Buffalo Intellectual Property Law Journal

Volume 2 | Number 1 Article 1

10-1-2003

Compliance Planning for Intellectural Property Crimes

Ray K. Harris
Fennemore Craig, P.C.

James D. Burgess Fennemore Craig, P.C.
false

BUFFALO
INTELLECTUAL PROPERTY
LAW JOURNAL

VOLUME 2 FALL 2003 NUMBER 1

ARTICLES

COMPLIANCE PLANNING FOR INTELLECTUAL PROPERTY CRIMES

RAY K. HARRIS†
JAMES D. BURGESS††

Infringement of intellectual property rights is not exclusively an issue for civil litigation. Increasingly, criminal law sanctions are available at both the federal and state level to deter intellectual property infringement.[1] The Department of Justice has published an IP crime prosecution manual addressing federal enforcement efforts.[2]

Two recent cases have drawn attention to the criminal law aspects of infringement of intellectual property rights:

†† Ray K. Harris is a Director at Fennemore Craig, P.C. in Phoenix, Arizona, and chairs its intellectual property practice. He is involved in commercial litigation, including intellectual property protection. He is a past chair of the Intellectual Property Section of the Arizona State Bar and a current Director of the Arizona Technology Council and the GSPED High Technology Industry Cluster. He is a graduate of the University of Arizona and its Law School, where he was Order of the Coif and Executive Editor of the Law Review.

† James D. Burgess is a Director at Fennemore Craig, P.C. in Phoenix, Arizona, and practices primarily business litigation and corporate compliance planning. He has developed compliance programs for companies in the high-tech, health care and manufacturing industries.

[1] In November 2001, the Council of Europe promulgated a cybercrime treaty signed by the United States. *See infra* note 159. Thus international law also recognizes criminal sanctions.

[2] David Goldstone, *Prosecuting Intellectual Property Crimes Manual*, Computer Crime and Intellectual Property Section (Jan. 2001), http://www.cybercrime.gov/ipmanual.htm.

•a Russian software developer, Demitry Sklyarov, and his employer, ElcomSoft, were federally indicted for circumventing e-book copyright protection technology in violation of the Digital Millennium Copyright Act.[3]

•Avant! Corporation was ordered to pay $195 million in restitution to Cadence Designs Systems, plus a $30 million fine, for trade secret theft under California law.[4]

In both examples, potential corporate criminal liability arose from violations of intellectual property rights by employees.[5] Congress and the courts are imposing criminal sanctions with greater frequency to protect intellectual property from misappropriation by competitors, former employees and hackers.

This article examines the criminal sanctions applicable to intellectual property infringement (trademarks, trade secrets and copyrights) and provides examples of reported criminal prosecutions. Corporate compliance planning is recommended to mitigate the risk of prosecution for intellectual property crimes.

---

[3] *See infra* note 160 *et seq.*

[4] *See infra* note 81 *et seq.*

[5] Related statutes offer some expanded protection for commercially sensitive and proprietary information. The National Information Infrastructure Protection Act of 1996 (PL 104-294) and the Computer Fraud and Abuse Act of 1996 criminalize unauthorized, intentional computer access resulting in damages. 18 U.S.C. § 1030 (a)(5)(B). *See* United States v. Middleton, 231 F.3d 1207 (9th Cir. 2000); America OnLine, Inc. v. LCGM, Inc., 46 F.Supp. 2d 444 (E.D. Va. 1998) (civil liability under state and federal computer crimes laws); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (civil liability for unauthorized use of computer system to e-mail trade secrets to competitor). The potential criminal liability under the Computer Fraud and Abuse Act is beyond the scope of this article. *See, e.g.,* M. Levinson & C. Paetsch, *The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information*, 19 COMPUTER & INTERNET LAWYER 11 (Sept. 2002).

