical competitors for chemical formulations is sufficient to make stolen chemical formula "good" within meaning of NSPA).

56. *E.g.*, United States v. Lyons, 992 F.2d 1029, 1033 (10th Cir. 1993) (holding that computer software stolen in conjunction with computer hardware was theft of tangible property).

57. *E.g.*, R.E. Davis Chem. Corp. v. Nalco Chem. Co., 757 F. Supp. 1499, 1512 (N.D. Ill. 1990) (noting that documents obtained and studied within boundaries of Texas had not crossed state lines).

58. *E.g.*, United States v. Schaffer, 266 F.2d 435, 439 (2d Cir. 1959), *aff'd*, 362 U.S. 511 (1960) (relying on legislative history to conclude that purpose of $5000 minimum value is to avoid placing too great a burden on Department of Justice).

59. *See Seagraves*, 265 F.2d at 880 (3d Cir. 1959) (looking to experts' valuation for type of maps stolen to determine their market value); *Greenwald*, 479 F.2d at 321 (acknowledging established market of chemical formulae and formulations). *But see* United States v. Coviello, 225 F.3d 54, 63 (1st Cir. 2000) (holding proper measure of loss was standard wholesale price of stolen CD-ROM discs); In re Vericker, 446 F.2d 244, 248 (2d Cir. 1971) (refusing to find market for papers showing individuals who are or may have engaged in criminal activity or showing procedures used by FBI in tracking them down); United States v. Willette, 764 F. Supp. 759, 761-62 (N.D.N.Y. 1991) (refusing to determine value of stolen knives based on retail price when owner was part of wholesale market).

60. *See* United States v. Wilson, 900 F.2d 1350, 1355-56 (9th Cir. 1990) (rejecting strict market value in cases of goods with no readily ascertainable market value and allowing any reasonable method of ascribing an equivalent monetary value to the items); United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (valuing trade secret by looking to amount owner invested in development and production of trade secret); *but see* Abbott v. United States, 239 F.2d 310, 312-13 (5th Cir. 1956) (rejecting alternate valuation scheme and interpreting § 2311 to require establishment of genuine market value—where willing buyers bargain with willing sellers—to meet minimum value requirement).

61. *See* United States v. Jackson, 576 F.2d 749, 757 (8th Cir. 1978) (approving use of "thieves' market value" as proper means of appraising stolen goods or chattels).

62. 18 U.S.C. § 2314 (1994) (describing crime of transportation of stolen property).

potential transgressor of § 2314 within the boundaries of the NSPA. The government must introduce evidence establishing that the defendant knew the items were stolen.[63] The defendant's knowledge of the illegal origin of the trade secret may be inferred from the defendant's behavior.[64]

6. Shortcomings of the NSPA

With the rapid growth of computerized digital technologies, prosecutors often have difficulty obtaining convictions under the NSPA. The intangible nature of many trade secrets has prevented the government from using the NSPA to prosecute trade secret theft because the statute is limited to "goods, wares, merchandise, securities or money," which are tangible property.[65]

For instance, in *United States v. Brown*,[66] the Tenth Circuit considered a prosecution under the NSPA arising out of the alleged theft of a computer program and its source code.[67] Although the stolen program was recovered at the defendant's residence, the prosecution could not prove that the software had been physically removed from plaintiff's place of business.[68] The intangible properties of computer programs led the court to state that for § 2314 to apply "there must be some tangible item taken, however insignificant or valueless it may be, absent the intangible component."[69] Accordingly, the Tenth Circuit held that the "essential ingredient of [§ 2314]—the involvement of physical 'goods, wares, [or] merchandise' that were themselves 'stolen, converted or taken by fraud'—was missing . . . ."[70]

---

63. 18 U.S.C. § 2314 (1994) ("[W]hoever transports . . . goods, wares, merchandise . . . knowing the same to have been stolen.").

64. *See* United States v. Bottone, 365 F.2d 389, 392-93 (2d Cir. 1966) (holding proof of defendant's comings and goings clearly sufficient to suggest he knew he was selling stolen goods).

65. 18 U.S.C. § 2314 (1994) (criminalizing theft of goods, wares, merchandise, securities, or money). *But see* United States v. Riggs, 739 F. Supp. 414, 421 (N.D. Ill. 1990) (applying NSPA's "goods, wares, or merchandise" definition to intangible proprietary business information affixed to some tangible medium such as a piece of paper).

66. *Brown*, 925 F.2d 1301 (affirming dismissal of indictment under NSPA because stolen computer program did not constitute goods under the act).

67. *Id.* at 1302.

68. *Id.* at 1305.

69. *Id.* at 1307 n.14. The court explained that:

> [section] 2314 applies only to physical "goods, wares or merchandise." Purely intellectual property is not within this category. It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible. It is true that the intellectual property involved in the instant case was more nearly "stolen, converted or taken by fraud" in the sense that it was at no time freely presented to the public . . . . We hold that the computer program itself is an intangible intellectual property, and as such, it alone cannot [sic] constitute goods, [or] wares . . . which have been stolen, converted or taken within the meaning of §§ 2314 or 2315.

Id. at 1307-08 (citations omitted).

70. *Id.* at 1307; *cf.* United States v. Lyons, 992 F.2d 1029, 1033 (10th Cir. 1993) (distinguishing *Brown* and allowing sentencing under NSPA because defendant stole both software and hardware).

Additionally, the NSPA does not allow for convictions based solely on attempted theft or receipt of stolen goods.[71]

C. *Trade Secrets Act*

Prior to the EEA, the only federal statute that specifically addressed the theft of trade secrets was the Trade Secrets Act ("TSA"), which prohibits the unauthorized disclosure of confidential information by government employees.[72] Due to two key shortcomings of the TSA, federal prosecutors have more often turned to the NSPA and Mail and Wire Fraud statutes for criminal misappropriation of trade secrets.[73] The first shortcoming is that the TSA does not apply to private sector employees.[74] Additionally, the statute provides only for misdemeanor sanctions, offering few deterrent effects.[75]

The statute has been used to seek the injunction of the government's release of technical data belonging to a government contractor.[76] However, in order for information to be considered "confidential" under the act, the party seeking an injunction must prove that substantial competitive harm would result from the disclosure of the information.[77]

D. *Mail and Wire Fraud Statutes*

The mail and wire fraud statutes[78] provide criminal sanctions for using or attempting to use the mails[79] and wire services to perpetrate

---

71. *See* United States v. Portrait of Wally, 105 F. Supp. 2d 288, 290-91 (S.D.N.Y. 2000) (holding applicable federal common law doctrine that a defendant "cannot be convicted of receiving stolen goods if, before the stolen goods reached the receiver, the goods had been recovered by their owner or his agent, including the police").

72. 18 U.S.C. § 1905 (1994) (criminalizing disclosure of confidential information by an officer or employee of the United States). *See* United States v. Wallington, 889 F.2d 573, 577-78 (5th Cir. 1989) (noting that the Act prohibits the disclosure of information only if the information is confidential, and the federal employee knew the information to be so).

73. *See* Pooley, *supra* note 15, at 179-80.

74. *See* 18 U.S.C. § 1905 (1994) (describing crime of disclosure of confidential information).

75. *See* Pooley, *supra* note 15, at 179; 18 U.S.C. § 1905 (1994) (providing for fines or imprisonment of not more than one year, or both, for disclosure of confidential information by an officer or employee of the United States).

76. *See* Megapulse, Inc. v. Lewis, 672 F.2d 959, 971 (D.C. Cir. 1982) (holding that district court had jurisdiction over suit brought by government contractor seeking injunctive relief to prevent an alleged violation of the Trade Secrets Act).

77. *See* Hercules, Inc. v. Marsh, 659 F. Supp. 849, 855 (W.D.Va. 1987) (holding that directory was not "confidential information" under the Trade Secrets Act because release of information could not cause competitive harm to objecting company).

78. 18 U.S.C. §§ 1341, 1343 (1994) (describing elements of mail or wire fraud crimes).

79. The mail fraud statute is flexible since almost any use of the mail brings one under the statute's prohibitions. *See* Schmuck v. United States, 489 U.S. 705, 710-11 (1989) (holding that use of the mails need not be essential part of scheme but only a "step in [the] plot").

fraud.[80] Unlike the NSPA, these statutes may be applied to the theft of intangible rights,[81] such as trade secrets.[82]

Violation of these statutes does not require proof that the scheme's victims were in fact defrauded,[83] that the defendant gained anything through the scheme,[84] or that there was reliance by the injured party.[85] Rather, violations turn on actual intent to harm the victim.[86]

Appellate courts have upheld convictions under the mail and wire fraud statutes even when there has been no violation of the NSPA.[87] The courts were able to do so because of the statute's broad definition of property.[88] However, under the mail and wire fraud statutes, use of the mail or wire is necessary for there to be a misappropriation.[89]

More recently, the mail and wire fraud statutes have been used to give owners of intellectual property standing to bring a civil claim under the Racketeer Influenced and Corrupt Organizations Act ("RICO").[90]

E. Racketeer Influenced and Corrupt Organizations Act

Criminal sanctions for theft of trade secrets are also available under the RICO.[91]

---

80. For a more extensive discussion of the mail and wire fraud statutes, see the MAIL AND WIRE FRAUD article in this issue. *See* United States v. McNeive, 536 F.2d 1245, 1247 (1976) (construing the statute in light of its manifest purpose to prohibit all attempts to defraud by any form of misrepresentation).

81. 18 U.S.C. § 1346 (1994) (defining "scheme or artifice to defraud" for purposes of mail fraud chapter).

82. *E.g.*, United States v. Henry, 29 F.3d 112, 114 (3d Cir. 1994) (stating that "[t]he statutes cover schemes to defraud another of intangible property, such as confidential business information").

83. *E.g.*, Sunbird Air Serv. v. Beech Aircraft Corp., Civ. A. No. 89-2181-V, 1992 WL 135021, at *4 (D. Kan. May 29, 1992) (rejecting defendant's argument in favor of its motion to dismiss that plaintiff had failed to show victims were actually defrauded).

84. *E.g.*, Ginsburg v. United States, 909 F.2d 982, 991 (7th Cir. 1990), *aff'd*, 909 F.2d 982 (7th Cir. 1990) (finding that "actual success of a scheme to defraud is not required for a mail fraud conviction").

85. *E.g.*, Shaw v. Rolex Watch U.S.A., Inc., 726 F. Supp. 969, 972 (S.D.N.Y.1989) (holding that the mail fraud statute itself does not require a showing of reliance).

86. *See* United States v. Dixon, 536 F.2d 1388, 1399 n.11 (2d Cir. 1976) (requiring that prosecution prove "some actual harm or injury was contemplated"); *see also* United States v. Von Barta, 635 F.2d 999, 1006 n.14 (2d Cir. 1980) (stating that to prove mail fraud, government must show defendant devised scheme with intent to defraud), *overruled on other grounds*, Ingber v. Enzor, 841 F.2d 450 (2d Cir. 1988); *cf.* United States v. Regent Office Supply Co., 421 F.2d 1174, 1181 (2d Cir. 1970) (stating that a showing of an intent to deceive, and even to induce, are not sufficient to constitute fraudulent intent).

87. FEDERAL PROSECUTION MANUAL, *supra* note 8, at 91-92; *see also* Abbott v. United States, 239 F.2d 310, 312, 315 (5th Cir. 1956) (sustaining conviction for use of mails to defraud, even when government failed to prove that defendant caused the interstate transportation of the stolen goods under NSPA).

88. FEDERAL PROSECUTION MANUAL, *supra* note 8, at 92.

89. 18 U.S.C. §§ 1341, 1343 (1994) (describing elements of mail or wire fraud crimes); *see also* Pooley, *supra* note 15, at 186.

90. *E.g.*, Johnson Elec. N. Am. Inc. v. Mabuchi Motor Am. Corp., 98 F. Supp. 2d 480, 488 (S.D.N.Y. 2000) (holding that patent owner had standing to bring civil claim under RICO, based upon mail and wire fraud).

91. 18 U.S.C. §§ 1961-1968 (1994) (criminalizing racketeer influenced and corrupt organizations activities). For a full discussion of §§ 1961-1968, see the RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS article in this issue.

Although many cases brought under RICO are civil actions,[92] the predicate acts necessary to sustain a RICO claim are violations of criminal law. Consequently, the elements of civil and criminal RICO actions are similar. The definition of racketeering activity applicable to the theft of trade secrets includes mail fraud,[93] wire fraud,[94] activity prohibited by the NSPA,[95] and the receipt of stolen property.[96]

Courts faced with trade secret theft charges have reached different conclusions on the definition of a "pattern of racketeering activity" within the meaning of the RICO statute.[97] The Court for the Eastern District of Pennsylvania held that the definition is met by a single scheme of trade secrets misappropriation if there are sufficient allegations of concerted activity directed toward a goal of injuring the plaintiff.[98] In that case, the plaintiff alleged that the defendant's scheme to misappropriate the plaintiff's trade secrets included multiple mailings and telephone conversations in violation of the mail fraud and wire fraud statutes.[99] The court held that this scheme established a pattern of racketeering activity.[100]

In contrast, the Court for the Central District of Illinois held that an isolated criminal episode, though accomplished through several fraudulent acts, does not evidence "threat of continuing criminal activity" so as to give rise to a pattern of racketeering activity within the meaning of RICO.[101]

---

92. *E.g.*, Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1084 (9th Cir. 1986) (recognizing civil RICO claims for trade secret theft but finding injunctive relief not available in the RICO action before the court).

93. 18 U.S.C. § 1341 (1994).

94. 18 U.S.C. § 1343 (1994).

95. 18 U.S.C. § 2314 (1994).

96. 18 U.S.C. § 2315 (1994). One commentator reports that Congress intended the criminal misappropriation of trade secrets to be a crime punishable under RICO, and thinks it likely that this will occur in the future. *See* Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 283 (1999) (speculating that Economic Espionage Act (EAA) was not included in the RICO amendments because the EEA was signed into law three months after RICO).

97. There must be at least two predicate acts of racketeering activity to establish a pattern of racketeering activity. 18 U.S.C. § 1961(5) (1994) (defining "pattern of racketeering activity" for purposes of RICO chapter).

98. S.I. Handling Sys., Inc. v. Heisley, 658 F. Supp. 362, 377 (E.D. Pa. 1986) (finding that multiple fraudulent mailings and telephone conversations established a pattern of racketeering activity).

99. *Id.* at 375 (noting that plaintiff avers that defendants' activities in misappropriating trade secrets were accompanied by mail and telephone communications and that the defendants engaged in interstate transportation of stolen articles).

100. *Id.* at 377 (finding that multiple fraudulent mailings and telephone conversations established a pattern of racketeering activity).

101. Fleet Mgmt. Sys., Inc. v. Archer-Daniels-Midland Co., 627 F. Supp. 550, 559 (C.D. Ill. 1986) (finding that there must be two or more criminal episodes through which the enterprise achieves its illegal goal). The suit alleged that the defendant had misappropriated computer software obtained by license from the plaintiff and then fraudulently misrepresented to plaintiff that it purged the software from its computer system in numerous mail and wire communications over the next two years. *Id.* at 552-53. *See* H.J., Inc. v. Northwestern Bell Tel. Co., 492 U.S. 229, 239 (1989) (relying on RICO's legislative history to conclude that to prove a pattern of racketeering activity a plaintiff or prosecutor must show that the racketeering predicates are related, and that they amount to or pose a threat of continued criminal activity).

F. State Law Provisions

In addition to the various federal statutes criminalizing the misappropriation of trade secrets, all states have enacted criminal statutes applicable to the theft, use, or disclosure of another's trade secrets.[102] These state statutes vary greatly in their scope and sanctions. Some specifically address trade secrets,[103] while others have been interpreted to cover trade secrets despite no explicit reference to them.[104]

---

102. ALA. CODE §§ 13A-8-1 to -23 (1994 & Supp. 2000) (theft and related offenses); ALASKA STAT. §§ 11.46.100-.295 (Michie 2000) (theft and related offenses); ARIZ. REV. STAT. ANN. §§ 13-1801 to -1818 (West. 1989 & Supp. 2000) (theft); ARK. CODE ANN. § 5-36-107 (Michie 1997) (theft of trade secrets); CAL. PENAL CODE § 499c (Deering 1998) (trade secrets, theft or unauthorized copying); COLO. REV. STAT. §§ 7-74-101 to -110 (2000) (uniform trade secrets act); CONN. GEN. STAT. § 53a-124 (1999) (larceny in the third degree, class D felony); DEL. CODE ANN. tit. 11, §§ 841-857 (1995 & Supp. 2000) (theft and related offenses); D.C. CODE ANN. §§ 48-501 to -510 (2000) (trade secrets); FLA. STAT. ANN. § 812.081 (West 2000) (trade secrets, theft); GA. CODE ANN. § 16-8-13 (Harrison Supp. 2000) (theft of trade secrets); HAW. REV. STAT. §§ 708-800 to –8204 (Michie 1999 & Supp. 2000) (offenses against property rights); IDAHO CODE §§ 48-801 to -807 (Michie 1997 & Supp. 2000) (trade secrets act); 720 ILL. COMP. STAT. 5/16-1 to -15 (1999) (theft and related offenses); IND. CODE §§ 24-2-3-1 to -8 (1998) (uniform trade secrets act); IOWA CODE §§ 550.1-.8 (1999) (trade secrets); KAN. STAT. ANN. §§ 60-3320 to -3325 (1994) (trade secrets); KY. REV. STAT. ANN. §§ 365.880-.900 (Michie 1996) (uniform trade secrets act); LA. REV. STAT. ANN. §§ 51.1431-.1439 (West 1987 & Supp. 2001) (uniform trade secrets act); ME. REV. STAT. ANN. tit. 17A, §§ 351-362 (West 1983 & Supp. 2000) (theft-consolidation); MD. CODE ANN., Commercial Law §§ 11-1201 to -1209 (2000) (uniform trade secrets act); MASS. GEN. LAWS ANN. ch. 93, §§ 42-42A (West 1997 & Supp. 2000) (taking of trade secrets), ch. 266, § 60A (stolen trade secrets) (West 2000); MICH. COMP. LAWS ANN. §445.1901-1910 (West Supp. 2000) (uniform trade secrets act); MINN. STAT. § 609.52 (1998 & Supp. 1999) (theft and related crimes); MISS. CODE ANN. §§ 75-26-1 to -19 (2000) (uniform trade secrets act); MO. ANN. STAT. §§ 570.010-.220 (West 1999 & Supp. 2001) (stealing and related offenses); MONT. CODE ANN. §§ 45-6-301 (2000) (theft and related offenses); NEB. REV. STAT. §§ 87-501 to -507 (2000) (trade secrets act); NEV. REV. STAT. §§ 600A.010-.100 (2000) (uniform trade secrets act); N.H. REV. STAT. ANN. §§ 637:1-:11 (1996 & Supp. 2000) (theft); N.J. STAT. ANN. § 2C:20-1 (West 1995 & Supp 2000) (theft and related offenses); N.M. STAT. ANN. §§ 57-3A-1 to -7 (Michie 1996) (uniform trade secrets act); N.Y. PENAL LAW §§ 155.00-.45 (McKinney 1999 & Supp. 2001) (larceny); N.C. GEN. STAT. § 14-75.1 (1999) (larceny of secret technical processes); N.D. CENT. CODE §§ 47-25.1-01 to -08 (1999) (trade secrets); OHIO REV. CODE ANN. §§ 2913.01-.82 (Anderson 1997 & Supp. 2000) (theft and fraud); OKLA. STAT. ANN tit. 21, § 1732 (West 1983 & Supp. 2001) (larceny of trade secrets); OR. REV. STAT §§ 164.015-.140 (1990 & Supp. 1998) (theft and related offenses); 18 PA. CONS. STAT. § 3930 (2000) (theft of trade secrets); R.I. GEN. LAWS § 11-41-1 (2000) (stealing as larceny); S.C. CODE ANN. § 16-13-30 (Law Co-op. 1985 & Supp. 2000) (petit larceny, grand larceny); S.D. CODIFIED LAWS ANN. §§ 22-1-2, 22-30A-1 to -3 (Michie 1998 & Supp. 2000) (theft); TENN. CODE ANN. § 39-14-138 (1997 & Supp. 2000) (theft of trade secrets); TEX. PENAL CODE ANN. § 31.05 (Vernon 1994 & Supp. 2001) (theft of trade secrets); UTAH CODE ANN. §§ 76-6-401, -404 (1999) (theft); VT. STAT. ANN. tit. 13, §§ 2501 to 2502 (1998) (grand larceny); V.A. CODE ANN. § 18.2-95 (Michie 1999 & Supp. 2000) (grand larceny defined; how punished); WASH REV. CODE § 19.108.010-.940 (1998) (uniform trade secrets act); W.VA. CODE ANN. § 61-3-13 (Michie 2000) (grand and petit larceny); WIS. STAT. § 943.205 (1998) (theft of trade secrets); WYO. STAT §§ 6-3-401 to -410, -502 (1999) (larceny and related offenses, crimes against intellectual property). *See generally* Linda B. Samuels & Bryan K. Johnson, *The Uniform Trade Secrets Act: The States' Response*, 24 CREIGHTON L. REV. 49 (1990) (analyzing the Uniform Trade Secrets Act as adopted by the states).