This article also does not address the sale and export of encryption products commercially available overseas. Encryption software was regulated by the Department of State, and now by the Department of Commerce, as munitions. Exportation is limited by regulation. In 1997, a District Court in San Francisco held the regulations violate the First Amendment right to free speech. Bernstein v. U.S. Dep't of State, 974 F.Supp. 1288 (N.D. Cal. 1997), *aff'd,* 176 F.3d 1132 (9th Cir. 1999) *reh'g. granted*, 192 F.3d 1308 (9th Cir. 1999) *Accord* Junger v. Daley, 209 F.3d 481 (6th Cir. 2000). Another District Court had previously ruled the regulations did not violate free speech. Karn v. U.S. Dep't of State, 925 F. Supp. 1 (D.D.C. 1996), *remanded* 107 F.3d. 923 (D.C. Cir. 1997). In response the Clinton administration expanded the definition of encryption software eligible for exportation. 65 FR 2492 (2000).

I.
CRIMINAL PENALTIES APPLY FOR MISUSE OF INTELLECTUAL PROPERTY

A. Trademark Infringement

A trademark is any word, symbol or device that identifies the source of goods and distinguishes those goods from competitors' goods.[6] Examples include: Coca Cola® (U.S. Reg. No. 22,406); Microsoft® (U.S. Reg. No. 1,200,236); and the Nike swoosh design (U.S. Reg. No. 977,190). Trademarks arise at common law from use with the goods and can be registered under either federal or state law, or both.[7] Trademarks are protected under common law without any registration.[8] The first person to use a trademark has the common law right to prevent use of a similar mark by a competitor that is likely to cause confusion in the marketplace.[9]

To avoid infringement, it is common to conduct clearance searches to identify any similar registered or unregistered marks before adopting new trademarks.[10] Statutory trademark damages are available as civil damages in counterfeiting cases.[11]

Trademark protection prevents competitors from confusing customers by their misuse of the name of a successful company or product.[12] Trademark protection generally requires proof: (1) the mark identifies a single source of goods; and (2) a competitor's use of a colorable imitation[13] confuses customers.[14] A trademark holder's rep-

---

[6] 15 U.S.C. § 1127, ARIZ. REV. STAT. § 44-1441(a)(7); *Restatement (Third) of Unfair Competition* § 9. "A service mark is a trademark that is used in connection with services." *Restatement (Third) of Unfair Competition* § 9. In January 1995, the American Law Institute published *The Restatement (Third) of Unfair Competition*. The *Restatement (Third) of Unfair Competition* represents the only restatement of the law of unfair competition since 1939. Sections 9-31 deal with trademarks.

[7] 15 U.S.C. § 1051; ARIZ. REV. STAT. § 44-1442.

[8] 15 U.S.C. § 1125, ARIZ. REV. STAT. § 44-1452. *See Restatement (Third) of Unfair Competition* § 19 (priority of rights based on use).

[9] 15 U.S.C. §§ 1052(d), 1065, 1115(b)(5); Mister Donut of America, Inc. v. Mr. Donut, Inc., 418 F.2d 838, 842 (9th Cir. 1969). ARIZ. REV. STAT. § 44-1451(A); *Restatement (Third) of Unfair Competition* § 20.

[10] *See, e.g.,* Int'l Star Class Yacht Racing Ass'n v. Tommy Hilfiger U.S.A., Inc., 146 F.3d 66 (2d Cir. 1998).

[11] 15 U.S.C. § 1117(c) ($500-1,000,000 per mark).

[12] Trademark law protects both consumers (who can rely on trademarks to identify efficiently the product they want) and trademark owners (who can prevent piracy of their investment in reputation). *See, e.g.,* Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 773, *reh'g denied*, 505 U.S. 1244 (1992); Mana Products, Inc. v. Columbia Cosmetics Mfg., Inc., 65 F.3d 1063, 1068 (2nd Cir. 1995); Thomas & Betts Corp. v. Panduit Corp., 65 F.3d 654, 657-658 (7th Cir. 1995), *cert. denied*, 516 U.S. 1159 (1996).

[13] *See*, 15 U.S.C. § 1127. "Counterfeit" marks are distinguished from colorable imitations, and are subject to enhanced sanctions, including criminal sanctions. 15 U.S.C.

utation is harmed when potential purchasers of its goods see *unauthentic goods* using the trademark and identify these counterfeit goods with the trademark holder.[15]

1. Prosecution Under the Trademark Counterfeiting Act of 1984

Since 1984, knowingly using a counterfeit mark with intent to traffic in goods or services can result in criminal liability.[16] In the last four years, approximately a dozen cases have been prosecuted for trademark counterfeiting.[17] In a 1998 case, sales of counterfeit memory chips and boards in IBM boxes lead to $3.3 million in fines and restitution.[18] The $2.2 million fine was "one of the largest ever for a criminal trademark case".[19]

Criminal liability requires proof of use of a counterfeit mark. A counterfeit mark is "a spurious mark (i) that is used in connection with trafficking in goods or services; (ii) that is identical with, or substantially indistinguishable from, a mark registered for those goods or services . . .; and (iii) the use of which is likely to cause confusion, to cause mistake, or to deceived."[20]

---

§ 1116(d). *See also* Too, Inc. v. TJX Companies, Inc., 229 F. Supp. 2d 825 (S. D. Ohio 2002).

[14] *See, Restatement (Third) of Unfair Competition*, §§ 9, 20; 1 McCarthy, TRADEMARKS & UNFAIR COMPETITION, §§ 3:3, 23:1 (4th Ed. 1997); 15 U.S.C. § 1114(1)(a); Petro Shopping Centers, L.P. v. James River Petroleum, Inc., 130 F.3d 88, 92 (4th Cir. 1997). Registration is *prima facia* evidence of the validity of the mark and plaintiff's exclusive right to use the mark in commerce. 15 U.S.C. § 1057(b). *See* 15 U.S.C. § 1115(a). Civil remedies for trademark infringement include injunctive relief (15 U.S.C. § 1116), damages (15 U.S.C. § 1117) and attorneys fees "in exceptional cases" (15 U.S.C. § 1117).

[15] U.S. v. Hanafy, 124 F. Supp. 2d 1016, 1024 (N.D. Tex. 2000), *aff'd* 302 F.2d 485 (5th Cir. 2002); United States v. Torkington, 812 F.2d 1347, 1353 (11th Cir. 1987) (emphasis added) (quoted approvingly by United States v. Yamin, 868 F.2d 130, 133 (5th Cir. 1989)). The "post sale confusion doctrine" established in federal trademark law recognizes that trademark protection extends to future consumers. *See, e.g.,* Esercizio v. Roberts, 944 F.2d 1235 (6th Cir. 1991), *cert. denied*, 505 U.S. 1219 (1992); 3 McCarthy, TRADEMARKS AND UNFAIR COMPETITION § 23:7. Thus it is not a defense to liability (including criminal liability) that the counterfeiter disclosed the products were fake to the initial buyer. State v. Marchiani, 336 N.J. Super. 541, 765 A.2d 765 (2001).

[16] 18 U.S.C. § 2320(a). Criminal liability can also be imposed for trafficking in counterfeit labels, computer programs, documentation or packaging, or motion pictures. 18 U.S.C. § 2318.

[17] http://www.cybercrime.gov/ipcases.htm (chart of cases).

[18] *Violation of IBM Trademark Results in $3.3 Million Fine and Restitution for Chicago Area Company*, http://www.cybercrime.gov/desktop.htm.

[19] *Id.*

[20] 18 U.S.C. § 2320(e)(1)(A). *See* United States v. Petrosian, 126 F.3d 1232, 1234 (9th Cir. 1997), *cert. denied*, 522 U.S. 1138 (1998). U.S. v. Hanafy, 124 F. Supp. 2d, 1016, 1022 (N.D. Tx. 2000), *aff'd* 302 F.3d 485, 487 (5th Cir. 2002); U.S. v. Sultan, 115 F.3d 321, 325 (5th Cir. 1997).

A "spurious mark" is "one that is false or inauthentic".[21] In order to prove a violation of 18 U.S.C. § 2320(a), 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.[22]

In addition to an infringement under the ordinary standard of trademark infringement, criminal trademark counterfeiting requires use of a counterfeit mark registered on the principal register.[23] Criminal liability can only occur "if a spurious mark is used on or in connection with goods or services for which the genuine mark is actually registered . . . and is in use."[24]

The legislative history indicates that this 1984 legislation was intended to "help stem. . .an 'epidemic' of commercial counterfeiting" by providing "stiff criminal penalties for those who intentionally traffic in goods or services knowing them to be counterfeit."[25] One court has suggested, "Congress intended to criminalize all of the conduct for which an individual may be civilly liable."[26] Thus, in *U.S. v. Petrosian*, sale of a generic cola under the "Coca Cola" trademark (use of a genuine trademark affixed to a counterfeit product) lead to a criminal conviction under the statutes prohibiting use of a counterfeit mark.[27]

Not all courts agree, however, that every violation of trademark law constitutes criminal conduct. In July 2000, $1.9 million in cash was forfeited and four defendants were convicted for selling counterfeit

---

[21] U.S. v. Petrosian, 126 F.3d at 1234.