103. For examples of state codes specifically addressing trade secrets, see COLO. REV. STAT. § 7-74-101 (2000) (uniform trade secrets act), FLA. STAT. ANN § 812.081(c) (2000) (defining "trade secret") and OKLA. STAT. ANN tit. 21, § 1732B(c) (West 1983 & Supp. 2000) (same).

104. For examples of state codes using the general theft statutes to cover theft of trade secrets, see N.H. REV. STAT. ANN § 637:2 (1996 & Supp. 2000) ("'Property' means anything of value, including . . . trade secrets, meaning the whole or any portion of any scientific or technical information, design, process, procedure, formula

However, the scope of protection afforded by some state statutes, like the scope of the NSPA, is limited because they apply only to the theft of tangible items.[105]

III. TRADEMARK COUNTERFEITING

Over the past several decades, the theft of trademarks, the symbols or names associated with brand names and products, has become an increasingly lucrative activity for criminals. It also has an equally significant yet opposite effect on the economy, as companies lose an estimated $200 billion a year to criminal commercial trademark counterfeiting.[106]

This Section will cover the various statutes the government uses to protect companies' investments in developing brand names and trademarks. Part A addresses the Trademark Counterfeiting Act of 1984, including its similarities to and differences from its civil counterpart, the Lanham Act. It also reviews defenses to charges of trademark counterfeiting and discusses the FBI's recent campaign against trademark counterfeiting. Part B covers the trademark counterfeiting provisions of RICO and the Money Laundering statute.

A. Trademark Counterfeiting Act

The Trademark Counterfeiting Act ("TCA") criminalizes the intentional trafficking in counterfeit goods or services.[107] To prove a violation of 18 U.S.C. § 2320, the government must establish that: (1) the defendant trafficked or attempted to traffic in goods or services; (2) such trafficking, or the attempt to traffic, was intentional; (3) the defendant used a counterfeit mark on or in connection with such goods or services; and (4) the defendant knew that the mark so used was counterfeit.[108] Counterfeit goods include those that have a mark identical to or

---

or invention which the owner thereof intends to be available only to persons selected by him.") and UTAH CODE ANN. §§ 76-6-401, 76-4-404 (1999) (same).

105. For examples of state codes requiring tangible items to cover theft of trade secrets, see GA. CODE ANN. § 16-8-13 (Supp. 2000) and TENN. CODE ANN § 39-3-1126 (1997 & Supp. 2000).

106. H.R. REP. NO. 104-556, at 2 (1996), *reprinted in* 1996 U.S.C.C.A.N. 1074, 1075 [hereinafter "ANTI-COUNTERFEITING HOUSE REPORT"]; *see* David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 CONN. L. REV. 1, 5 (1998) (discussing the reasons for criminalizing trademark counterfeiting, as well as the elements, defenses, and punishments for the crime).

107. 18 U.S.C. § 2320 (1994 & Supp. IV 1998) (describing the crime of trafficking in counterfeit goods or services); *see* Coblenz, *supra* note 96, at 273-83 (describing the elements of the TCA).

108. United States v. Sultan, 115 F.3d 321, 325 (5th Cir. 1997) (presenting requirements for prosecuting criminal trademark counterfeiting offense); United States v. Torkington, 812 F.2d 1347, 1349 (11th Cir. 1987) (explaining the requirement that a counterfeit mark must be likely to cause confusion among prospective purchasers); *see* Foxworthy v. Custom Tees, 879 F. Supp. 1200, 1212 (N.D. Ga. 1995) (stating that the question is whether the public, not purchaser alone, would be confused by the use of the mark); United States v. Hon, 904 F.2d 803, 804-08 (2d Cir. 1990) (explaining "likelihood of confusion" element includes confusion among general, non-purchasing public, not just actual or prospective purchasers).

substantially indistinguishable from a registered trademark.[109] The government need not prove that the defendant had a criminal intent.[110] The government may also prosecute conspiracies to violate the statute.[111]

1. Defenses

The TCA incorporates the defenses of its civil counterpart, the Lanham Act.[112] These defenses include equitable defenses, such as laches, unclean hands, estoppel, fraud in obtaining the trademark registration, use of mark in violation of antitrust laws, invalid trademark, abandonment, misrepresentation, fair use, unregistered good faith prior use, and registered prior use.[113]

Although the TCA defines a counterfeit mark as one likely to cause confusion,[114] courts have rejected the argument that the actual purchaser should not have been confused or deceived by the counterfeit mark.[115]

2. Penalties

Under the TCA an individual who intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark shall be fined no more than $2 million, imprisoned not more than ten years, or both.[116] For organizations, the fine may be no more than $5 million.[117] Although the statutory punishment is severe, most convictions result in substantially lesser sentences.[118] This is a result of the actual sentencing being determined under the United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.").[119]

3. Operation Counter Copy

In 1997, the FBI launched a nationwide crackdown on criminal trademark and copyright fraud, called Operation "Counter Copy."[120] This operation involved

109. 18 U.S.C. § 2320(e)(1) (1994 & Supp. IV 1998) (defining the term "counterfeit mark"). Because the statute applies only to registered trademarks, common law marks and marks on the supplemental register are not protected. Owners of these marks must rely on civil remedies. *See* Coblenz, *supra* note 96, at 276-77.

110. *See* United States v. Baker, 807 F.2d 427, 428-29 (5th Cir. 1986) (relying on legislative history to show that criminal intent is not required).

111. FEDERAL PROSECUTION MANUAL, *supra* note 8, at 91.

112. 15 U.S.C. § 1051 (1994 & Supp. IV 1998).

113. FEDERAL PROSECUTION MANUAL, *supra* note 8, at 9-3871; 15 U.S.C. §1115 (1994).

114. 18 U.S.C. § 2320(e)(1) (1994 & Supp. IV 1998).

115. For a more in-depth discussion of this argument, see Coblenz, *supra* note 96, at 275.

116. 18 U.S.C. § 2320(a) (1994).

117. 18 U.S.C. § 2320(a) (1994). Repeat offenders, whether individuals or organizations, will receive harsher penalties. 18 U.S.C. § 2320(a) (1994).

118. Coblenz, *supra* note 96, at 282 (discussing convictions in intellectual property).

119. *Id.* at 282 (explain).

120. *See FBI Library—A Report to the American People—Chapter 4: Continuing to Respond to Protect Americans at* http://www.fbi.gov/library/5-year/1993-98/report7.htm (last visited Feb. 27, 2001) (reporting the results of Operation Counter Copy).

eleven FBI field divisions and netted seventeen indictments on federal trademark or copyright violations.[121]

B. RICO and Money Laundering Acts

As with theft of trade secrets, trademark counterfeiting is also illegal under RICO and the money laundering statutes. In 1994, Congress added trademark counterfeiting to the list of unlawful activities under the money laundering statute.[122] Similarly, the Anticounterfeiting Consumer Protection Act of 1996 made trademark and copyright counterfeiting a predicate offense under RICO.[123] Due to frustration with the usefulness of the TCA in providing remedies to trademark counterfeiting, Congress amended the RICO statute to enable the government to counter organized criminal activity as a whole "rather than merely react to each crime the organization commits."[124]

Penalties for violations of the RICO and money laundering statutes are significantly more severe than those under the TCA.[125] While the aforementioned amendments do not expand the definition of conduct that is illegal under the TCA and do not necessarily increase penalties associated with that conduct, their provisions do increase penalties when used to prosecute an organized crime.[126]

Under RICO, fines can be up to twice the gross profits or other proceeds of the activity.[127] Similarly, the penalty for a money laundering violation is a maximum sentence of twenty years and a maximum fine of $500,000 or twice the amount involved in the transaction, whichever is greater.[128]

In addition to fines and imprisonment, the amended RICO statute allows law enforcement officials, including customs agents, to seize counterfeit goods and any "personal or real estate assets connected with the criminal enterprise."[129]

IV. COPYRIGHT

Part A of this section discusses the Copyright Act, emphasizing the elements of

---

121. *Id.*

122. 18 U.S.C. § 1956(c)(7)(D) (1994 & Supp. IV 1998).

123. Pub. L. 104-153, §§ 2, 3, 110 Stat. 1386 (1996) (amending 18 U.S.C. § 1961(1)(B)).

124. ANTICOUNTERFEITING HOUSE REPORT, *supra* note 106, at 3.

125. *See generally* MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT: A TREATISE ON THE LAW OF LITERARY, MUSICAL AND ARTISTIC PROPERTY, AND THE PROTECTION OF IDEAS §15.05[B] (1998) (discussing how Congress broadened the scope of federal criminal copyright liability through amendment of the criminal law).

126. ANTICOUNTERFEITING HOUSE REPORT, *supra* note 106, at 6. The Act increases criminal penalties by providing increased jail time and criminal fines.

127. 18 U.S.C. § 1963(a) (1994).

128. 18 U.S.C. § 1956(a)(1) (1994).

129. ANTICOUNTERFEITING HOUSE REPORT, *supra* note 106, at 6.

the criminal copyright infringement offense and affirmative defenses and the effects of reverse engineering. Parts B through E describe the application of the NSPA, mail and wire fraud statutes, RICO, and the money laundering statutes to criminal copyright infringement. Part F discusses pending legislation to extend copyright protection to computer databases and other collections of information.

A. Copyright Act

The Constitution grants Congress the power to legislate the area of copyright.[130] Criminal copyright infringement, first introduced into federal law in 1897, has traditionally been distinguished from civil violations by the requirement that the conduct be willful and undertaken for profit.[131] The criminal copyright statute has been frequently amended as Congress attempted to strengthen the Act and broaden its scope.[132] The Copyright Act of 1976 relaxed the *mens rea* requirement by requiring only that the infringement be undertaken willfully and for purposes of commercial advantage or private financial gain, rather than "for profit."[133] This lower threshold eases the burden of proving that the transgressor acted "for profit." In 1982, Congress increased the sanctions for criminal infringement, codifying stricter fines for criminal infringement in a separate statute.[134]

Enacted in October 1992, the Copyright Felony Act[135] responded primarily to

---

130. U.S. CONST. art. I, § 8, cl. 8. (Congress shall have the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.")

131. *See* United States v. LaMacchia, 871 F. Supp. 535, 539 (D. Mass. 1994) (requiring commercial exploitation for the criminal offense of software piracy). *See generally* Mary Jane Saunders, *Criminal Copyright Infringement and the Copyright Felony Act*, 71 DENV. U. L. REV. 671, 672 (1994) (discussing requirements for criminal copyright infringement); Robert A. Spanner, *The Brave New World of Criminal Software Infringement Prosecutions*, COMPUTER LAW. 12 No. 11 at 1 (Nov. 1995) (discussing various factors involved in criminal software prosecutions); Kent Walker, *Federal Criminal Remedies for the Theft of Intellectual Property*, 16 HASTINGS COMM. & ENT. L.J. 681 (1994) (presenting U.S. Attorney's view on factors for prosecuting high-technology crime as distinguished from civil infringement).

132. *E.g.*, *LaMacchia*, 871 F. Supp. at 539-40 (discussing history of criminal copyright law); Saunders, *supra* note 131, at 679-80 (describing criminal copyright statute).

133. Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended at 17 U.S.C. § 506(a) (1994)). The 1976 Act changed the nature of the criminal copyright system by substituting a single federal statutory copyright for dual copyright codes. Federal law now preempts the field of copyrights. 17 U.S.C. §301(a) (1994) (stating that the federal statute preempts state law); FEDERAL PROSECUTION MANUAL, *supra* note 8, at 9-3831.

134. Act of May 24, 1982, Pub. L. No. 97-180, 96 Stat. 91 (codified at 18 U.S.C. § 2319 (1994)). While certain acts of criminal copyright infringement were defined as felonies, most infringements remained misdemeanor offenses. 18 U.S.C. § 2319 (1994 & Supp. IV 1998). The criminal copyright law supplements private civil remedies by punishing conduct that undermines the integrity of the copyright system despite the conduct's inability to rise to the level of civil action. 17 U.S.C. §§ 506(c)-(e) (1996); FEDERAL PROSECUTION MANUAL, *supra* note 8, at 9-3831.

135. Pub. L. No. 102-561, 106 Stat. 4233 (codified as amended at 18 U.S.C. § 2319(b)-(c) (1994)). For an in-depth discussion of the legislative history of the Copyright Felony Act, see Saunders, *supra* note 131, at 679-80.

the growing problem of large-scale computer software piracy.[136] Prior to the passage of the Act, only unauthorized copying of sound recordings, motion pictures, or audiovisual works was a federal felony.[137] The Act amended 18 U.S.C. § 2319 by broadening its coverage to protect all copyrighted works and lowering the numerical and monetary thresholds for felony sanctions.[138] The *mens rea* requirement remained unchanged.[139]

Finally, in December 1997, the No Electronic Theft Act ("NET Act") was enacted.[140] This Act modified criminal copyright statutes by removing the financial gain requirement and making illegal reproduction or distribution of copyrighted materials a federal crime.[141] The government need only prove either that the infringer acted for financial gain, or that she reproduced or distributed one or more copies of copyrighted works that have a total retail value of $1,000.[142] Thus, the criminal copyright statute now reaches those infringers who act solely to harm another or for non-financial gratification.[143]

Because a copyright cannot exist before an expression is captured in a fixed,

---

136. For a discussion of what constitutes copyright infringement of computer software, compare MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993) (asserting that "copying" occurs even when a copyrighted program is temporarily loaded into a computer's RAM (random access memory)), with Stenograph, L.L.C. v. Bossard Assocs., Inc., 144 F.3d 96, 100 (D.C. Cir. 1998) (holding that defendant who loaded validly copyrighted software onto computer without owner's permission and used software as designed had copied and infringed copyright of software). However, the Court's explanation in *MAI Sys.* has been criticized for "failing to recognize the distinction between ownership of a copyright, which can be licensed, and ownership of copies of the copyrighted software." DSC Communications Corp. v. Pulse Communications, Inc., 170 F.3d 1354, 1360 (Fed. Cir. 1999) (finding telephone companies that used manufacturer's copyrighted software were not necessarily "owners" of copies of that software). *See* Applied Info. Management, Inc. v. Icart, 976 F. Supp. 149, 153-154 (E.D.N.Y. 1997) (discussing factors used to determine whether a licensee owns a copy of a computer program); Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1368-73 (N.D. Cal. 1995) (holding internet provider not liable for copyrighted material loaded onto computer by third party when provider lacked knowledge material was copyrighted).

137. For a comparison of the old and revised statute, *see* Carl H. Loewenson, Jr. & Marta E. Nelson, *Congress Toughens Criminal Copyright Law*, N.Y. L.J., Nov. 13, 1992, at 1 (suggesting that companies should establish and publicize internal policies against unauthorized software copying, in light of statutory developments).

138. 18 U.S.C. § 2319 (1994 & Supp. IV 1998). Under the 1992 Act, felony sanctions applied to ten or more copies made within a 180-day period, with a retail value more than $2,500. 18 U.S.C. § 2319(b) (1994 & Supp. IV 1998).

139. 17 U.S.C. § 506(a) (1994).

140. No Electronic Theft (NET) Act of 1997, Pub. L. No. 105-147, 111 Stat. 2678 (1997).

141. *See* Michael Coblenz, *Intellectual Property Crimes*, 9 ALB. L.J. SCI. & TECH. 235, 249 (1999) (commenting on history of criminal copyright statutes). The NET Act is the centerpiece of DOJ efforts to combat intellectual property infringement, especially in the New York-New Jersey area, California, Massachusetts and the Southern District of Florida. Deputy Attorney General Eric H. Holder, Jr., Press Conference Announcing the Intellectual Property Rights Initiative, *available at* http://www.usdoj.gov/criminal/cybercrime/dagipini.htm (July 23, 1999) (detailing a new interdepartmental commitment).

142. NET Act of 1997, § 2(b) (amending 17 U.S.C. § 506(a)) (1997).

143. H.R. REP. NO. 105-339, at 3-5 (1997) (describing legislative justifications for removal of "financial gain" requirement for criminal copyright infringement). *But see* Wendy M. Grossman, *Cyber View: Downloading As a Crime*, SCI. AM., Mar. 1998, at 37 (criticizing NET Act for absence of fair-use exemptions).

tangible medium,[144] musical or dramatic performances may not be protected by copyright until they are recorded. An artist's interest in his performance is protected against unauthorized recording by 18 U.S.C. § 2319A. This section, added in December 1994, provides for both fines and imprisonment for bootlegging, recording, reproduction, transmission, and distribution (whether for sale or not) of live musical performances.[145]

1. Elements of the Offense

The government has the burden of proving four elements in a criminal prosecution for copyright infringement under 17 U.S.C. § 506: (1) that a valid copyright exists; (2) infringement of that copyright; (3) that the violation was performed willfully; and (4) either (a) that the infringement was for purposes of commercial advantage or private financial gain, or (b) that the infringer reproduced or distributed, during any 180-day period, one or more copies or phonorecords of one or more copyrighted works, with a total retail value of more than $1,000.[146] The elements of a § 2319A violation are similar.[147]

a. Existence of a Valid Copyright

The first element of the criminal copyright offense is the existence of a valid copyright.[148] A certificate of registration issued within five years after the work's first publication constitutes prima facie evidence of a valid copyright.[149] Presentation of the certificate shifts the burden to the defendant, who can then challenge it

144. 17 U.S.C. 102(a) (1994) (excluding ideas, procedures, and concepts from copyright protection).

145. The section also provides for forfeiture, seizure, and destruction of such unauthorized recordings, and encompasses the distribution in the United States of copies of unauthorized recordings made outside the United States. 18 U.S.C. § 2319A(b)-(c) (1994 & Supp. IV 1998).

146. 17 U.S.C. § 506(c)-(d) (1994 & Supp V 1999). Section 506(c) now refers to Fraudulent Copyright Notice; § 506(d) to Fraudulent Removal of Copyright Notice. Evidence of reproduction or distribution of a copyrighted work, by itself, is not sufficient to establish a willful infringement under subsection (a). 17 U.S.C. § 506(a) (1994 and Supp. V 1999).

147. 18 U.S.C. § 2319A(a) (1994). Section 2319A(a) states in relevant part:

> [w]hoever, without the consent of the performer or performers involved, knowingly and for purposes of commercial advantage or private financial gain— (1) fixes the sounds or sounds and images of a live musical performance in a copy or phonorecord, or reproduces copies or phonorecords of such a performance from an unauthorized fixation; (2) transmits or otherwise communicates to the public the sounds or sounds and images of a live musical performance; or (3) distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or traffics in any copy or phonorecord fixed as described in paragraph (1), regardless of whether the fixations occurred in the United States[.]

18 U.S.C. § 2319A(a) (1994).

148. CRIMINAL RESOURCE MANUAL No. 1848, *available in* the JUSTICE MANUAL (2d ed.), *available at* www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9 /crm00000.htm. [hereinafter RESOURCE MANUAL].

149. 17 U.S.C. § 410(c); United States v. Taxe, 540 F.2d 961, 966 (9th Cir. 1976) (holding that the certificate establishes the date of copyright unless contrary evidence is presented).

by showing that the copyright was obtained by fraud that the registration certificate is not genuine, or that the work cannot be copyrighted.[150]

b. Infringement

Infringement of a valid copyright is the threshold requirement for both criminal and civil copyright infringement cases.[151] The copyright infringement can be proven by direct evidence[152] or by indirect evidence showing that the defendant had access to the copyrighted work and that the alleged copy is "substantially similar" in idea and in expression of idea.[153] The substantial similarity test is a two step analysis that requires: (1) a showing of substantial similarity in the basic ideas involved, established by focusing on specific "extrinsic" criteria, such as the type of work involved, the materials used, the subject matter, and the setting for the subject; and (2) a showing that the defendant's alleged copy expresses the same "intrinsic" substance and value as the original work.[154]

As an alternative to the substantial similarity test, courts may employ the "virtual identity" standard, or they may apply both. Whereas the substantial similarity test allows the potentially infringing work to be broken down into protected and unprotected elements that are then compared to elements of the

150. *E.g.*, United States v. Backer, 134 F.2d 533, 535 (2d Cir. 1943) (examining the validity of the certificate when challenged); Durham Indus. v. Tomy Corp., 630 F.2d 905, 908-09 (2d Cir. 1980) (invalidating a copyright for lack of origination, despite certificate of registration).

151. RESOURCE MANUAL, *supra* note 148, at 1849 ("Once the validity of the copyright has been established, the government must then prove that the defendant infringed upon that right.").

152. *E.g.*, United States v. Larracuente, 952 F.2d 672, 673 (2d Cir. 1992) (holding infringement can be proven by evidence of a valid copyright plus copying); United States v. One Sharp Photocopier, 771 F. Supp. 980, 984 (D. Minn. 1991) (holding that government met burden of proving probable cause to make forfeiture of software duplicating machine appropriate).

153. *See* Apple Computer, Inc. v. Microsoft Corp., 35 F.3d 1435, 1442 (9th Cir. 1994) (upholding use of circumstantial evidence of copying as sufficient because direct evidence is usually not available); Transwestern Publ'g Co. v. Multimedia Mktg. Assoc., 133 F.3d 773, 775 (10th Cir. 1998) (upholding finding of no infringement where the two directories at issue possessed several significant differences); United States v. Cohen, 946 F.2d 430, 433-34 (6th Cir. 1991) (upholding conviction of criminal copyright infringement supported by circumstantial evidence); United States v. O'Reilly, 794 F.2d 613, 615 (11th Cir. 1987) (noting that the copy need not be identical in all respects); *see also* Saunders, *supra* note 131, at 682-85 (discussing methods of proving first element of offense). Some circuits apply the inverse ratio rule, which requires a lesser showing of similarity when the showing of access is high. Three Boys Music Corp. v. Bolton, 212 F.3d 477, 485 (9th Cir. 2000) (noting that plaintiff can prove infringement even without evidence of access if works are "strikingly similar"); Selle v. Gibb, 741 F.2d 896, 904 n.4 (7th Cir. 1984) (stating that when there is virtually no evidence of access, considerable similarity is necessary). However, the inverse ratio rule has yet to be applied in the criminal context.

154. *See* Smith v. Jackson, 84 F.3d 1213, 1218 (9th Cir. 1996) (discussing extrinsic and intrinsic prongs of substantial similarity test). The extrinsic test is based on external, objective criteria as to whether the two works share a similarity of ideas and expression. The intrinsic test employs a subjective standard: whether an ordinary, reasonable observer would find a substantial similarity of expression of the shared idea. *Id.*; *see also* Ford Motor Co. v. Summit Motor Prod., 930 F.2d 277, 291 (3d Cir. 1991) (noting the extrinsic test involves expert testimony while intrinsic analysis utilizes the lay perspective).

original work, the virtual identity test looks at the two works as a whole to determine if they are virtually identical.[155]

Some courts allow the allegedly infringing work to be separated from the non infringing work by filtering out copyright-protected from non-protected components.[156]

The copyright infringement element may be established even though the person distributing the infringing work did not produce the copies herself.[157]

c. Willfulness

The third element of the criminal copyright offense is willfulness.[158] A majority of the courts have interpreted the term "willfully" to mean that the government must show that the defendant specifically intended to violate the copyright law.[159] The Second Circuit has taken a different view, holding that "willfulness" requires only an intent to copy, rather than intent to infringe.[160]

---

155. For a comparison of the virtual identity and substantial similarity tests for infringement, *see Apple Computer*, 35 F.3d at 1442-43. Virtual identity may be a more useful standard for determining infringement in the case of "reverse engineering," whereby programmers dissect legally obtained software and then instruct a third set of programmers on functional requirements of the software, thus creating "virtually identical" software programs which are not exact copies of one another. *See* McCulloch v. Albert E. Price, Inc., 823 F.2d 316 (9th Cir. 1996) (holding that it is not necessary under the substantial similarity test to determine the scope of copyright protection or to identify the idea behind a copyright holder's work).

156. *See Apple Computer*, 35 F.3d at 1442-47 (describing court's proper dissection of the Microsoft graphical user interface (GUI) into protected and unprotected components for purposes of evaluating substantial similarity); Lotus Dev. Corp. v. Paperback Software Int'l, 740 F. Supp. 37, 67 (D. Mass. 1990) (stating that only those components that are copyrightable should be analyzed). *But see* Atari Games Corp. v. Oman, 888 F.2d 878, 882-83 (D.C. Cir. 1989) (declaring that sequence of frames in computer game must be analyzed as a whole and not on a component-by-component basis).

157. *E.g.*, United States v. Moore, 604 F.2d 1228, 1234 n.4 (9th Cir. 1979) (stating that because the government established criminal infringement by proving that defendants distributed copyrighted sound recordings, it was not necessary to prove defendants also reproduced infringing recordings).

158. 17 U.S.C. § 506. Congress intended to permit courts to continue defining the term. H.R. Rep. No. 102-997, pt. 4-5, at 4 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3573 (recognizing, but allowing, the lack of federal uniformity).

159. United States v. Heilman, 614 F.2d 1133, 1137-38 (7th Cir. 1980) (finding willful infringement of copyright when defendant knew material was copyrighted); *see* United States v. Moran, 757 F. Supp. 1046, 1050-52 (D. Neb. 1991) (contrasting willfulness in civil and criminal contexts); Saunders, *supra* note 131, at 688 (comparing majority and minority rules). *See generally* Coblenz, *supra* note 141, at 248 (explaining requirements for intent element); *cf.* United States v. Manzer, 69 F.3d 222, 227-28 (8th Cir. 1995) (holding that copyright notice on plastic module containing copyrighted software was sufficient to put defendant on notice for purpose of willfulness).

160. *See* United States v. Backer, 134 F.2d 533, 535 (2d Cir. 1943) (holding that defendant guilty of infringement even though he intended to make copies closely resembling copyrighted work without causing "copyright trouble"); Saunders, *supra* note 131, at 688 (comparing majority and minority rules). *But see* Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L.Q. 835, 877 (1999) (discussing willfulness requirement and questioning whether the Second Circuit has truly articulated a different view).

d. Financial Gain or Threshold Violation

Congress modified the fourth element of the criminal copyright offense to require the government to prove either intent to obtain financial gain or that one or more copies were reproduced or distributed with a total value of more than $1,000.[161] Thus, the infringer need not intend to realize financial gain to be found guilty.

Furthermore, a defendant need not actually realize commercial advantage or private financial gain for a court to find intent; it is enough that the defendant commits the violation for the purpose of financial gain.[162] Profit may be sought either through monetary transactions or through bartering for other protected materials.[163]

2. Defenses

While the criminal copyright infringement statute does not provide explicit statutory defenses, civil defenses are available.[164] One common defense is the "first sale" doctrine.[165] According to the doctrine, upon sale, the author conveys title of the particular copy of a copyrighted work and abolishes his right to restrict subsequent sales of that particular copy.[166] The purchaser does not, however, gain the right to reproduce and distribute additional copies of the work.[167] Further, the benefits of the doctrine do not extend to rental or loan arrangements.[168] The first sale defense applies to copies that were imported into the United States.[169]

---

161. Pub. L. No. 105-147, § 2(b), 111 Stat. 2678 (1997) (amending 17 U.S.C. § 506(a)).

162. *See* United States v. Cross, 816 F.2d 297, 301 (holding fact that copies were not sold for money irrelevant where hope of gain existed) (citing *Moore*, 604 F.2d at 1235); United States v. Shabazz, 724 F.2d 1536, 1540 (11th Cir. 1984) (holding that defendant who "sold pirated tapes, solicited wholesale customers and shipped large quantities of tapes out of state" had intent to make profit); United States v. Wise, 550 F.2d 1180, 1195 (9th Cir. 1977) (holding that whether gain was realized is irrelevant).

163. H.R. REP. 105-339 (1997).

164. *See* Coblenz, *supra* note 141, at 251 (explaining civil defenses available for copyright infringement).

165. 17 U.S.C. § 109 (1994). Section 109(a) provides: "the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy . . . ." *Id.*

166. *Id.* A lawful original sale of the work is necessary for the first sale doctrine to apply. *See* United States v. Cohen, 946 F.2d 430, 434 (6th Cir. 1991) (recognizing that individuals can rent or sell a copy of copyrighted work if lawfully obtained by that individual); United States v. Drum, 733 F.2d 1503, 1507 (11th Cir. 1984) (stating that government may prove absence of first sale by evidence of source of the recordings or by evidence that recordings were never authorized); Microsoft Corp. v. Harmony Computers & Elecs., Inc., 846 F. Supp. 208, 213 (E.D.N.Y. 1994) (holding that defendant who obtained copyrighted product from a licensee could not invoke first sale doctrine to avoid liability for subsequent sale). *But see* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453-55 (7th Cir. 1996) (holding "shrink-wrap" license, a package label limiting use of work, enforceable under state contract law while not creating exclusive rights otherwise preempted by Copyright Act).

167. 17 U.S.C. § 109 (1994). These rights are reserved for copyright owners in 17 U.S.C. § (1994).

168. 17 U.S.C. § 109(d) (1994).

169. Quality King Distribs., Inc. v. L'anza Research Int'l, Inc. 523 U.S. 135, 152 (1998). ("The whole point of the first sale doctrine is that once the copyright owner places a copyrighted item in the stream of commerce by selling it, he has exhausted his exclusive statutory right to control its distribution."). However, the Supreme Court

Other defenses include fair use, parody, and *scènes à faire*. Fair use is an "equitable rule of reason,"[170] requiring the balancing of factors to protect the copyright owner while still promoting the purpose behind copyright laws, namely fostering creativity.[171] A defense of fair use as parody[172] requires an examination of the expressive intent of the infringing work to determine if it has a "critical bearing on the substance or style" of the original work.[173] A *scènes à faire* defense[174] relies on the fact that the infringing elements are so common or integral to the type of work being produced that it is impossible to create works in the same category without those elements, and therefore, they may not be protected by copyright.[175]

3. *Penalties*

At first, the maximum penalty imposed under 18 U.S.C. § 2319(b)(3) was one

---

did not address "cases in which the allegedly infringing imports were manufactured abroad." *Id.* at 154 (Ginsburg, J., concurring). *See generally* Joan Biskupic, *Court Lets Discounters Keep Selling U.S.-made Goods They Buy Overseas*, WASH. POST, Mar. 10, 1998, at A7 (noting concerns by U.S. manufacturers, including software and recording industries, that this decision would legitimize the multi-billion dollar "gray market" industry which undercuts their domestic marketing).

170. Sony Corp. of Am. v. Universal Studios, Inc., 464 U.S. 417, 448 (1984) (holding that manufacture and sale of VCR's did not constitute contributory infringement). The Supreme Court has noted that "since the doctrine is an equitable rule of reason, no generally applicable definition is possible, and each case raising the question must be decided on its own facts." *Id.* at 448 n. 31 (quoting H.R. REP. No. 94-146 at 65-66, *reprinted in* 1976 U.S.C.C.A.N. 5680).

171. *See* Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc., 109 F.3d 1394, 1399 (9th Cir. 1997) (applying four elements of fair use doctrine to parody of Dr. Seuss poetry). The four factors to be considered by a court to determine if the fair use defense exists are (1) purpose and character of the accused use; (2) nature of copyrighted work; (3) importance of the portion used in relation to the copyrighted work as a whole; (4) the effect of the accused use on the potential market for or value of the copyrighted work. 17 U.S.C. §107 (1994). Congress viewed these factors as guidelines to be weighed in light of the objectives of copyright law, rather than as a definitive test. *Dr. Seuss*, 109 F.3d at 1399.

172. *E.g.*, Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579-80 (1994) (finding that song which would otherwise infringe on copyright was fair use as parody); Leibovitz v. Paramount Pictures Corp., 948 F. Supp. 1214, 1221 (S.D.N.Y. 1996), *aff'd*, 137 F.3d 109 (2d Cir. 1998) (rejecting claim that all commercial use of protected elements of copyrighted work is de facto infringement and holding that movie ad that parodied copyrighted photograph did not infringe on the copyrighted work).

173. *Campbell*, 510 U.S. at 580. "For the purpose of copyright law . . . the heart of any parodist's claim to quote from existing material, is the use of some elements of a prior author's composition to create a new one that, at least in part, comments on that author's works." *Id.* See also Leibovitz, 948 F. Supp. at 1220 (noting that a work must comment upon or criticize the copyrighted work to qualify as a parody).

174. *See* Smith v. Jackson, 84 F.3d 1213, 1219 (9th Cir. 1996) (noting that *scènes à faire* defense turns on whether alleged copying can be explained by the common presence of same motives with a particular field of work); Atari, Inc. v. North Am. Philips Consumer Elecs. Corp., 672 F.2d 607, 616-19 (7th Cir. 1982) (stating that *scènes à faire* refers to "incidents, characters, or settings" that are standard in the treatment of a given subject (quoting Alexander v. Haley, 460 F. Supp. 40, 45 (S.D.N.Y. 1978))).

175. *See* North Am. Bear Co., Inc. v. Carson Pirie Scott & Co., No. 91 C 4550, 1991 WL 259031, * 3 (N.D. Ill. Nov. 27, 1991) (noting that protecting expression of a general idea would bestow a monopoly of the idea upon copyright owner); McDonald v. Multimedia Entertainment, Inc., 20 U.S.P.Q. 2d (BNA) 1372, 1375 (S.D.N.Y. 1991) (finding that single musical note or three-note sequence is too common to receive protection). *See generally* WILLIAM PATRY, THE FAIR USE PRIVILEGE IN COPYRIGHT LAW 63-64, 465-66 (1985).

year imprisonment, $25,000 fine, or both. Congress soon realized this penalty did not provide an adequate deterrent to those engaged in the business of record and tape piracy. Consequently, Congress provided specific enhanced penalties for copyright infringement involving sound recordings, phonorecords, motion pictures, and audiovisual works.[176] In 1992, Congress again altered the penalties for criminal copyright infringement.[177] The basic offense now carries a maximum sentence of up to five years in prison.[178] Any subsequent offense increases the penalty to up to ten years of imprisonment.[179] All other violations are misdemeanors.[180] In addition, the court may order the forfeiture of infringing copies and equipment used in their manufacture.[181]

The Copyright Damages Improvement Act of 1999 was enacted to compel changes in the Sentencing Guidelines, which further impact statutory penalties.[182] The new Guidelines increase the base offense level to eight.[183] Enhancement is permitted for offenses involving manufacture, importation, or uploading of infringing works.[184] The offense level is further increased if the infringement amount exceeds $2,000.[185]

4. Reverse Engineering

Because only the expression of an idea, and not the idea itself, may be protected under copyright, a copy made for the purposes of reverse engineering may represent a fair use exception to the copyright doctrine. Reverse engineering is the process, now most often applied to software, where a protected work is broken down to its component and non-protected parts, from which a similar, competitive but non-copy product may be created.[186] When determining whether non-literal elements[187] of computer programs are substantially similar in copyright infringe-

---

176. FEDERAL PROSECUTION MANUAL, *supra* note 8, at 9-1549. Currently, as the number of infringing copies increases, so does the maximum sentence imposed.

177. *Id.*

178. 18 U.S.C. § 2319(b)(1) (1994). The penalty is for the "reproduction or distribution during any 180-day period, of at least 10 copies . . . with a retail value of less than $2500." *Id.*

179. 18 U.S.C. § 2319(b)(2) (1994).

180. 18 U.S.C. § 2319(b)(3) (1994).

181. 17 U.S.C. § 506(b).

182. Pub. L. 106-160, § 3, Dec. 9, 1999, 113 Stat. 1774, provides that: "Within 120 days after the date of enactment of this Act . . . the Commission shall promulgate emergency guideline amendments to implement § 2(g) of the No Electronic Theft ("NET") Act."

183. U.S. SENTENCING GUIDELINES MANUAL § 2B5.3 (1998 & Supp. 1999) [hereinafter U.S.S.G. MANUAL].

184. U.S.S.G. MANUAL § 2B5.3(b)(2) (1998) (increasing the base by two levels or to twelve, whichever is higher).

185. U.S.S.G. MANUAL § 2B5.3(b)(1) (1998) (noting that the retail value depends on the value of the infringed item, not on the offensive copy).