[22] U.S. v. Hanafy, 302 F.3d 485, 487 (5th Cir. 2002); United States v. Sultan, 115 F.3d 321, 325 (5th Cir. 1997).

[23] J. DRATLER, INTELLECTUAL PROPERTY: COMMERCIAL, CREATIVE, AND INDUSTRIAL PROPERTY § 11.09(4) (1999).

[24] S. Rep. No. 526, at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3627, 3636; U.S. v. Giles, 213 F.3d 1247, 1251 (10th Cir. 2000).

[25] S. REP. No. 98-526 at 5 (1984), *reprinted in* 1984 U.S. Code Cong. and Admin. News 3627, 3631. In 1996, Congress enhanced civil and criminal penalties for infringing copyrights and trademarks. Penalties can include fines up to $2 million and imprisonment for up to 10 years for individuals and fines up to $5 million for other legal entities. 18 U.S.C. § 2320(a). Individual repeat offenders can be fined up to $5 million and imprisoned up to 20 years and entities can be fined up to $15 million. *Id.* Trafficking in counterfeit goods is also now a predicate act under the RICO statutes. 18 U.S.C. § 1961(1). The predicate act provision can not be applied retroactively. Snowden v. Lexmark Int'l Inc., 237 F.3d 620 (6th Cir. 2001).

[26] U. S. v. Petrosian, 126 F.3d 1232, 1234 (9th Cir. 1997), *cert. denied.*, 522 U.S. 1138 (1998).

[27] U. S. v. Petrosian, 126 F.3d 1232 (9th Cir. 1997). *See also* U.S. v. Cho, 136 F.3d 982 (5th Cir. 1998)(retail value governs sentencing guidelines).

Enfamil infant formula.[28] The District Court Judge subsequently held the mark was not counterfeit because the goods were genuine and granted a motion for acquittal.[29] The Fifth Circuit affirmed. Repackaging genuine goods, even though actionable under civil trademark law,[30] is not criminal under 18 U.S.C. § 2320.[31]

As a criminal statute, the Trademark Counterfeiting Act must be construed narrowly.[32] However, a criminal statute must also be interpreted to accomplish its legislative purposes.[33] Even construed narrowly, however, the risk of prosecution remains.

2. *Prosecution Under State Trademark Law*

State law also prohibits use of counterfeit trademarks.[34] Arizona law, for example, recognized the possible imposition of criminal liability for sale of counterfeit goods.[35] In 1998, the Arizona legislature enhanced criminal penalties for the use of counterfeit marks.[36] The statutory elements are: (1) "knowingly and with intent to sell or distribute"; and (2) distributing "any item that bears a counterfeit mark".[37] An injured person may file an action for recovery of up to

---

[28] *Federal Jury Convicts Four Individuals on Charges of Trademark Counterfeit Conspiracy for Reselling Infant Formula*, http://www.cybercrime.gov/babyfood.htm. Conspiracy to sell counterfeit Similac baby formula lead to a recent conviction in another well publicized case. *Fugitive Who Sold Counterfeit Baby Formula Convicted of Federal Criminal Charges*, http://www.cybercrime.gov/mostafaConvict.htm.

[29] U.S. v. Hanafy, 124 F. Supp. 2d 1016 (N.D. Tex. 2000), *aff'd*, 203 F.3d 485 (5th Cir. 2002).

[30] *See* Prestonettes Inc. v. Coty, 266 U.S. 359 (1924) (repackaging must be disclosed on label); Enesco Corp. v. Price/Costco, Inc., 146 F.3d 1083, 1086 (9th Cir. 1998); Monsanto Corp. v. Heskel Trading, Inc., 13 F. Supp. 2d 349, 356-58 (E.D.N.Y. 1998).