186. PATRY, *supra* note 175, at 468-77.

187. The literal elements of a computer program are the source and object code. Nonliteral elements include a program's structure, sequence and organization expressed through "general flow charts . . . organization of inter-modular relationships, parameter lists, and macros," which are produced by the code's interaction with

ment cases, courts apply the Abstraction-Filtration-Comparison method.[188] First, the court breaks down the allegedly infringing program into its constituent structural parts and isolates each level of abstraction contained within that structure.[189] Then the court sifts protected expression from non-protected material.[190] Finally, the court compares the material structure of the allegedly infringing program with the protected core of the original work.[191] While reverse engineering is often at issue in trade secret violations, the Abstraction-Filtration-Comparison analysis has also been applied to copyright violations in software cases.[192]

B. National Stolen Property Act

In the past, courts extended the protections of the NSPA to copyrighted goods.[193] This extension was effectively overruled when the Supreme Court, in *Dowling v. United States*,[194] held that the NSPA[195] does not prohibit the interstate transportation of goods infringing on another's copyright.[196] Because there had been no actual physical removal or theft of the property, the Court held that the Act's requirement that the goods be "stolen, converted or taken by fraud" was not met.

---

hardware and operating programs. Computer Assoc. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 702 (2d Cir. 1992) (holding that the nonliteral elements of the examined works were not substantially similar).

188. *E.g.*, Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823, 834 (10th Cir. 1993) (adopting the test and remanding for application).

189. *E.g.*, Mitek Holdings, Inc. v. Arce Eng'g Co. 89 F.3d 1548, 1555 (11th Cir. 1996) (holding that a list of allegedly protected elements provided by the plaintiff rendered abstraction unnecessary).

190. Under the filtration prong, the court removes elements that are: (1) taken from the public domain; (2) dictated by efficiency; or (3) required by factors external to the program, such as compatibility with other programs, demands of the industry served, and mechanical specifications of the computers which will run the program. *See Computer Assoc. Int'l.*, 982 F.2d at 707 (noting that a monopoly will not be granted where there is effectively only one way to express an idea).

191. *E.g., Computer Assoc. Int'l.*, 982 F.2d at 710-11 (holding that nonliteral elements of compatibility of rewritten computer programs were not substantially similar).

192. *E.g.*, Sega Enterprises, Ltd. v. Accolade, Inc., 977 F.2d 1510, 1518 (9th Cir. 1993) (holding that reverse engineering undertaken for legitimate purpose is "as a matter of law a fair use of the copyrighted work"); *but see* Atari Games Corp. v. Nintendo of Am., Inc., 975 F.2d 832, 843 (Fed. Cir. 1992) ("The fair use reproductions of a computer program must not exceed what is necessary to understand the unprotected elements of the work.").

193. *E.g.*, United States v. Belmont, 715 F.2d 459, 461 (9th Cir. 1983) (applying Act to interstate transportation of "off the air" copies of motion pictures); United States v. Drebin, 557 F.2d 1316, 1328 (9th Cir. 1977) (holding that copies of copyrighted motion pictures constitute goods, wares, or merchandise, and thus fall within the meaning of the Act).

194. 473 U.S. 207 (1985).

195. 18 U.S.C. § 2314 (1994).

196. *Dowling*, 473 U.S. at 216. The defendants in *Dowling* taped, without authorization, commercially unreleased Elvis Presley performances and produced record albums. *Id.* at 214. The Supreme Court, citing the Copyright Act, concluded that Congress had not intended for the National Stolen Property Act to apply to copyright infringement. *Id.* at 221-27.

C. Mail and Wire Fraud Statutes

The mail and wire fraud statutes[197] impose criminal penalties on those who utilize the mail or wires to defraud others through copyright infringement.[198] To establish a violation of either statute, the government must meet the same criteria as set out in Section II.D. of this Article. Additionally, one district court has held that federal copyright law does "not necessarily preempt other proprietary rights."[199] Because the defendants in that prosecution would not profit from their infringement until transmission by wire had occurred, this court held that remedies were not limited to those provided by the copyright statute, and that prosecution under the wire fraud statute was acceptable.[200]

D. Racketeer Influenced and Corrupt Organizations Act

As with theft of trade secrets and trademark counterfeiting, RICO[201] claims can be brought for copyright infringement if the infringing acts continue over a period of time and relate to each other in a common plan created by the violators with the intent to defraud.[202] The Anticounterfeiting Consumer Protection Act of 1996 made copyright counterfeiting a racketeering activity under RICO.[203]

E. Money Laundering Act

18 U.S.C. § 1956, the money laundering statute, defines money laundering, and includes the receipt of proceeds from trafficking in counterfeit goods or goods infringing on copyright as specified unlawful activities.[204]

F. The Database Protection Bill

In October 1997, Representative Howard Coble introduced the Collections of

197. 18 U.S.C. §§ 1341, 1343 (1994).

198. *See* United States v. Manzer, 69 F.3d 222, 229 (8th Cir. 1995) (using mail and telephone to sell unauthorized satellite decryption equipment); United States v. Shultz, 482 F.2d 1179, 1182 (6th Cir. 1973) (using mails to sell counterfeit sound recordings); Cooper v. United States, 639 F. Supp. 176, 180 (M.D. Fla. 1986) (using wires, specifically telephones, to distribute thousands of pirated sound recordings).

199. United States v. Wang, 898 F. Supp. 758, 760 (D. Colo. 1995).

200. *Id.* (holding that wire fraud statute could be applied).

201. 18 U.S.C. §§ 1961-1968 (1994).

202. *See supra* Section II.E. of this Article (discussing RICO); *see also* United States v. Drum, 733 F.2d 1503, 1506 (11th Cir. 1981) (applying RICO to charges arising out of sound recording copyright infringement business); United States v. Sam Goody, Inc., 506 F. Supp. 380 (E.D.N.Y. 1981) (holding repeat copyright infringers who satisfied RICO criteria could not avoid prosecution on the grounds they were not members of organized crime because RICO applies to any enterprise, both legal and illegal).

203. Pub. L. 104-153, § 3, 110 Stat. 1386 (1996) (amending 18 U.S.C. § 1961(1)).

204. 18 U.S.C. § 1956(c)(7)(D) (1994 & Supp. IV 1998). For further discussion of this statute, and its applicability to copyright law, see the MONEY LAUNDERING article in this issue.

Information Antipiracy Act,[205] which would provide criminal penalties for the use of all or part of a "collection of information gathered, organized, or maintained by another person through the investment of substantial monetary or other resources."[206] A violation of the proposed law would require willful action, that the act be undertaken for commercial or financial advantage—whether direct or indirect—and that the perpetrator cause loss or damage to the compiler of the information.[207] The Act passed the House on May 19, 1998.[208] The Act was introduced into the Senate on July 10, 1998, but was not enacted.[209]

On Jan. 19, 1999, Coble reintroduced the bill, as H.R. 354,[210] with two new additions. H.R. 354 adds fair use provisions for educational, research, and scientific uses, and also clarifies that information contained in a database cannot be protected for more than fifteen years.[211] However, research officials and administrative officials criticize the Bill for having an unnecessarily broad scope of protection, as well as inadequate provisions for ensuring free access to government databases.[212]

V. ONLINE SERVERS: CRIMINAL VIOLATIONS OF THE COPYRIGHT FELONY ACT

This section outlines the application of the Copyright Act to on-line activities. Part A discusses criminal liability of individuals who transfer files in cyberspace, emphasizing conduct that constitutes infringement, the financial gain/threshold requirement and the first sale doctrine. Part B addresses Internet Service Providers' liability for activities on their networks.

A. Criminal Liability

A criminal violation of the Copyright Act occurs when one willfully reproduces or publicly distributes any kind of copyrighted work.[213] The Copyright Act of

205. H.R. 2652, 105th Cong. (1997). The Bill essentially created additional protection for database providers against database piracy by adding a new Chapter 14 to 17 U.S.C. § 101. *See Collections of Information Bill Reintroduced; Fair Use, Time Limitation Provisions Included*, [Jan.-June] ELEC. COMMERCE & LAW REP. (B.N.A.) Vol. 4, No. 4 (Jan. 27, 1999) (discussing new provisions to bill).

206. *Id.* at § 1201; 143 CONG. REC. E2000 (daily ed. Oct. 9, 1997) (introductory remarks of Rep. Coble).

207. H.R. 2652, 105th Cong. § 1207(a).

208. 144 Cong. Rec. H3398-01.

209. 1997 US S.B. 2291 (SN).

210. H.R. 354, 106th Cong. (1999).

211. *See Collections of Information Bill*, *supra* note 205 (discussing new provisions to H.R. 354).

212. *See Database Bill is Still Flawed, Overbroad, Adminstration, Researchers Tell Panel*, [Jan.-June] ELEC. COMMERCE & LAW REP. (B.N.A.) Vol. 4, No. 12 (Mar. 24, 1999) (discussing flaws in database bill).

213. For a general overview of the elements of the criminal copyright offense, see *supra* Section IV.A.1. of this Article.

1976[214] protects the use of the text files,[215] image files,[216] and sound files[217] on the Internet.[218] Criminal copyright infringement that: (1) is facilitated by or achieved through the Internet, and (2) meets the statutorily prescribed number of copies or dollar value may lead to felony prosecution.[219] Systematic, unauthorized trading in copyrighted works on the Internet—whether sound, picture, or text files, or unlicensed software distribution—potentially qualifies as trafficking in counterfeit works.[220] The protection that is, and should be afforded digital works is in dispute. Commentators have argued that several areas of the Act should be amended in light of the growing use of cyberspace.[221] Two issues that are particularly

214. Pub. L. No. 94-553, § 101, 90 Stat. 2541-2589 (codified as amended in scattered sections of 17 U.S.C.).

215. 17 U.S.C. § 101 (1994). The 1980 amendment to the 1976 Act places computer programs within the category of protected "literary works." Computer databases are also included in the category of "literary works." H.R. REP. No. 94-1476, at 54, *reprinted in* 1976 U.S.C.C.A.N. 5659, 5667 (1975).

216. *E.g.*, Playboy Enter., Inc. v. Frena, 839 F. Supp. 1552, 1555 (M.D. Fla. 1993) (recognizing full copyright protection for digitized magazine pictures).

217. *See* UMG Recordings, Inc. v. MP3.com, 92 F. Supp. 2d 349 (S.D.N.Y. 2000) (granting summary judgment for copyright infringement of musical recordings posted on the internet in the MP3 format). In an out-of-court settlement, defendant CompuServe agreed to compensate music publishers for prior use of the copyrighted songs. CompuServe also guaranteed that its music bulletin board managers would obtain licensing agreements for the future use of any copyrighted material, as well as pay royalties to the copyright holders. Matthew Goldstein, *Accord Ends On-Line Suit Over Music*, N.Y. L.J., Nov. 8, 1995, at 1; *see* Alan J. Hartnick, *1st Mechanical License in Cyberspace*, N.Y. L.J., Feb. 16, 1996, at 5 (discussing need for such licenses to protect copyrighted works).

218. The "Internet" refers to the on-line world and is used interchangeably with "cyberspace" and "Web." It is described as "an international network of interconnected computers" from which any number of users may access a "wide variety of communication and information retrieval methods." Reno v. ACLU, 521 U.S. 844, 849 (1997) (explaining and adopting Internet terminology).

219. 18 U.S.C. § 2319 (1994). Infringement of ten copies or phonorecords of one or more copyrighted works valued at more than $2,500 carries a maximum sentence of five years for a first offense and ten years for a second offense. Infringement of one or more copies or phonorecords which have a total retail value of more than $1,000 carries a maximum sentence of one year. 18 U.S.C. § 2319(b) (1994) *amended by* Pub. L. No. 105-47, § 2(d), 111 Stat. 2678, 2679 (1997).

220. 18 U.S.C. §§ 2319, 2319A (1994).

221. The White House created the National Information Infrastructure Task Force ("IITF") in February 1992 to investigate regulatory needs for the on-line world. The IITF then formed the Working Group on Intellectual Property to examine the intellectual property implications of the National Information Infrastructure ("NII"). On July 7, 1994, the Working Group released a preliminary draft of its report, known as the "Green Paper." Following testimony and public comments on this draft, the Working Group released in September 1995 a final version of the report, known as the "White Paper." Its main finding was that "with no more than minor clarification and limited amendment the Copyright Act will provide the necessary balance of protection of rights." WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 17 (1995), *available at* www.uspto.gov/web/offices/com/doc/ipnii/ (last visited Mar. 15, 2001) [hereinafter "WHITE PAPER"].

Several commentators have criticized the authors of the WHITE PAPER for overbreadth and lack of technical knowledge. *See* Andrew Grosso, *Copyright and the Internet: A Footnote, A Sleight of Hand, and a Call to Reason*, FED. LAW., Jan. 1997, at 44 (arguing that the WHITE PAPER definitions make "mere viewing" over the Internet unlawful); Joseph V. Myers III, *Speaking Frankly About Copyright Infringement on Computer Bulletin Boards: Lessons to Be Learned from Frank Music, Netcom and the White Paper*, 49 VAND. L. REV. 439, 450-62 (1996) (criticizing the WHITE PAPER for overstating liability contemplated by Copyright Act and distinguishing display

problematic in the context of cyberspace are addressed here: (1) the "first sale doctrine" exception; and (2) the statutory requirement that criminal liability be based on findings of intent and commercial or financial gain.

1. Infringement Via the Internet

Unauthorized file transfers of copyrighted materials infringe upon the copyright holder's exclusive rights in two ways; uploading[222] files violates the rights of distribution and downloading[223] violates reproduction rights.[224]

In *Napster,* the Ninth Circuit held that such conduct does not constitute fair use.[225] First, sending a file to an anonymous requester cannot be considered a personal use and the purpose of saving the expense of purchasing copies is more properly viewed as commercial.[226] Second, copying an entire work weighs against findings of fair use.[227] Courts have refused to acknowledge unauthorized sampling or space-shifting as fair uses in the context of file transfers.[228]

2. The Financial Gain Requirement or Threshold Violation

The "commercial advantage" or "financial gain" requirement for a finding of

---

from reproduction with regard to on-line violations of the Act); Pamela Samuelson, *The Copyright Grab*, 4.01 WIRED 135 (1996) (criticizing WHITE PAPER for misrepresenting judicial copyright precedent and extending copyright protection beyond traditional commercial applications); Pamela Samuelson, *Intellectual Property Issues Raised by the National Information Infrastructure*, PRACTICING LAW INSTITUTE, PATENTS, COPYRIGHTS, TRADEMARKS AND LITERARY PROPERTY COURSE HANDBOOK SERIES, 454 PLI/PAT 43, 48, 56-57 (1996). *See generally* EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 48 (1994) (DISCUSSING COPYRIGHT PROTECTION ISSUES RAISED BY INTERNET); LANCE ROSE, NETLAW 83 (1995) (arguing United States intellectual property laws have evolved along with technology and can protect intellectual property rights of owners in cyberspace); Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet*, 12 BERKELEY TECH. L.J. 15, 32 (1997) (analyzing deficiencies of traditional copyright concepts with regard to Internet conventions and use).

222. Uploading denotes placing files onto a server from which they may be accessed by anyone browsing the Web.

223. Downloading is the act of retrieving or accessing any information over the Internet.

224. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001) (finding Napster users directly infringed copyrights and that the service could be held contributorily and vicariously liable).

225. *Id.* at 1014-15.

226. *Id.* 1015.

227. *Id.* 1016.

228. *Id.* 1018-19. Through sampling, individuals make temporary copies of a work to decide whether they will purchase it. The Ninth Circuit held unauthorized sampling is a commercial use, regardless whether "some users eventually purchase the" work. *Id.* at 1018. Space-shifting involves individuals who download files of works they previously purchased to gain the convenience of using a different format of the same work. *E.g.*, Sony v. Univ. City Studios, Inc., 464 U.S. 417, 423 (holding time-shifting, by recording television shows for later home viewing, is a fair use); Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1079 (9th Cir. 1999) (copying music files from a computer to a portable MP3 player is fair use). However, general file sharing is not within the protected area of space-shifting because it simultaneously distributes the copyright material to the public. *See Napster*, 239 F.3d at 1019 (discussing transfer of MP3 files); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349, 351-52 (same).

criminal copyright liability has previously hindered prosecutors.[229] In *United States v. LaMacchia*,[230] the defendant, who set up a secret bulletin board and distributed unauthorized copies of commercially published, copyrighted software, escaped criminal liability because he neither sought nor received financial or commercial gain from his actions.[231]

In 1997, Congress enacted the NET Act, with the purpose of "criminalizing *LaMacchia*-like behavior."[232] The NET Act amended 17 U.S.C. § 506(a) to permit the government to prove either financial gain or that one or more copies, or phonorecords of one or more copyrighted works, were reproduced or distributed during any 180-day period, provided that the copies have a total retail value exceeding $1,000.[233] Moreover, financially motivated transactions include trading infringing material for other copyrighted works.[234]

3. The Internet and the First Sale Doctrine

The first sale doctrine allows a copyright holder to legally sell or give away her copy of the work.[235] Applied to file transfers in cyberspace, the doctrine permits a person who legally installs or downloads[236] a copy of a file to her own disk to freely redistribute that copy, whether or not she assesses a fee to anyone else by sending the file and then deleting her copy.[237]

---

229. WHITE PAPER, *supra* note 221, at 228-29. The requirement led the Working Group to conclude that current copyright law is "insufficient to prevent flagrant copyright violations in the NII context." *Id.* at 127-28.

230. 871 F. Supp. 535 (D. Mass. 1994).

231. *Id.* at 537. Warez sites are anonymous, often short-lived file-transfer protocol ("FTP") sites that exist solely to disseminate unlicensed copies of software and/or passwords for pirate software. They are not usually maintained for profit or malicious purposes and can be accessed by any user of the Internet of Usenet. *See* David McCandles, *Warez War*, 5.04 WIRED 133, 134-35 (1997) ("Warez crackers, traders, and collectors do not pirate software to make a living; they pirate software because they can. The more the manufacturers harden a product with tricky serial numbers and anticopy systems, the more fun it becomes to break.").

232. H.R. REP. No. 105-339, at 3, 8 (1997) (explaining "*LaMacchia*-like behavior" as "[C]omputerized misappropriation in which the infringer does not realize a direct financial benefit but whose actions nonetheless substantially damage the market for copyrighted works."); *supra* notes 141-43 and accompanying text (discussing NET Act). *See generally* NIMMER & NIMMER, *supra* note 125, at § 15.01(B)(2). This Bill was known as the "Anti-*LaMacchia*" Bill because the Court's decision outraged the computer software industry. Coblenz, *supra* note 141, at 249.

233. Pub. L. No. 105-339, § 2(b), 111 Stat. 2678 (1997) (amending 17 U.S.C. § 506(a)). The NET redefined "financial gain" to include "the receipt or expectation of receipt." 17 U.S.C. § 101 (1997).

234. No Electronic Theft Act (NET Act), Pub. L. No. 105-147, 18 U.S.C. § 101; *see also* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1015 (9th Cir. 2001) (noting, in dicta, that the conduct of Napster users was within the NET Act's meaning of financial gain).

235. 17 U.S.C. § 109(a) (1994) (allowing owner of a "particular copy or phonorecord lawfully made . . . or any person authorized by such owner" to, without copyright owner's authority, "sell or otherwise dispose of the possession of that copy or phonorecord"). For a general overview of the first sale doctrine, see *supra* Section IV.A.2. of this Article.