[31] U.S. v. Hanafy, 302 F.3d 485 (5th Cir. 2002).

[32] *Id.*; U.S. v. Giles, 213 F.3d 1247 (10th Cir. 2000) (trafficking in counterfeit labels unattached to goods is not prohibited by law).

[33] State v. Marchiani, 336 N.J. Super. 541, 545, 765 A.2d 765, 767 (2001).

[34] *See, e.g.*, State v. Marchiani, 336 N.J. Super. 541, 765 A.2d 765 (2001); Nazemi v. Texas, 28 S.W.3d 806 (Tex. Ct. Crim. App. 2000).

[35] Ariz. Rev.Stat. § 44-1453 (2002). A Georgia statute attempting to criminalize use of trade names or logos as misleading e-mail addresses or hyperlinks was struck down under the First Amendment. American Civil Liberties Union of Georgia v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997). The use of trademarks on the Internet, however, may continue to elicit punitive legislation.

[36] Knowingly possessing or advertising an item bearing a counterfeit mark with intent to sell or distribute is a class 1 misdemeanor, and is a felony if the person has a previous conviction for counterfeiting or the value of the counterfeit goods is greater than $1,000. ARIZ. REV. STAT. § 44-1453 (2002). Knowingly using computer software that displays a counterfeit state registered mark for commercial purposes is a class 5 felony. *Id.* § 44-1455. Penalties can range from probation to 2 1/2 years in prison and a $150,000 fine.

[37] *Id.* § 44-1453(A). Common law unfair competition may be established by proof that the defendants engaged in deceptive practices causing confusion to the ordinary consumer. Wright v. Palmer, 11 Ariz. App. 292, 464 P.2d 363 (1970); Taylor v. Quebedaux, 617 P.2d 23, 24 (Ariz. 1980).

treble damages and the cost of suit—including reasonable attorneys fees.[38] Prior registration of intellectual property rights also gives the owner the benefit of various statutory presumptions.[39] The court may order restitution to the intellectual property owner.[40]

Soon after the changes in Arizona law took effect, sale of counterfeit software and apparel lead to well publicized prosecutions.[41]

Arizona also created a cause of action for trademark infringement against any person who distributes or uses an unauthorized copy of computer software, knowing it to be an unauthorized copy, if it displays a trademark registered in Arizona.[42] This provision has not yet been tested in the courts.

B. Misappropriation of Trade Secrets

Unlike trademark protection, which can arise under either federal or state law, trade secret protection has traditionally been a matter of state law alone. The classic example of a trade secret is the formula for Coke®. Typically, at least some employees must be given access to confidential, proprietary information. Because employment is increasingly transitory, proprietary information must be protected from disclosure to subsequent employers. Trade secret laws attempt to balance protection of the employer's proprietary information with utilization of the employee's training and experience.[43] The California Supreme Court will have to balance First Amendment rights in a case holding an injunction against disclosure of a trade secret (DVD decryption technology) as an impermissible prior restraint on speech.[44]

---

[38] ARIZ. REV. STAT. § 44-1453(J).

[39] *Id.* §§ 44-1444(B) (2002) (proof of state trademark registration), 1453(I) (facts stated in certificate of registration).

[40] *Id.* § 44-1453(F). Counterfeiting trademarks is a predicate offense under the Arizona RICO statute. *Id.* § 13-2301(D)(4)(bb) (2000). A single act will suffice to establish a pattern of activity. *Id.* § 13-2314.04(S)(3)(b).

[41] Judi Villa, *Raid Targets Software Sellers*, ARIZONA REPUBLIC, Oct. 1, 1998, at B1; Brent Whiting, *Vendor Accused of Sales of Counterfeit Products Police Seize Articles Stamped With bogus Labels*, ARIZONA REPUBLIC, Dec. 23, 1998, at 1.

[42] The legislation also makes the unauthorized use, removal or alteration of a software trademark, with the intent to deceive, a trademark infringement. The definition of infringement is modified to more closely parallel federal law. *Cf.* ARIZ. REV. STAT. ANN. § 44-1451(A)(1) (West 2003) *and* 15 U.S.C.A. § 1125 (West 2003).