236. Downloading is the act of retrieving or accessing any information over the Internet. By way of contrast, "uploading" denotes placing files onto a server from which they may be accessed by anyone browsing the Web.

237. If the downloader is the equivalent of a record buyer, then, just as the latter may legally resell her copy of the record, the former may resell whatever she downloaded. The difference between the two scenarios is that the

However, there is a split in views regarding the situation where a copy is lawfully downloaded to a computer, rather than to a disk. Some argue that it is permissible to subsequently transmit the file provided that the initial purchaser deletes the copy on her computer at substantially the same time as she transmits a copy to another.[238] Others maintain that this still violates the exclusive rights of the copyright owner.[239]

B. Internet Service Provider Liability

Criminal liability for copyright infringement is predicated on a finding that the alleged perpetrator acted willfully.[240] The cyberspace context complicates the prosecutor's job because the defendant can convincingly argue an unknowing contribution to or commission of an offense.[241] The expansion of copyright law to address the internet has yielded civil cases involving allegations of copyright infringement directed against the system operator ("Sysop")[242] or the bulletin board service ("BBS").[243] A service provider may be held liable for contributory[244]

---

record seller sacrifices her copy of the record, whereas the download likely retains a copy of what she downloaded. WHITE PAPER, *supra* note 221, at 95.

238. William Sloan Coats et al., *Streaming into the Future: Music and Video Online*, 20 LOY. L.A. ENT. L. REV. 285, 294 (2000) (arguing that the doctrine depends on the fact that the number of copies does not increase); David L. Hayes, *Advanced Copyright Issues on the Internet*, 7 TEX. INTELL. PROP. L.J. 1, 99 (1998) (same).

239. WHITE PAPER, *supra* note 221, at 95 (noting that this constitutes further copying).

240. 17 U.S.C. § 506(a) (1994 and Supp. IV 1998).

241. In contrast, a finding of civil copyright vicarious liability requires only that the defendant be in a position to control the use of the copyrighted works and had authorized such use without the owner's permission. *See* Sony Corp. v Universal City Studios, Inc. 464 U.S. 417, 437 (1984). *See generally* NIMMER & NIMMER, *supra* note 125, § 12.04(A)(2)(a).

242. The sysop is the entity that runs the on-line system or service.

243. *See* Sega Enter. Ltd. v. Maphia, No. CIV.A. 93-4262 CW, 1997 WL 337558, at * 1 (N.D. Cal. June 9, 1997) (permanently enjoining BBS operator from "displaying, transferring or making available" copyrighted video games illegally copied by persons using BBS, upon finding owner knowingly facilitated infringement); Sega Enter. Ltd. v. Maphia, 857 F. Supp. 679, 683 (N.D. Cal. 1994) (holding defendant Sysop liable because it operated electronic bulletin board to which users uploaded plaintiff's copyrighted games, while other users downloaded them, and defendant had specific knowledge of, and at times even solicited, infringing actions); Playboy Enter. v. Frena, 839 F. Supp. 1552, 1556-57 (M.D. Fla. 1993) (holding operator of computer BBS, which was accessible to customers for fee, liable for copyright infringement because users had downloaded plaintiff's unauthorized pictures); *see also* Playboy Enter. v. Russ Hardenburgh Inc., 982 F. Supp. 503, 511-12 (N.D. Ohio 1997) (collecting cases discussing direct or contributory infringement by BBS Sysop for allegedly displaying and distributing copyrighted documents placed on-line by subscribers).

244. To hold a party liable for contributory infringement, the government must prove that the system provider 1) knew or had reason to know of direct infringement by its users and 2) induced or materially contributed to the infringing conduct. *See* Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845 (11th Cir. 1990) (articulating well-settled test for contributory infringer (citing Casella v. Morris, 820 F. 2d 362, 365 (11th Cir. 1987))); *see also* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020-24 (9th Cir. 2001) (finding likelihood of contributory liability where Napster had actual knowledge of infringing material and materially contributed by providing support services without which users could not find and download music with ease); Polygram Intern. Pub., Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314 (D. Mass. 1994) (ruling that "defendant can be held contributorily liable for authorizing another to publicly perform a work without permission of copyright owner" (citing Danjaq, S.A. v. MGM/UA Communications, Co., 773 F. Supp. 194, 200-202 (C.D. Cal. 1991))), *aff'd*, 979 F.2d 772 (9th Cir. 1992); NIMMER & NIMMER, *supra* note 125, § 12.04(A)(2)(a) (explaining standard of knowledge is objective: "know, or have reason to know").

or vicarious[245] copyright infringement.

In *Religious Technology Center v. Netcom On-Line Communication Service, Inc.*,[246] the district court held that, absent a showing of actual knowledge of specific acts of infringement, a BBS service provider could not be held directly or vicariously liable for civil copyright infringement committed by a subscriber.[247] At the December 1996 Geneva meeting of the World Intellectual Property Organization ("WIPO"), liability for Internet Service Providers ("ISPs") and Sysops was almost unanimously rejected.[248] In response to this international discussion, Congress provided a safe harbor to ISP's through the Digital Millennium Copyright Act, which codified the holding of *Netcom*.[249]

In general, 17 U.S.C. § 512 exempts a service provider[250] from liability for monetary, injunctive or other equitable relief for copyright infringement by reason of the provider's transmitting, routing, or providing a connection for such material, or temporarily storing such material in the course of such a transmission, routing, or connection.[251] The provider remains exempt from liability for copyright infringement so long as the provider has no "actual knowledge" and is not aware of

---

245. Vicarious liability for copyright infringement extends beyond the employer-employee relationship to a defendant that has 1) the right and ability to supervise the infringing activity and 2) a direct financial interest in the infringing activity. *Napster*, 2001 WL 115033, *16-*18 (finding Napster was financially interested because future revenues depended on increased userbase and that the company maintained the right and technological ability to supervise users' conduct by locating infringing materials listed on its search indices); Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.2d 259, 262 (9th Cir. 1971) (holding complaint stated a cause of action despite no employer-employee relationship).

246. 907 F. Supp. 1361 (N.D. Cal. 1995).

247. *Id.* at 1374 (holding that liability might exist where provider fails to remove infringing works after receiving notice of posting on network).

248. *See generally* Bruce G. Joseph, *The New WIPO Copyright and Phonograms Treaties: Twenty-One Days in Geneva and the Return to Washington*, *in* GLOBAL TRADEMARK AND COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY RIGHTS IN THE INTERNATIONAL MARKETPLACE, 488 PLI/PAT 371 (1997) (describing outcome of WIPO meeting); Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369 (1997) (same).

249. 17 U.S.C. § 512 (1994); Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2877 (1998).

250. The statute defines a service provider, as used in subsection (a) of the statute, as "an entity offering the transmission, routing, or providing or connections for digital online communications, between or among points specified by a user, or material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C. § 512(k)(1)(A) (1994). For all other subsections in the statute "the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)." 17 U.S.C. § 512(k)(1)(B) (1994).

251. 17 U.S.C. § 512(a) (1994). Such liability exemption will only apply, however, if:

> (1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission . . . is carried out through an automatic technical process without selection by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider . . . is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients . . . for a longer period that is reasonably necessary for the transmission; (5) the material is transmitted through the system or network without modification of its content.

17 U.S.C. § 512(a) (1994).

information indicating that the material is infringing, and such provider "does not receive a financial benefit directly attributable to the infringing activity."[252] Although the law does not require a provider to monitor or otherwise seek out information indicating infringement, the law does require that a provider, upon obtaining such information, expediently remove or disable access to such material.[253] Those who knowingly, materially misrepresent that the material is infringing, or that the material was removed or disabled by mistake or misrepresented, are liable for damages.[254] Where a provider removes or disables access to such material in "good faith," or based on circumstances "from which infringing activity is apparent, regardless of whether the material is ultimately determined to be infringing," she will generally[255] not be liable.[256]

VI. PATENT

This Section is divided into three parts. Part A discusses criminal liability for false patent marking. Part B addresses counterfeiting and forging of letters patent. Finally, Part C discusses whether the National Stolen Property Act applies to patent infringement.

A. False Marking

While most federal remedies for patent misuse are civil, the Patent Act establishes criminal liability for infringement.[257] The false affixing, marking, or use of the following constitutes false marking under the statute if done in connection to sales or advertising: (1) "the name or any imitation of the name of the patentee," (2) the patent number, or (3) the words "patent" or "patentee."[258] Additionally, the use of the word "patent," or any word or number indicating that

252. 17 U.S.C. § 512(c)(1)(A)(i), (ii), (c)(1)(B) (1994).

253. 17 U.S.C. § 512(c)(1)(A)(iii), (c)(1)(C) (1994). However, such limitations on liability are contingent upon the provider's designation of an agent to receive notifications of such infringement and making contact information available through its service. 17 U.S.C. § 512(c)(2) (1994).

254. 17 U.S.C. § 512(f)(1)-(2) (1994).

255. 17 U.S.C. § 512(g)(2) (1994) (discussing an exception under which a service provider could be liable for taking down material).

256. 17 U.S.C. § 512(g)(1) (1994).

257. 35 U.S.C. § 292 (1994) (providing a *qui tam* cause of action whereby a penalty, in the form of a fine not more than $500 for each offense, may be imposed and divided between the person bringing suit and the United States). *But see* Filmon Process Corp. v. Spell-Right Corp., 404 F.2d 1351, 1355 (D.C. Cir. 1968) (holding that although 35 U.S.C. § 292 is penal in nature, it is not a criminal statute).

258. 35 U.S.C. § 292(a) (1994); *see also* Lang v. Pacific Marine and Supply Co., 895 F.2d 761, 765 (Fed. Cir. 1990) (holding trial court's dismissal of false marking count proper because alleged infringing ship hull was still being manufactured and the article "must be completed before section 292 will allow a claim to continue"); Arcadia Mach. & Tool v. Sturm, Ruger & Co., 786 F.2d 1124, 1125 (Fed. Cir. 1986) (holding that label declaring contents of package "may be manufactured under" one or more listed patents or pending applications did not violate false patent marking statute when box was used for various models); Cal. Med. Prod. v. Tecnol Med. Prod., 921 F. Supp. 1219, 1261 (D. Del. 1995) (finding that affixing the patent number to an article where the patent had lapsed did not violate the false marking statute because the patent was then reinstated). *But see* Telectronics Pacing Systems v. Ventritex, 982 F.2d 1520 (Fed. Cir. 1992) (holding that "a patentee should be unable to seek a

the item is patented, in connection with a non-patented item violates this statute, as does the use of the words "patent applied for," "patent pending," or any other words falsely conveying the status of a patent.[259] To prove any of the above violations, deceitful intent of the defendant must be shown.[260]

B. Counterfeiting or Forging Letters Patent

Letters patent is the display of information on the item that the government has given the manufacturer the right to exclude others from making.[261] The Letters Patent statute[262] imposes criminal sanctions on persons forging, counterfeiting, or altering any letters patent, as well as knowingly passing, uttering, or publishing as genuine, any such letters patent.[263]

C. National Stolen Property Act

In addition to excluding interstate transportation of goods infringing on another's copyright from the coverage of the NSPA,[264] *Dowling v. United States*[265] implied, and has been interpreted to mean, that the Act also does not apply to the interstate transportation of goods infringing on patents.[266] Because patent infringement, like copyright infringement, does not involve a physical taking, the Supreme

---

declaration of infringement against a future infringer when a future infringer is able to maintain a declaratory judgment action for non infringement under the same circumstances.").

259. 35 U.S.C. § 292(a) (1994); *see* Project Strategies Corp. v. Nat'l Communications Corp., 948 F. Supp. 218, 226-27 (E.D.N.Y. 1996) (holding patent marking statute was not violated in part because the use of the phrase "U.S. and foreign patents granted and pending" was not false or misleading where the granted patent was foreign and the pending patent was in the United States).

260. 35 U.S.C. § 292(a) (1994); *see also* Boyd v. Schildkraut Giftware Corp., 936 F.2d 76, 79 (2d Cir. 1991) (holding cosmetic compact case manufacturer who misunderstood instructions to delete reference to patent holder's patent number and shipped compacts with holder's number had not intended to deceive the public); Brose v. Sears, 455 F.2d 763, 769 (5th Cir. 1972) (affirming trial court's dismissal of plaintiff's *qui tam* suit because the intent of Sears to deceive the public was not proven); *Project Strategies Corp.*, 948 F. Supp. at 227 (holding patent marking statute was not violated in part because "there wasn't a scintilla of evidence of any intent to deceive the public"); Johnston v. Textron, Inc., 579 F. Supp. 783, 794–96 (D. R.I. 1984) (finding intent to deceive the public by the use of the word "patented" in a radio advertisement in connection with a non-patented article after being notified by patent holder of the falsity of such use), *aff'd*, 758 F.2d 666 (Fed. Cir. 1984).

261. 18 U.S.C. § 497 (1994) (making criminal the forging, counterfeiting, or altering of any letters patent, as well as knowingly passing, uttering, or publishing as genuine, any such letters patent).

262. 18 U.S.C. § 497 (1994).

263. 18 U.S.C. § 497 (1994).

264. 18 U.S.C. § 2314 (1994) (holding anyone knowingly involved in the transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting shall be fined or imprisoned under this title not more than ten years, or both).

265. 473 U.S. 207 (1985) (holding that a National Stolen Property Act provision imposing criminal penalties for interstate transportation of stolen property did not reach the interstate transportation of "bootleg records," that is, unauthorized copies of commercially unreleased performances of famous entertainer; the phonorecords were not "stolen, converted or taken by fraud" except in the sense that they were manufactured and distributed without the consent of the copyright owners of the musical compositions performed on the records).

266. *See id.* at 227 ("Despite its undoubted power to do so, however, Congress has not provided criminal penalties for distribution of goods infringing valid patents."); *see also* Naso v. Park, 850 F. Supp. 264, 275

Court took a literal view of the Act's requirement that the copyrighted goods in dispute be "stolen, converted or taken by fraud."[267] The Supreme Court has not revisited the issues decided in *Dowling*, although the circuits have weighed in on the Court's literal view of the Act.[268]

VII. ART CRIMES

Art crime has become a booming multi-billion dollar industry,[269] third only to illegal drug smuggling and arms trading markets.[270] Crimes span simple theft and vandalism[271] to forgery,[272] money laundering,[273] and various forms of fraud.[274]

(S.D.N.Y. 1984) (holding patent-infringing microform reels were not stolen, converted, or fraudulently-taken goods under the meaning of the National Stolen Property Act).

267. *Dowling*, 473 U.S. at 216-17 (finding that National Stolen Property Act "contemplate[s] a physical identity between the items unlawfully obtained and those eventually transported" and finding that language of copyright statutes clearly distinguishes possessory interests of copyright holder from ordinary property interests).

268. *See* United States v. Lennon, 814 F.2d 185 (5th Cir. 1987) (refusing to extend the Dowling exception from the National Stolen Property Act penalty for copyrighted items to a case where money launderer mingled fraudulently obtained funds with legitimate funds and then transported all funds across state lines); United States v. Wallach, 935 F.2d 445 (2d Cir. 1991) (holding that the unique nature of copyrights, which do not provide a copyright holder with the full panoply of property rights over their work—namely possessory rights—allowed for the *Dowling* court to find the National Stolen Property Act was inapplicable to copyright infringers, and that that reasoning could not be extended to interstate transportation of fraudulently acquired checks).

269. *See* David Holmstrom, *Stolen-Art Market Is a Big Business at $2 Billion A Year*, CHRISTIAN SCI. MONITOR, Aug. 11, 1994, at 1; Michael James, *Internet May Shed Light on Shadowy Art Thieves; FBI and Interpol to Display Stolen Works on Web Sites*, BALTIMORE SUN, Aug. 17, 1998, at 1A (citing Art Loss Register's estimates of $3 billion of stolen, unaccounted artworks, numbering over 100,000); *see also* Christine Spolar, *Antiques Up for Grabs in Budapest: Hungarian Families Vie to Sell Heirlooms to Posh Galleries*, WASH. POST, Dec. 31, 1997, at A17 (discussing natural growth in illicit art trade when prices escalate and currency falters and warning that "[a]s prices soar, the potential for fraud multiplies").

270. *See* Steve Lopez with Charlotte Faltermeyer, *The Great Art Caper: Is the Heist of the Century About to Be Solved? Two Cons May Hold the Answer*, TIME MAG., Nov. 17, 1997, at 74 (tracing recent developments in recovery efforts of nine works valued at $300 million stolen from Boston's Gardner Museum in 1990); *cf.* Anthony J. Del Piano, *The Fine Art of Forgery, Theft and Fraud*, CRIM. JUST., Summer 1993, at 16, 17 (contending that art theft is *second* only to illicit drug market); Jason Bernetto & Antoine Banet-Rivet, INDEP. (London), July 26, 1999, at 7 (stating that underground art crime industry is worth £3 billion a year and is second only to the illegal drug trade).

271. *See* David Rosenzweig, *Ex-UCLA official collapses at Sentencing in Art Theft Court: Former Head of Student Counseling, Who is Undergoing Chemotherapy, is Given 10 Month Sentence*, L.A. TIMES, November 9, 1999, at B2 (showing UCLA's Director of Counseling was sentenced to ten months in jail and forced to pay $41,280 in restitution to the gallery to whom she sold a stolen work by Arthur Wesley Dow for $200,000); Alan Riding, *A Crime Wave in Chateau Country: Burglars Scramble to Meet the Demand for French Antiquities*, N.Y. TIMES, May 11, 1999, at E1 (increasing international demand for 18th and 19th century French art has resulted in a rash of burglaries of rural French chateaux); William Touhy, *Picture This: Art Thievery is Thriving*, L.A. TIMES, Aug. 16, 1994, at H1. Theft and vandalism of art, despite their often tremendously costly and devastating effects, usually do not demand the degree of sophistication that characterizes white collar crime; however, the subsequent resale or laundering of stolen art, a major element of white collar art crime, is complex and sophisticated. *See* Del Piano, *supra* note 270, at 18 (noting trafficking of stolen art transforms simple thefts into complex criminal enterprises). For review and discussion on the use of civil actions to seek relief in art crimes, see generally Steven A. Bibas, Note, *The Case Against Statutes of Limitations for Stolen Art*, 103 YALE L.J. 2437 (1994), in which the author rejects property approaches to art crimes and argues for the elimination of statutes of limitation for victims who report art thefts. *See generally* Ashton Hawkins, et al., *A Tale of Two Innocents: Creating an Equitable Balance Between the Rights of Former Owners and Good Faith Purchasers of Stolen Art*, 64 FORDHAM L. REV. 49 (1995) (advocating legislative encouragement of international arts registry to establish rights and liability limitations for

White-collar art criminals act as gallery or auction house dealers,[275] museum directors or curators,[276] and collectors.[277] Even artists may engage in tactics

purchasers of valuable art); William G. Pearlstein, *Claims for the Repatriation of Cultural Property: Prospects for a Managed Antiquities Market*, 28 LAW & POL'Y INT'L BUS. 123 (1996) (analyzing patrimony claims and proposing managed antiquities market). Ongoing investigations into World War II looting has vaulted consideration of this issue to the forefront of the art world. *See* John Authers & Richard Wolffe, *Looted Art Quandary for Museums: U.S. to Reveal Details of Traffickers*, FIN. TIMES (London), Dec. 2, 1998, at 4 (discussing Nazi's theft of over $2 billion in art at 1945 prices and the U.S. State Department's plan to release a list of "more than 2,000 art dealers suspected of trafficking in art looted by the Nazis").

272. *See* Cristina Carlisle, *As Latin American Art Prices Rise, So Do Forgeries*, N.Y. TIMES, Oct. 6, 1998, at E2 ("[T]he recent boom in prices for Latin works has created a parallel fake market, particularly for modern Cuban masters."); Julie K.L. Dam et al., *The Faking Game Demand Keeps Growing for Big-Name Art—and Brazen Forgers are Happy to Provide an Endless Supply*, TIME INT., Mar. 10, 1997, at 50 (citing former New York Metropolitan Museum of Art director's estimate that "half forgeries" and "outright fakes" comprise nearly half the art on the market); Alycen Mitchell, *Seeing Red Over Riopelle: Art Dealers and Collectors are Getting Badly Burned by Forgeries of his Work*, FIN. POST, Nov. 22, 1997, at 30 (discussing first picture forger convicted in Canada amidst wave of fake Riopelles). For some fascinating accounts of big-time art fraud, see LEE CATTERALL, THE GREAT DALÍ ART FRAUD AND OTHER DECEPTIONS (1992); THOMAS HOVING, FALSE IMPRESSIONS: THE HUNT FOR BIG-TIME ART FAKES (1996); JAMES KOOBATIAN, FAKING IT: AN INTERNATIONAL BIBLIOGRAPHY OF ART AND LITERARY FORGERIES, 1949-1986 (1987).

273. For example, the Drug Enforcement Agency (DEA) staged "Operation Dinero" to uncover money laundering by the Cali Columbia drug cartel, netting three paintings attributed to Picasso, Rubens and Reynolds. *See* Anna J. Kisluk, *DEA Operation Nets 3 Pictures*, IFAR REP., Dec. 1995, at 6, 8; *see also* United States v. Crabtree, No. 92-6330, 1993 WL 359689, at *1 (10th. Cir. Sept. 3, 1993) (affirming defendant's money laundering conviction where defendant transferred $50,000 of proceeds from the sale of a Renoir painting to an account to hide funds from the bankrupt estate); Antony Thorncroft, *Landscape of Larceny*, FIN. POST, Mar. 15, 1997, at 26 (describing botched attempts to sell $170 million worth of Old Masters taken in the Russborough heist leading to use of paintings as collateral for other crimes); *Customs Auction of a Dalí Accents Laundering by Art*, MONEY LAUNDERING ALERT, June 1, 1995 (noting "large disparity between cash bank deposits made by auction houses and cash receipts reported by them on IRS Form 8300"); Jo Durden-Smith, *Masterpieces as Money*, TOWN & COUNTRY MONTHLY, July 1, 1996, at 30 (concluding art works are just another form of money). For a general discussion of money laundering, see the MONEY LAUNDERING article in this issue.

274. *See* Jeff Leeds, *Former Doctor Is Convicted in Art Fraud Case*, L.A. TIMES, July 21, 1999, at C1 (describing man convicted of eighteen counts, including conspiracy and wire fraud, after he faked theft of Monet and Picasso paintings from his home to get $17.5 million insurance settlement).

275. "[Thirty to forty] percent of the world's available antiquities pass through the sale rooms in New York and London. Roughly [ninety] percent of these pieces are of unknown provenance, meaning they are almost certainly stolen, smuggled, or both." Richard McGill Murphy, *A Corrupt Culture*, NEW LEADER, Feb. 23, 1998, at 15 (reviewing Peter Watson's SOTHEBY'S: THE INSIDE STORY, a scathing exposé of the reputed auction house). Sotheby's reactions to such claims have been startling. "Sotheby's was breaking no laws selling smuggled material. We are here to make money" explained former London managing director. Julie Rekai Rickerd, *Revealing the Rot of a Venerable Auction House*, FIN. POST, Feb. 21, 1998, at R5. Watson also accused Sotheby's of creating a false market by manufacturing telephone bids to increase floor auction prices. *Id.; see also* Lisa J. Borodkin, Note, *The Economics of Antiquities Looting and a Proposed Legal Alternative*, 95 COLUM. L. REV. 377, 385–86 (1995) (discussing ways in which art auction system contributes to perpetration of art fraud).

276. *See* JOHN E CONKLIN, ART CRIME 87 (1994) (asserting that art fraud can be perpetrated by collectors, dealers, museums, and auction houses alike); Laura McFarland-Taylor, Comment, *Tracking Stolen Artworks on the Internet: A New Standard for Due Diligence*, 16 J. MARSHALL J. COMPUTER & INFO. L. 937 (detailing an account of how Sotheby's staff "allowed 'smuggled artifacts which had been taken from religious sites' to be sold through Sotheby's"); Steven F. Grover, Note, *The Need for Civil-Law Nations to Adopt Discovery Rules in Art Replevin Actions: A Comparative Study*, 70 TEX. L. REV. 1431, 1438 (1992) (asserting some reputable museum staffers may be tempted by lucrative corruption).

277. *See* Dalya Alberge, *Dealers Hand Over £1 Million Art to Swindlers*, TIMES (London), Sept. 1, 1999 (describing how Italian man posing as collector duped more than a dozen respected, leading gallery owners

facilitating subsequent white-collar crime.[278] An appraiser may refuse to authenticate a legitimate artwork as part of a conspiracy to drive up the value of the remaining stock.[279] These perpetrators use their positions of power or privilege to commit non-violent crimes that often require an advanced level of education and intellect.[280]

More recently, Sotheby's, the world's largest art auction house, has been under investigation for alleged price-fixing and securities fraud.[281] On Oct. 5, 2000, Sotheby's announced its former President and CEO, Diana Brooks, was pleading guilty to price-fixing based on conversations she had with Christie's, the world's second largest art auction house.[282]

Several obstacles to detection of art crimes exist: auction houses and collectors may often be reticent to report fraud;[283] and swindled buyers, who may fear embarrassment or unwelcome attention by thieves and IRS agents, continue the deception in order to resell the piece, or balk at the threat to the legitimacy of the remaining pieces in their collection.[284] The complexity and expense of accurate authentication also impedes detection.[285]

---

and dealers in elaborate scam resulting in loss of many important works, including some by Guardi and Geerards).

278. *See* CONKLIN, *supra* note 276, at 84 (hypothesizing that Dalí signed blank sheets of art paper to make inexpensive photographic reproductions, which were then marketed as high-priced "originals" or "limited editions").

279. *But see* Kramer v. Pollock-Krasner Found., 890 F. Supp. 250 (S.D.N.Y. 1995) (rejecting dealer's allegation of conspiracy by authenticators in refusing to authenticate his alleged Pollock painting); Vitale v. Marlborough Gallery, 32 U.S.P.Q. 2d 1283 (S.D.N.Y. 1994) (dismissing purchaser of alleged Pollock painting's claim that authenticators and dealers conspired in refusing to authenticate his painting).

280. *See* Steven Mark Levy, *Liability of the Art Expert for Professional Malpractice*, 1991 WIS. L. REV. 595, 596 ("Fine arts experts, including authenticators, appraisers and consultants, wield tremendous financial power in the art market.").

281. In addition to pleading guilty to securities fraud for making false statements in SEC filing regarding a price-fixing operation Sotheby's was running with Christie's, the auction house and its executive director were named defendants in a shareholder's class action, filed in the Southern District of New York. *In re* Sotheby's Holdings, No. 00 Civ. 1041 (DLC) (Aug. 31, 2000) (ordering all other defendants named in the class action suit to be dismissed leaving Sotheby's and its President, Diana Brooks, alone to face charges of price-fixing and securities fraud).

282. *See* Statement from Sotheby's Board of Director's, Oct. 5, 2000, *available at* http://www.sothebys.com/about/pressrelease/index.html (last visited Mar. 2, 2001).

283. *See* Harlan Levy & Constance Lowenthal, *Stolen and Smuggled Art*, N.Y.L.J., Dec. 9, 1997, at 1 (discussing the failure of Christie's auction house to alert authorities when it learned that a manuscript submitted to be sold was stolen from a cathedral in occupied Germany after WWII; instead, Christie's simply returned the manuscript to the seller's agent).

284. Denise M. Topolnicki & J. Howard Green, *The Fine Art of Fraud*, MONEY, Sept. 1986, at 73. Furthermore, there is no simple either-or dichotomy between authentic and fake art works. *See* R.H. MARIJNISSEN, PAINTINGS, GENUINE, FRAUD, FAKE: MODERN METHODS OF EXAMINING PAINTINGS 20-34 (1985) (listing fifteen categories of "authenticity").

285. *See* Lawrence S. Bauman, Note, *Legal Control of the Fabrication and Marketing of Fake Paintings*, 24 STAN. L. REV. 930, 935–36 (1972) (noting unavailability of art experts for the purposes of authentication and providing several reasons for this problem). For examples of high-priced scientific authentication techniques, see David Conrads, *Progress is Real for Those in the Business of Spotting Fakes: Scientists and Art Historians are*

In addition, many art crimes are easy to perpetrate.[286] Novice collectors are often willing to rely on a dealer's reputation instead of researching their purchases, which encourages and rewards art crime.[287]

The international art community has welcomed several recent innovations in purchasing art,[288] publicizing art theft,[289] tracing provenance,[290] and registering works of art.[291]

Erecting a Formidable Barrier Between Art Forgers and Art Museums, CHRISTIAN SCI. MONITOR, Oct. 8, 1996, at 12 and Leonard D. Du Boff, *Controlling the Artful Con: Authentication and Regulation*, 27 HASTINGS L.J. 973, 988–97 (1976).

286. *See* Mitchell, *supra* note 271, at 30 (explaining forgers' preference for modern art because its simpler style facilitates imitation and does not require complicated antiquating techniques).

287. *See* Robin Morris Collin, *The Law and Stolen Art, Artifacts, and Antiquities*, 36 HOW. L.J. 17, 27 (1993) (stating that consumers seldom inquire into legitimacy of art work); Topolnicki & Green, *supra* note 284, at 73 (noting that victims of many art frauds are usually novice collectors); *cf.* Balog v. Center Art Gallery-Hawaii, Inc., 745 F. Supp. 1556, 1562 (D. Haw. 1990) ("[S]ome well-executed fakes have fooled even knowledgeable buyers and dealers."); Bauman, *supra* note 285, at 932–34 (citing numerous methods of forgery, such as faked signatures, completions of unfinished canvases, misrepresentation of a work's author, reproductions, pastiches [a method of combining elements of several works to create a new work], and faked unfinished drawings).

288. *See generally* Colin Watson, *Bleak Picture on Theft and Fraud*, CANBERRA TIMES, Jan. 13, 2000, at 11 (uncovering the huge money making potential for countries in trafficking in stolen cultural artifacts—even their own—is so great that there is little compliance with the UNIDROIT Convention of 1995. In addition, many major owners of looted art and cultural artifacts are not signatories to the convention, like the UK); Stephen K. Urice, *World War II and the Movement of Cultural Property: an Introduction and Brief Bibliography for the Museum Administrator*, LEGAL PROBLEMS OF MUSEUM ADMINISTRATION, ALI-ABA COURSE OF STUDY MATERIALS, Mar. 26, 1998 (listing books and websites to consult when researching potential acquisitions).

289. The Art Loss Register maintains an international, permanent, computerized clearinghouse on stolen and missing art; their image database of over 60,000 items has been instrumental in the recovery of numerous stolen objects. For more information regarding the Register, see *The Art Loss Register, available at* http://www.artloss.com (last visited Mar. 15, 2001); *see also* Eric V. Copage, *A Rogues' Gallery*, N.Y. TIMES, § 14, at 4 (noting Art Loss Register's success in helping to recover more than 900 items worth $75 million over past eight years); Barbara Lantin, *The Art of Helping Police with Inquiries*, INDEP. (London), Apr. 3, 1996 (discussing role of Art Loss Register). The International Foundation for Art Research (IFAR), a non-profit organization dedicated to preventing and recovering stolen, forged, and misattributed art works, maintains the ALR's U.S. office. *See generally* Bennetto & Banet-Rivet, *supra* note 270, at 7 (discussing CD-ROM database of photographs and descriptions of over 17,000 art and antique items now available for use by "police forces, museums, auction houses, and dealers in Interpol's 177 member countries"). *But cf.* Laura McFarland-Taylor, Comment, *Tracking Stolen Artworks on the Internet: A New Standard for Due Diligence*, 16 J. MARSHALL J. COMPUTER & INFO. L. 937, 963-68 (1998) (discussing confusion caused by the high number of web sites concerned with stolen art and the need for one official site to effectively combat art crimes to be used by international law enforcement, owners, sellers, and purchasers).

290. The Getty Research Institute for the History of Art and the Humanities (an independent entity of J. Paul Getty Trust) has established the "Getty Provenance Index" which documents the provenance (history of ownership) of over a half-million art works, which are coded by means of their "Object ID Checklist." This database is currently available on-line and on CD-ROM. *See* The Getty Research Institute for the History of Art and the Humanities, *The Getty Provenance Index, available at* http://piedi.getty.edu:80 (last visited Feb. 25 2001).

291. A San Francisco high-technology firm has developed a digital registration process, "ISIS," (Intrinsic Signature Identification System) that could help resolve disputes about authenticity and ownership of art works, thereby discouraging forgery and theft. The process is "based on the premise that all objects contain unique microscopic physical features and random anomalies that cannot be duplicated." Suzanne Muchnic, *Have Forgers Finally Met Their Match? A New Digital Registration Process Could Discourage Forgery and Theft and Help Resolve Disputes About Authenticity and Ownership of Valuable Artworks*, L.A. TIMES, July 2, 1995, at Calendar 50 (concluding that the success of this project remains uncertain). For further information on ISIS, see Verification Technologies, Inc., *Main Page, available at* http://www.netventure.com/vti/isis (last visited Feb. 25, 2001).

However, a lack of effective legislation[292] and the application of inconsistent due diligence standards by courts[293] have hampered attempts at effective containment and resolution of art crimes. The remainder of this Section examines existing federal and state laws that have met with limited success in combating art crimes.

Part A of this Section addresses the federal measures applied to art crime prosecutions, specifically the Theft of Major Artwork Act, the National Stolen Property Act, the mail and wire fraud statutes, the Copyright Felony Act, and compliance with UNESCO and UNIDROIT treaties. Part B reviews state art crime prosecutions under larceny and forgery laws that have been extended to protect art and antiquities.

A. Federal Statutes

1. Theft of Major Artwork Act

The Theft of Major Artwork Act[294] ("TMAA") specifically targets criminals that have stolen or fraudulently obtained "any object of cultural heritage"[295] from a "museum."[296]

---

292. *See* Bauman, *supra* note 285, at 931 (asserting existing state and federal regulatory attempts to control art crime frequently fail because available statutes for prosecution of art crime are primarily intended for other purposes, thus requiring creative tailoring to be of much use); Du Boff, *supra* note 285, at 998 (stating such statutes may also be ineffective because their penalties are insufficient deterrents in light of the potential profits). Faced with this statutory futility, prosecutors frequently choose not to waste precious funds and time on a losing battle. *See Balog*, 745 F. Supp. at 1564 (stating dealer's authentication of a work, unless that dealer witnessed work being produced, "can never be more than an educated guess or opinion"); Du Boff, *supra* note 285, at 998 (asserting intent requirement for fraudulent authentication may encourage sellers to intentionally not authenticate works).

293. *See* McFarland-Taylor, *supra* note 289, at 939 (arguing for "an internationally recognized standard of due diligence in reporting lost or stolen artworks utilizing the Internet"). *But see* Under Secretary of State Thomas Pickering, Address before the Centennial Celebration of the American Schools of Oriental Research (Apr. 14, 2000) (outlining steps taken by the United States to combat international trafficking in stolen cultural property, including historic artifacts, sculptures, and architectural pieces. The United States, as the first art-importing country to ratify the 1970 UNESCO Convention on Cultural Property has entered into bi-lateral arrangements with the following eight nations in order to protect an array of archaeological treasures: Cambodia, Canada, Cyprus, Peru, El Salvador, Guatemala, Mali, and Bolivia), *available at* http:// www.state.gov/www/policy_remarks/ 2000/2000-index.html#apr (last visited Feb. 25, 2001).

294. *See* 18 U.S.C. § 668 (1994) (laying out the standard and penalties for theft of major artwork which include fines and a sentence of no longer than ten years). The Act is part of the much larger Violent Crime Control and Law Enforcement Act of 1994, Pub.L. 103-322, Sept. 13, 1994, 108 Stat. 1796 (amending the Omnibus Crime Control and Safe Streets Act of 1968 to allow grants for the purpose of developing and implementing residential substance abuse treatment programs within State correctional facilities, as well as within local correctional facilities in which inmates are incarcerated for a period of time sufficient to permit substance abuse treatment); *cf.* S. 2783, 106th Cong. (2d sess. 2000) (21st Century Law Enforcement Law Enforcement and Public Safety Act, proposing changes to the "Omnibus Crime Control and Safe Streets Act of 1968").

295. 18 U.S.C. § 668(a)(2) (1994) ("[O]bject of cultural heritage" is defined to include "any object that is either (a) over 100 years old and worth over $5,000, or (b) worth at least $100,000, regardless of age.").

296. 18 U.S.C. § 668(a)(1) (1994). Museum is defined broadly enough to include most libraries. The Act protects any organized and permanent institutions that (a) are in the United States, (b) are "established for an

The TMAA also penalizes possession of an object known to be stolen or fraudulently obtained.[297] The statute of limitations for returning an indictment or filing information extends to twenty years after commission of the art theft[298] to compensate for the often delayed detection of such crimes and the unique difficulties of recovering stolen works.[299]

The first reported charge under this statute occurred in January 1998, when the FBI in Philadelphia charged two defendants for the theft of over two hundred relics from the Historical Society of Pennsylvania.[300] The TMAA has also been utilized in the prosecution of cases involving thefts from the New York Public Library for the Performing Arts.[301] Most recently, federal courts have used the act to justify sentencing computation based on cultural and market value of item stolen.[302]

2. *National Stolen Property Act*

The NSPA prohibits the transportation,[303] sale, and receipt or possession of stolen goods valued at or over $5,000 that have crossed state or United States boundaries.[304] To obtain a conviction, the defendant must have knowledge that the good is stolen.[305]

---

essentially educational or aesthetic purpose," (c) have a professional staff, and (d) own and regularly display to the public tangible objects. *Id.*

297. 18 U.S.C. § 668(b)(2) (1994) (making both theft of a cultural artifact and knowing receipt, concealment, exhibition or disposition of a stolen cultural artifact a crime punishable by fine or prison sentence).

298. 18 U.S.C. § 3294 (1994) (providing a twenty year statute of limitations for art theft prosecuted under § 668).

299. *See* Patty Gerstenblith, *Cultural Property and World War II: Some Implications for American Museums: A Legal Background*, LEGAL PROBLEMS OF MUSEUM ADMINISTRATION, ALI-ABA COURSE OF STUDY MATERIALS, Mar. 26, 1998, at 20 (discussing judicial side-stepping of traditional statute of limitations in order to facilitate art recovery).

300. *See* Joseph A. Slobodzian, *Case of the Missing History; FBI Recovers Artifacts Worth $3 Million; Electrician, Janitor Charged*, WASH. POST, Jan. 8, 1998, at B7 (describing stolen objects, including artifacts, from Revolutionary War and Civil War eras).

301. *See* United States v. O'Higgins, 55 F. Supp. 2d 172, 175 (S.D.N.Y 1998) (rejecting defendant's Commerce Clause challenge to § 668 for theft of one leaf from a Mozart piano minuet, and an essay and three letters by Richard Wagner because the theft of objects of cultural heritage "has a substantial impact on the national economy" by impacting the price of art across state lines and increasing the cost of insurance); Bill Alden, *Theft of Cultural Objects Crime Clears Constitutional Hurdle*, N.Y.L.J., Oct. 15, 1998, at 1 (describing *O'Higgins*' determination that the Act is constitutional).

302. *E.g.*, United States v. Medford, 194 F.3d 419, 425 (3d Cir. 1999) (holding that the cultural value of an artifact or artwork stolen can be added to the market value for sentencing purposes).

303. 18 U.S.C. §2314 (1994).

304. 18 U.S.C. §2315 (1994); *see* United States v. Trupin, 117 F.3d 678, 685 (2d Cir. 1997) (rejecting defendant's Commerce Clause challenge to 18 U.S.C. § 2315 and affirming defendant's conviction for possession of stolen painting, "Le Petit Concert" by Marc Chagall).

305. 18 U.S.C. §§ 2314, 2315 (1994); *see Trupin*, 117 F.3d at 681 (finding sufficient evidence of defendant's knowledge that painting was stolen due to defendant's lack of insurance coverage for the painting, the unrecorded status of the painting in defendant's personal property inventory, and defendant's decision to not display the painting). *See generally* Levy & Lowenthal, *supra* note 283, at 1 (stating that although no art dealer has ever been indicted under the National Stolen Property Act for knowingly returning stolen art "to a party other than its true

3. *Mail and Wire Fraud Statutes*

United States v. Center Art Gallery-Hawaii, Inc.[306] exemplifies the successful prosecution of art crime using mail and wire fraud statutes.[307] The gallery and its two owners were each convicted[308] for activities involving the largest art fraud ring in history.[309] The defendants, however, were not prosecuted for the sale of forged works of art, nor for their false appraisals, but rather for mailing false authentication certificates to customers and soliciting further business over the telephone in violation of mail and wire fraud statutes.[310]

Despite some prosecutorial success,[311] the requisite demonstration of criminal intent inhibits wide scale utilization of mail and wire fraud statutes to punish art crime.

4. *Copyright Felony Act*

A stringent *mens rea* requirement similarly limits the usefulness and success of art crime prosecutions pursued under the Copyright Felony Act.[312] The statute protects only unpublished works and works not in the public domain, leav-

---

owner," as Christie's did when it returned a stolen manuscript to seller's agent, statute's language would permit such interpretation if a "creative and aggressive prosecutor" was interested).

306. Cr. No. 89 00125 03 HM (D. Haw. May 4, 1990), *aff'd*, Nos. 90-10612, 90-10616, 90-10617, 1993 WL 118176 (9th Cir. Apr. 15, 1993) (finding gallery owners operating a large art fraud ring guilty of mail and wire fraud, as opposed to any art specific crime).

307. 18 U.S.C. § 1341 (1994) (mail fraud); 18 U.S.C. § 1343 (1994) (wire fraud).

308. The gallery's president was fined $750,000 and given a three-year prison sentence, and the vice-president was fined $282,000 and given a two-and-a-half year prison sentence. They were also ordered to pay restitution. *See* CONKLIN, *supra* note 276, at 83. *See generally* CATTERALL, *supra* note 272, at 163-328 (reviewing development of Center Art Galleries frauds).

309. *See Art Gallery, Officers Convicted in Dali Case*, NAT'L L.J., May 21, 1990, at 6 (deeming scandal "the largest art fraud in history at a consumer loss of more than $100 million from 1977 to 1989").

310. In addition, civil litigation based upon the same conduct paralleled the criminal prosecution. *See* Granat v. Center Art Galleries-Hawaii, Inc., No. 91-7252 (RLC), 1993 WL 403977, at *1, *8 (S.D.N.Y. Oct. 6, 1993) (denying defendants' motion to dismiss complaint that sought damages resulting from purchases of over-valued Monet and Gaugin paintings); Balog v. Center Art Gallery-Hawaii, Inc., 745 F. Supp. 1556, 1573 (D. Haw. 1990) (denying defendants' motion for judgment on the pleadings finding any applicable statute of limitations tolled).

311. *See* United States v. Austin, 54 F.3d 394, 405 (7th Cir. 1995) (affirming in part defendant's convictions for mail and wire fraud through sales of counterfeit art works); United States v. Amiel, 95 F.3d 135, 145-46 (2d Cir. 1993) (affirming defendants' mail fraud convictions for their distribution of fraudulent art work). The Amiel defendants were running what was reputed to be "the single largest worldwide source and distribution network of bogus prints." David S. Hilzenrath, *Cracking Down on Counterfeit Art; U.S. Charges 4 in the Global Distribution of Bogus Prints*, WASH. POST, Jan. 31, 1992, at C1. A dealer of the Amiel works also pled guilty to mail fraud. *Id.* In *United States v. Burke*, four owners and representatives of Manhattan's Barclay Gallery were each charged and convicted of all twenty-two counts of mail fraud and twenty-eight counts of wire fraud. No. 88 Cr. 722 (MBM) (S.D.N.Y. 1990); CATTERALL, *supra* note 272, at 96. The gallery "allegedly used high-pressure telephone sales pitches" to perpetrate its scheme. Arnold H. Lubasch, *U.S. Accuses 4 of High Profits in Fake Dali Art*, N.Y. TIMES, Oct. 4, 1988, at B6; *see also* Marianne Yen, *4 Charged in Dali Art Fraud*, WASH. POST, Oct. 4, 1988, at D1 (describing Barclay Gallery's sales methods).

312. 18 U.S.C. §§ 2319(b)-(c) (1994) (criminal infringement of a copyright).

ing many older works unprotected.[313] Also, many forgeries do not involve copying.[314]

5. UNESCO and UNIDROIT: Enforcement by Treaties

In 1970, the United Nations Educational, Scientific, and Cultural Organization ("UNESCO") adopted the "Convention on Cultural Property Implementation,"[315] which the United States implemented in 1983 through the Cultural Property Implementation Act ("CPIA").[316] However, legislation currently pending could allow for improved procedures for restricting the importation of stolen archaeological and ethnological material.[317] The treaty intends to protect the "cultural patrimony" of countries "from the pillage of archaeological or ethnological materials" by providing import restrictions for such objects.[318] The CPIA established the "Cultural Property Advisory Committee,"[319] which has led to restrictions on imports of antiquities from several countries.[320] In addition, the CPIA grants authority to the United Stated for the seizure and forfeiture of cultural property that is in violation of import restrictions.[321]

Because several countries considered major forces in the art trade failed to ratify

313. *See* Bauman, *supra* note 285, at 939 (noting limited use of copyright laws in art crimes prosecution).

314. *Id.*

315. Nov. 14, 1970, 10 I.L.M. 289, 823 U.N.T.S. 231. *See generally* ELIZABETH SIMPSON, THE SPOILS OF WAR; WORLD WAR II AND ITS AFTERMATH: THE LOSS, REAPPEARANCE, AND RECOVERY OF CULTURAL PROPERTY 272–311 (1997) (setting forth relevant treaties).

316. Pub. L. 97-416, Title III, 96 Stat. 2329, 2350 (1983) (codified at 19 U.S.C. §§ 2601-2613 (1994)). Because the CPIA mainly restricts the importation of illegally imported foreign cultural property and only affords redress to foreign state parties to the UNESCO convention, it does not provide private causes of action and is thus "limited to an extremely small . . . subset of potential claims." *See* Hawkins et. al., *supra* note 270, at 83. *See generally* Lawrence M. Kaye, *The Future of the Past: Recovering Cultural Property*, 4 CARDOZO J. INT'L & COMP. L. 23, 24–25 (1996) (discussing history of international response to illicit trade in cultural property); John P. Shinn, Comment, *A New World Order For Cultural Property: Addressing the Failure of International and Domestic Regulation of the International Art Market*, 34 SANTA CLARA L. REV. 977 (1994) (proposing amendments to the Convention to increase its efficiency in reducing illegal art trade); John Henry Merryman, *Thinking About the Elgin Marbles*, 83 MICH. L. REV. 1881, 1892-1893 (1985) (discussing inability of the Convention and subsequent legislation like the CPIA to reduce the illegal traffic of cultural property); Marilyn Phelan, *A Synopsis of the Laws Protecting Our Cultural Heritage*, 28 NEW ENG. L. REV. 63, 98 (1993) (discussing enactment, purpose, and scope of CPIA).

317. Cultural Property Procedural Reform Act, H.R.4372, 106th Cong., 2d session (2000).

318. 19 U.S.C. § 2602(a) (1994). To be considered an object of archaeological interest, the object must be of cultural significance, be at least 250 years old, and be discovered in land or under water. 19 U.S.C. § 2601(2)(i) (1994). To be considered an object of ethnological interest, the object must be "the product of a tribal or non-industrial society" and be "important to the cultural heritage of a people." 19 U.S.C. § 2601(2)(ii) (1994).

319. 19 U.S.C. § 2605 (1994) (establishing the Cultural Property Advisory Committee).

320. *See* Carl Nagin, *Hot Art: Illegal Traffic in Antiquities*, TOWN & COUNTRY MONTHLY, Mar. 1, 1995, at 138 (discussing effectiveness of committee despite its "cumbersome bureaucratic process").

321. 19 U.S.C. § 2609 (1994) (seizure and forfeiture statute); *see* United States v. An Original Manuscript Dated November 19, 1778, No. 96 Civ. 6221 (LAP), 1999 WL 97894, at *8 (S.D.N.Y. Feb. 22, 1999) (ordering forfeiture to United States of illegally imported original manuscript bearing Junipero Serra's signature that belonged to "Californias" collection of Mexican National Archives).

the 1970 UNESCO Convention, UNESCO asked the International Institute for the Unification of Private Law, Rome ("UNIDROIT") to prepare a new treaty that would provide protection to art trade in the rest of the world.[322] This treaty, completed on June 24, 1995, would greatly expand protection, but has a significant restriction: it only applies to art works stolen or looted after the date that the host country has ratified the treaty.[323] Thus far, out of the twenty-two countries who have signed the treaty, only three have ratified it, while two others have acceded to it.[324] The United States abstained from voting on the treaty and has not yet signed or ratified the UNIDROIT convention. This convention has generated significant controversy in the United States and the United Kingdom because art dealers claim they will no longer be able to exhibit or sell works in countries that have ratified the convention, on the grounds that the works might be confiscated by the country of origin, leaving art dealers without a cause of action.[325]

B. State Approaches

Various states have recognized the importance of promoting the arts by

---

322. Final Act of the Diplomatic Conference for the Adoption of the Draft UNIDROIT Convention on the International Return of Stolen or Illegally Exported Cultural Objects, June 24, 1995, 34 I.L.M. 1322 [hereinafter UNIDROIT]. The final title of the treaty is "UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects."

323. *Id.* at 1334–35, art. 10 (stating provisions apply prospectively, not retroactively).

324. *See List of the States Which Signed the Convention, available at* http://www.tufts.edu/departments/fletcher/multi/www/unidroit95-rat.html (last visited Feb. 25, 2001) (listing 22 signatories). As of January 1998, Lithuania, Paraguay, and Romania ratified the UNIDROIT treaty while China and Ecuador acceded to it. On Jan. 21, 1998, the fifth ratification instrument was deposited by Romania with the Italian government. Consequently, pursuant to Article 12, paragraph 1 (UNIDROIT, Ch. 5, art. 12(1), 34 I.L.M. at 1335), the treaty will enter into force between these five nations on July 1, 1998. *See* Letter from Marina Schneider, Research Officer, Unidroit Secretariat (Feb. 12, 1998) (on file with the *American Criminal Law Review*) (noting "that Peru and Hungary have already passed the law permitting the ratification and we are waiting for the formal deposit of the instruments"); *see also* Richard P. Greenfield, *The Trouble with the Trojan Gold*, NEWSDAY (N.Y.), Jan. 7, 1996, at A38 (explaining why United States has abstained from voting on UNIDROIT convention); *Kimbell to Host Swiss Collection: Paintings Find Temporary Sanctuary in Fort Worth*, DALLAS MORNING NEWS, July 5, 1997, at 43A (discussing problems in ratification process). For general discussion and analysis of UNIDROIT, see Marina Schneider, *The UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects, available at* http://www.city.ac.uk/artspol/schneider.html (last visited Feb. 25, 2001) (describing history and purposes of the convention). *See generally* Brian Bengs, Note, *Dead on Arrival? A Comparison of the UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects and U.S. Property Law*, 6 TRANSNAT'L L. & CONTEMP. PROBS. 503 (1996) (analyzing potential effects of UNIDROIT on United States property law); Marilyn E. Phelan, *The UNIDROIT Convention on Stolen or Illegally Exported Cultural Objects Confirms a Separate Property Status for Cultural Treasures*, 5 Vill. Sports & Ent. L.J. 31 (1998) (discussing importance of following UNIDROIT due to the "universal value of cultural property"); Jennifer Howard, *Objects of Desire; Contested Artifacts Are the Prize in an International Culture Clash*, WASH. POST, Dec. 14, 1997, at C1 (describing inherent complications in repatriating artistic and cultural objects).

325. *E.g.*, Godfrey Barker & Laura Stewart, *The Arts: Maastricht—the Last Art Fair?*, DAILY TELEGRAPH (London), Mar. 11, 1996, at 18 (claiming if the Netherlands ratifies treaty, art dealers will move annual fair from Maastricht to non-ratifying country); Hawkins, *supra* note 271, at 86 ("[i]f adopted, UNIDROIT would effectively supplant the CPIA.").

including provisions aimed at their protection and encouraging their development.[326] A number of states have enacted criminal simulation statutes designed to customize existing forgery laws, which, without such modification, are limited to actions associated with written documents and checks. For example, New York's Criminal Simulation Statute[327] extended New York's preexisting statute aimed at forgery of cultural property[328] to "antiques, *objets d'art*, rare books, and comparable matter."[329]

Twenty-six other states and Guam have codified similar "criminal simulation" provisions into their penal codes,[330] reflecting a growing awareness of the special type of protection needed in the art community. In three states, however, these statutes do not apply to all art and antiquities, but are limited to certain excavated or historical objects.[331] Imposing stricter requirements, two states require disclosure of the number of copies in limited editions of fine art works, with penalties and injunctions for inadequate or erroneous disclosure.[332] In addition, states often

326. *E.g.*, ALA. CODE § 32-6-470 (2000) (promoting the arts with a statute aimed at "raising funds for arts education, including the fine arts by providing for a distinctive license tag or plate to raise funds for art education."); N.Y. ARTS & CULT. AFF LAW. § 3.01 (McKinney 1984) (stating promotion of arts as statutory goal).

327. N.Y. PENAL LAW § 170.45 (McKinney 1984) (making a person is guilty of a class A misdemeanor criminal simulation when (1) "[w]ith intent to defraud, he makes or alters any object in such manner that it appears to have an antiquity, rarity, source or authorship which it does not in fact possess;" or (2) [w]ith knowledge of its true character and with intent to defraud, he utters or possesses an object so simulated."). The New York statute "substantially adopts a similar provision of the MODEL PENAL CODE (§ 224.2)." Staff Notes of the Commission on Revision of the Penal Law, N.Y. PENAL LAW § 170.45 (McKinney 1984).

328. Former N.Y. PENAL LAW § 959 was aimed at the "[r]eproduction or forgery of archeological objects." Staff Notes of the Commission on Revision of the Penal Law, N.Y. PENAL LAW § 170.45 (McKinney 1984).

329. N.Y. PENAL LAW § 170.45 (MCKINNEY 1984); *see* N.Y. ARTS & CULT. AFF. LAW § 13.03 (McKinney Supp. 1997) (falsifying certificates of authenticity for a work of fine arts is a class A misdemeanor).

330. *See* ALA. CODE § 13A-9-10 (1995); ALASKA STAT. § 11.46.530 (Michie 1996); ARIZ. REV. STAT. ANN. § 13-2004 (West 1989); ARK. CODE ANN. § 5-37-213 (Michie 1993); COLO. REV. STAT. § 18-5-110 (1990); CONN. GEN. STAT. ANN. § 53a-141 (West 1994); FLA. STAT. ch. 267.13 (1993); 9 GUAM CODE ANN. § 46.16 (1995); HAW. REV. STAT. § 708-855 (1993); IOWA CODE § 715A.3 (1997); KY. REV. STAT. ANN. § 516.110 (Banks-Baldwin 1995); ME. REV. STAT. ANN. tit. 17A, § 705 (West 1983); MISS. CODE ANN. § 39-7-27 (1996); MO. REV. STAT. § 570.090 (1979); MONT. CODE ANN. § 22-3-441 (1995); NEB. REV. STAT. § 28-606 (1995); N.H. REV. STAT. ANN. § 227-C:17 (1989); N.J. STAT. ANN. § 2C:21-2 (West 1995); OHIO REV. CODE ANN. § 2913.32 (Anderson 1996); OR. REV. STAT. § 165.037 (1995); 18 PA. CONS. STAT. ANN. § 4102 (1983 & Supp. 1997); S.D. CODIFIED LAWS ANN. § 1-20-37 (Michie 1992); TENN. CODE ANN. § 39-14-115 (1997); TEX. CODE ANN. § 32.22 (1994); UTAH CODE ANN. § 76-6-518 (1995 & Supp. 1997); VT. STAT. ANN. tit. 13, § 2023 (Supp. 1996); WIS. STAT. ANN. § 943.38 (West 1996).

331. These three states are Florida, Montana, and South Dakota. FLA. STAT. ch. 267.13 (1993) (limiting application to "any archaeological or historical object"); MONT. CODE ANN. § 22-3-441 (1995) (limiting application to heritage property or paleontological remains); S.D. CODIFIED LAWS § 1-20-37 (Michie 1992) (limiting application to "any archaeological, paleontological, ethnological or historical" object).

332. *E.g.*, CAL. CIVIL CODE §§ 1744(a)(10), 1745 to 1745.5 (West 1985 & Supp. 1997) (requiring disclosure of total size of limited editions with penalty not to exceed $1,000 for each violation); 815 ILL. COMP. STAT. § 345/0.01-9 (West 1997) (same).

use traditional statutes, such as conspiracy[333] or grand larceny, to prosecute art-related fraud.[334]

VIII. SENTENCING

Several provisions of the Guidelines are applicable to the theft of intellectual property.[335] This Section delineates the provisions applicable to each statute: the EEA, the NSPA, the Trade Secrets Act, the Mail and Wire Fraud statutes, RICO, the TCA and Copyright Felony Act, and False Marking and Counterfeiting or Forging Letters Patent statutes. Because a defendant may be prosecuted under any combination of these statutes, the grouping analysis must be considered when determining the defendant's sentence after a multi-count conviction.[336]

A. Economic Espionage Act of 1996

Defendants convicted of violating 18 U.S.C. § 1831 may be imprisoned for a maximum of fifteen years and/or fined $500,000.[337] Those convicted of violating § 1832 may be imprisoned for up to ten years and/or fined $500,000.[338] Defen-

333. In February 1987, the New York Attorney General's Office obtained the first felony convictions in the nation against the operators of a telephone boiler-room gallery in its conspiracy prosecution of four defendants in the Carol Convertine Gallery case. *See* Topolnicki & Green, *supra* note 284, at 73. The defendants reached potential customers over the telephone and by mailing brochures and price lists and providing false certificates of authentication. Two defendants pleaded guilty to conspiracy, and two others were convicted of nine counts of fraud. One defendant was convicted of an additional eight misdemeanor counts for the issuance of the false certificates. *See* CONKLIN, *supra* note 276, at 82–83. The gallery was in part supplied by another member of the Amiel family. *See* Douglas C. McGill, *Fake Art Prints: Big Business Getting Bigger*, N.Y. TIMES, July 22, 1987, at A1; *see also* United States v. Amiel, 813 F. Supp. 958, 959 (E.D.N.Y. 1993) (describing convictions obtained in that prosecution). In related civil litigation, a French corporation which claimed an exclusive license in Dalí works filed a civil RICO suit, under 18 U.S.C. § 1962(c) (enterprise involvement in racketeering), based on predicate acts of money laundering, mail fraud, and wire fraud. *See* Galerie Furstenberg v. Coffaro, 697 F. Supp. 1282, 1294 (S.D.N.Y. 1988) (dismissing plaintiff's money laundering, conspiracy, and trademark claims, but allowing civil RICO suit based solely on mail and wire fraud acts).

334. *See* People v. Mahboubian, 543 N.E.2d 34, 36 (N.Y. 1989) (discussing defendants' attempts to defraud insurance company by staging theft of art forgeries and collecting on the value of authentic pieces); *cf.* Bill Callahan, *Art Dealer Sentenced in Wieghorst Swindle*, SAN DIEGO UNION-TRIB., Sept. 27, 1989, at B3 (citing unreported California case in which art dealer Louis Almeida was convicted on six counts of grand theft, carrying sentence of up to seven and one half years in state prison, for selling forgeries of paintings of Olaf Wieghorst).

335. U.S. SENTENCING GUIDELINES MANUAL (1998) [hereinafter U.S.S.G. MANUAL].

336. U.S.S.G. MANUAL §§ 3D1.1–3D1.5 (1998) (explaining calculation of single offense level for multi-count convictions. This section explains how the U.S.S.G. MANUAL rules seek to provide incremental punishment for significant additional criminal conduct. To assess a multiple count sentence the most serious offense is used as a starting point. Any additional counts determine how much to increase the offense level, but, convictions on multiple counts do not result in a sentence enhancement unless they represent additional conduct that is not otherwise accounted for).

337. 18 U.S.C. § 1831(a) (Supp. IV 1998).

338. 18 U.S.C. § 1832(a) (Supp. IV 1998).

dants are sentenced under § 2B1.1,[339] which permits an increase by two offense levels for trade secret theft where the defendant knew or intended that it would benefit a foreign government, instrumentality, or agent.[340] Although the EEA mandates forfeiture of any proceeds or property derived from violations, property used to commit or facilitate the commission of the crime may be forfeited only at the discretion of the court.[341] Existing state law continues to provide alternative relief; the EEA specifically states that it does not "preempt or displace any other remedies, whether civil or criminal."

B. National Stolen Property Act

The NSPA imposes imprisonment for not more than ten years and/or a fine determined under Title 18.[342] Defendants convicted of violating the Act are sentenced under § 2B1.1.[343] The base offense level of four applies where the total loss to the victim is $100 or less.[344] The offense level rises as the financial loss to the victim increases, up to a maximum increase of twenty offense levels for losses exceeding $80,000,000.[345] Additionally, if the offense involved more than minimal planning, the offense level is increased by two levels.[346] If the defendant is a person in the business of receiving and selling stolen property, the offense level is increased by four levels.[347]

C. Trade Secrets Act

Violations of the Trade Secrets Act may result in a maximum one-year imprisonment, a fine determined under Title 18, or both; moreover, the convicted person is removed from office or employment.[348] Defendants are sentenced under § 2H3.1 of the Guidelines for a Trade Secrets Act conviction.[349] The base offense

339. U.S.S.G. MANUAL § 2B1.1 (1999). Section 2B1.1 covers offenses involving economic espionage under 18 U.S.C. § 1831 and also applies to theft of trade secrets violations as defined under § 1832.

340. U.S.S.G. MANUAL § 2.B1.1(b)(7) (1998).

341. 18 U.S.C. § 1834(a)(1) (Supp. IV 1998). The court may consider "the nature, scope, and proportionality of the use of the property in the offense." 18 U.S.C. § 1834(a)(2) (Supp. IV 1998). The forfeiture provision has been likened to the forfeiture provision in RICO. *See* Michael Coblenz, *Criminal Punishment of Trade Secret Theft Under New Federal Law: The Economic Espionage Act of 1996*, A.B.A. IP NEWSL., Spring 1997, at 11 & 49 (discussing factors court may consider in determining whether to impose forfeiture).

342. 18 U.S.C. § 2314 (1994) (describing who falls under the Act for crimes involving stolen property). Section 2314 was amended in 1994 to remove the outdated maximum fine. Pub. L. No. 103-322, Title XXXIII, § 330016(1)(L), 108 Stat. 1796, 2147 (1994).

343. U.S.S.G. MANUAL § 2B1.1 (1998).

344. U.S.S.G. MANUAL § 2B1.1(a), (b)(1) (1998).

345. U.S.S.G. MANUAL § 2B1.1(b)(1) (1998).

346. U.S.S.G. MANUAL § 2B1.1(b)(4)(A) (1998).

347. U.S.S.G. MANUAL § 2B1.1(b)(4)(B) (1998).

348. 18 U.S.C. § 1905 (1994) (making it a misdemeanor for any employee of the United States to disclose trade secrets "[t]o any extent not authorized by law").

349. U.S.S.G. MANUAL app. A (1998) (laying out the rules for invasions of privacy and eavesdropping).

level of nine is increased by three if the purpose of the conduct was to obtain commercial advantage or economic gain.[350] If the conduct facilitated another offense, § 2H3.1 requires the application of the guidelines for the other offense when that offense level is the greater of the two.[351]

D. Mail and Wire Fraud Statutes

Defendants convicted of mail and wire fraud risk a maximum five-year sentence and/or a fine determined under Title 18.[352] If the crimes affect a financial institution, fines can increase to $1 million and the prison term can expand to thirty years.[353] Defendants convicted of mail or wire fraud are sentenced under § 2F1.1 of the Guidelines.[354] The base offense level of six applies where the total loss to the victim is $2,000 or less.[355] As the financial loss to the victim increases, the offense level then rises up to a maximum increase of eighteen offense levels for losses exceeding $80 million.[356] Additionally, the offense level can be elevated by two levels if the offense was committed through mass-marketing[357] and by another two if the crime involved either a scheme to defraud more than one victim or more than minimal planning.[358]

E. Racketeer Influenced and Corrupt Organizations Act

Convictions under RICO carry a maximum sentence of twenty years and/or a fine determined under Title 18.[359] Additionally, RICO requires that the defendant forfeit any interests in enterprises established, operated, or maintained in violation of the statute.[360] Defendants convicted under RICO violations are sentenced under

---

350. U.S.S.G. MANUAL §§ 2H3.1(a)-(b) (1998) (setting the base level offense for economic gain from the crime).

351. U.S.S.G. MANUAL § 2H3.1(c)(1) (1998) (setting the guidelines for a cross reference offense).

352. 18 U.S.C. §§ 1341, 1343 (1994) (covering mail fraud and wire, radio or television fraud, respectively).

353. 18 U.S.C. §§ 1341, 1343 (protecting financial institutions in cases of mail and wire fraud).

354. U.S.S.G. MANUAL app. A (1998). For a complete discussion of sentencing under Wire and Mail Fraud, see the MAIL AND WIRE FRAUD article in this issue.

355. U.S.S.G. MANUAL §§ 2F1.1(a)-(b) (1998) (setting the base level offense).

356. U.S.S.G. MANUAL § 2F1.1(b)(1) (1998); *see* United States v. Austin, 54 F.3d 394, 402 (7th Cir. 1995) (upholding sentence based on sales revenue of $3.8 million, even though the art works "were worthless fakes" having no value).

357. U.S.S.G. MANUAL § 2F1.1(b)(3) (1998) (involving fraud or deceit through mass-marketing).

358. U.S.S.G. MANUAL § 2F1.1(b)(2) (1998); *see* United States v. Mett, 65 F.3d 1531, 1537 (9th Cir. 1995) (sustaining increased sentence).

359. 18 U.S.C. § 1963(a) (1994) (stating criminal penalties attendant to a RICO conviction). Two bills currently pending in Congress may affect sentencing under this and other statutes. 21st Century Law Enforcement and Public Safety Act, S. 2783, 106th Cong., 2d session (June 26, 2000), Money Laundering Act of 2000, H.R. 4695, 106th Cong,, 2d session (June 20, 2000).

360. 18 U.S.C. § 1963(a) (1994) (concerning any proceeds obtained from racketeering activity).

§ 2E1.1.[361] The Anticounterfeiting Consumer Protection Act of 1996[362] broadens the scope of RICO to include intellectual property violations but does not change the penalties.

F. Trademark Counterfeiting Act and Copyright Felony Act

Defendants convicted of violating the TCA face a prison term of not more than ten years and/or a fine of up to $2 million.[363] Organizations convicted of trafficking in counterfeit goods risk a maximum fine of $5 million.[364] However, a first-time conviction for trafficking goods that bear forged or counterfeited labels may result in not more than five years imprisonment and/or a fine determined under Title 18.[365] Upon a determination that any articles in the possession of a defendant bear counterfeit marks, the goods may be ordered destroyed.[366]

A violation of the Copyright Felony Act constitutes the reproduction or distribution, during any 180-day period, of at least ten unauthorized copies of one or more copyrighted works with a collective value of more than $2,500.[367] First-time offenders may be imprisoned for not more than five years[368] and/or fined not more than $250,000 for an individual, or $500,000 for an organization.[369] Repeat offenders risk an increase in the maximum prison sentence to ten years.[370] In addition, if the offender derives personal financial gain from the offense or causes third-party financial losses, the offender may be fined up to the greater of twice the gross gain or twice the gross loss.[371] The Copyright Felony Act prescribes a misdemeanor sentence of a maximum one-year imprisonment and a

---

361. *See* U.S.S.G. MANUAL app. A (1998). For a complete discussion of sentencing under RICO, see the RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT article in this issue.

362. Pub. L. No. 104–153, § 3, 110 Stat. 1386 (1996) (amending 18 U.S.C. § 1961(1)(B)).

363. 18 U.S.C. § 2320(a) (1994) (trafficking in counterfeit goods or services).

364. *See id.* § 2320(a) (1994) (requiring higher penalties for repeat offenders).

365. 18 U.S.C. § 2318(a) (1994 and Supp. IV 1998). In 1996, the statute was amended to include "computer program(s)." Pub. L. No. 104–153, §§ 4(a)-(b), 110 Stat. 1386, 1387 (1996).

366. 18 U.S.C. § 2320(b) (1994); *see* Vuitton v. White, 945 F.2d 569, 575–76 (3d Cir. 1991) (discussing requirements for relief under the ex parte seizure provision of the Act); Time Warner v. Does 1-2, 876 F. Supp. 407 (E.D.N.Y. 1994) (explaining that although Congress granted an ex parte seizure right for infringement cases, the search and seizure must comport with certain safeguards intended to guard civil defendants' Fourth Amendment rights. Specifically, the court held that a seizure carried out by a private investigator—not a United States Marshall—violates a civil defendant's Fourth Amendment rights).

367. 18 U.S.C. § 2319(b)(1) (1994). The Copyright Felony Act does not require that all affected copyrights be of the same class or held by the same copyright owner. *See* Saunders, *supra* note 131, at 690. The ten copies or phonorecords can be an aggregation of works by different authors, allowing for the establishment of a case of criminal copyright infringement against an infringer who has adversely affected several different copyright holders.

368. 18 U.S.C. §2319(b)(1) (1994) (explaining sentence for criminal copyright infringement).

369. 18 U.S.C. §§ 3571(b)-(c) (1994) (establishing a range of fines for individuals and organizations contingent upon loss to victim and the class of the felony of the conviction).

370. 18 U.S.C. § 2319(b)(2) (1994) (explaining sentence for repeat offender).

371. 18 U.S.C. § 3571(d) (1994).

fine not to exceed $100,000 for any criminal copyright infringement failing to meet the numerical thresholds described above.[372] Finally, § 506(b) grants the court the discretion to order the forfeiture and destruction of infringing items and all implements, devices, or equipment used in their manufacture.[373]

Violations of § 2319A can result in imprisonment for up to five years, and/or a fine determined under Title 18.[374] Subsequent offenses carry maximum ten-year sentences and/or fines.[375] The convicted must also surrender rights to the illegal material.[376]

Defendants convicted of trademark counterfeiting or criminal copyright infringement are sentenced under § 2B5.3 of the Guidelines,[377] starting with base offense level of six.[378] If the retail value of the infringing items exceeds $2,000, the offense level then rises as the financial loss to the victim increases, rising up to a maximum increase of eighteen offense levels for losses exceeding $80 million.[379] Retail value of the infringing items refers to the infringing items and not of the genuine items or materials; however, the retail value of the genuine items may be relevant in determining that of the infringing items.[380]

G. False Marking and Counterfeiting or Forging Letters Patent

False marking violations under § 292 result in maximum fines of $500 per

---

372. 18 U.S.C. §§ 2319(b)(3), 3571(b)(5) (1994).

373. 17 U.S.C. § 506(b) (1994); *see* United States v. One Sharp Photocopier, 771 F. Supp. 980, 984 (D. Minn. 1991) (finding that the government is entitled to forfeiture of a copier used to illegally duplicate software operations manual accompanying copyrighted computer software).

374. 18 U.S.C. § 2319A(a) (1994) (setting the sentence of fines).

375. *See id.* § 2319A(a) (1994) (defining the offense of trafficking involving musical performances).

376. 18 U.S.C. §§ 2319A(b)-(c) (1994) (stating that defendant must relinquish rights).

377. U.S.S.G. MANUAL App. A (1998) (This table is the same used for fraud and deceit).

378. U.S.S.G. MANUAL § 2B5.3(a) (1998) (setting the base offense level for trafficking).

379. U.S.S.G. MANUAL § 2B5.3(b)(1) (1998) (referring to § 2F1.1 table for increase in offense levels); *see* U.S.S.G. MANUAL § 2F1.1(b)(1) (1998). The reference in § 2B5.3 to the table contained in § 2F1.1 applies only to the actual table, not to the entire offense guideline, meaning that enhancements contained in § 2F1.1 are not applicable to defendants convicted of violating §§ 2319 or 2320. "An instruction to use a particular subsection or the table from another offense guideline refers only to the particular subsection or table referenced, and not to the entire offense guideline." U.S.S.G. MANUAL § 1B1.5(b)(2) (1998); *see also* United States v. Cho, 136 F.3d 982, 984-86 (5th Cir. 1998) (stating that § 2B5.3(b)(1) makes reference only to the table in § 2F1.1 and not to the table's prefatory sentence, stating "loss" is the offense characteristic as opposed to "retail value" in § 2B5.3(b)(1), which is the correct factor in determining sentence enhancement for defendant's trademark infringement conviction). *But cf.* Roger J. Miner, *Considering Copyright Crimes*, 42 J. COPYRIGHT SOC'Y U.S.A. 303, 307 (1995) (criticizing the Guidelines penalties for copyright felonies as "much too low").

380. *See* United States v. Kim, 963 F.2d 65, 67-71 (5th Cir. 1992) (holding that although the phrase "retail value of the infringing items" in the Guidelines refers to the value of actual counterfeit items, defendant did not provide sufficient evidence to calculate counterfeit handbags' retail value; thus, retail value of genuine Gucci and Vuitton handbags was relevant); *cf.* United States v. Larracuente, 952 F.2d 672, 674-675 (2d Cir. 1992) (holding "[w]here, as here, unauthorized copies are prepared with sufficient quality to permit their distribution through normal retail outlets, the value of the infringing items is their normal retail price to ultimate consumers who purchase from such outlets," but finding that the result may be different if "infringing items were of obviously inferior quality").

offense,[381] where each false marking is subject to a separate fine.[382] One-half of the proceeds from a § 292 conviction go to the citizen who brings the crime to the attention of the government; the other half goes to the United States.[383]

Violations of the Letters Patent statute[384] risk a maximum ten-year imprisonment and/or[385] fines pursuant to § 3571 of Title 18.[386] Defendants convicted of counterfeiting or forging letters patent are sentenced under § 2F1.1 of the Guidelines.[387]

CAROL NOONAN
JEFFERY RASKIN

Jeffrey Raskin is an associate at Greines, Martin, Stein & Richland LLP.

381. 35 U.S.C. § 292(a) (1994) (establishing fines for forgery and counterfeiting); *e.g.*, Accent Designs, Inc. v. Jan Jewelry Designs, Inc., 827 F. Supp. 957, 968-70 (S.D.N.Y. 1993) (applying § 292(a)'s fining mechanism).

382. *E.g.*, Krieger v. Colby, 106 F. Supp. 124, 131 (S.D. Cal. 1952) (imposing eight separate fines on defendants who received shipments of goods with labels violating the predecessor to § 292). *But see* Sadler-Cisar, Inc. v. Commercial Sales Network, Inc., 786 F. Supp. 1287, 1296 (N.D. Ohio 1991) (holding that "continuous markings over a given time constitute a single offense" under § 292(a)).

383. 35 U.S.C. § 292(b) (1994); *see* Mainland Indus., Inc. v. Standal's Patents, Ltd., 229 U.S.P.Q. (BNA) 43, 46 (D. Or. 1985) (holding that half the fines are payable to the United States), *aff'd*, 799 F.2d 746 (Fed. Cir. 1986) *overruled on other grounds by* A.C. Auckerman v. R.L. Chaides Const. 960 F2.d 1020 (Fed. Cir. 1992) (holding the burden of persuasion for summary judgment in a patent infringement case does not shift by reason of the patentee's six-year delay in bring suit).

384. 18 U.S.C. § 497 (1994) (letters patent statute).

385. 18 U.S.C. § 497 (1994) (setting imprisonment guidelines for false marking violations).

386. 18 U.S.C. § 3571(b) (1994) (outlining fines for individuals); 18 U.S.C. § 3571(c) (1994) (setting forth fines for organizations); 18 U.S.C. § 3571(d) (1994) (stating that fine equals twice gross gain or loss when violators have pecuniary gain or if victim suffer loss).

387. U.S.S.G. MANUAL app. A (1998) (pointing to the guidelines for forging letters patent).