[43] *See* Amex Distributing Co., Inc. v. Mascari, 724 P.2d 596, 602 (Ariz. Ct. App. 1986); RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 42, cmt. b (1995). Generally, although the *Restatement (Third) of Unfair Competition* employs its own terminology, the principles established are consistent with the Uniform Trade Secrets Act. Sections 39-45 address trade secret law.

[44] DVD Copy Control Assoc. v. Bunner, 113 Cal.Rptr.2d 338, 93 (Cal. Ct. App. 2001), *review granted* 117 41 P.3d 2 (Cal. 2002).

Arizona has adopted the Uniform Trade Secret Act definition of a trade secret as proprietary information, which (1) derives independent economic value, actual or potential, as a result of not being generally known or ascertainable; and (2) is subject to reasonable efforts to maintain secrecy.[45] Trade secret protection applies to formulas, patterns, compilations, programs, devices, methods, techniques or processes which give a company a competitive advantage because they are not generally known.[46]

While no specific set of security measures is mandated, trade secrets must be subject to "reasonable efforts" to maintain secrecy.[47] "[R]easonable efforts to maintain secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on 'need to know basis', and controlling plant access."[48] What is reasonable varies with the circumstances of each case, but, generally: physical access should be strictly limited; nonemployee access should be prohibited; proprietary statements should appear on all copies of confidential material; employees should be required to sign confidentiality agreements[49] and participate in exit interviews; employment manuals should describe material that is proprietary and confidential; and licenses should acknowledge that the material is proprietary and confidential, contain covenants against dis-

---

[45] ARIZ. REV. STAT. ANN. § 44-401(4) (West 2003). The *Restatement (Third) of Unfair Competition* defines a trade secret as "any information that can be used in the operation of a business enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995). "The concept of a trade secret as defined in this Section is intended to be consistent with" the Uniform Trade Secret Act. *Id.* at cmt. b.

[46] ARIZ. REV. STAT. ANN. § 44-401. Trade secrets include: strategic plans; product development materials; internal financial records; lists of key suppliers or employees; programs; methods; techniques; processes and know-how. *See* Prudential Ins. Co. of Am. v. Pochiro, 736 P.2d 1180, 1183 (App. 1987) (customer list); Morton v. Rogers, 514 P.2d 752, 756 (Ariz. Ct. App. 1973) (formula for cleaning solutions). Enterprise Leasing Co. of Phoenix v. Ehmke, 3 P.3d 1064 (Ariz. Ct. App. 1999) (financial records and expansion plans. Components of the trade secret may be in the public domain as long as the combination is not generally known and yields a competitive advantage as a result. Tracer Research Corp. v. National Environmental Services, Inc., 843 F.Supp. 568, 582 (D. Ariz. 1993).

[47] ARIZ. REV. STAT. ANN. § 44-401(4)(b) (West 2003). *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 39, cmt. g (1995) ("precautions to maintain secrecy may take many forms"). 1 ROBERT MILGRIM, TRADE SECRETS §1.04 (1995); Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174 (7th Cir. 1991); Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 901 (Minn. 1983).

[48] Uniform Trade Secrets Act § 1 cmt.

[49] Confidentiality agreements can be critical in establishing reasonable efforts to maintain secrecy. For example, an engineer who agreed to "forever keep secret" the employer's source code was recently sentenced to 2 years in prison after offering the software over the Internet. *Former Engineer of White Plains Software Company Receives Two Years in Prison for Theft of Trade Secret*, at www.cybercrime.gov/kissaneSent.htm.

closure, copying or reverse engineering, and require return of material upon termination.[50]

Misappropriation of a trade secret exposes the wrongdoer to injunctive relief and damages.[51] Misappropriation is acquisition or disclosure of secret information by improper means.[52] Improper means include: "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy or espionage."[53] The most common form of misappropriation, of course, results from hiring former employees with knowledge of the trade secret.[54] If a former employee goes to work for a competitor, the former employee and the competitor often receive a letter stating that the former employee had access to trade secrets and is under an obligation not to disclose those trade secrets in his new employment. One consequence of such a letter is the new employer may be sued as a joint tortfeasor for trade secret misappropriation.[55]

---

[50] *See, e.g.,* Data General Corp. v. Grumman Systems Support Corp., 825 F.Supp. 340, 359 (D. Mass. 1993), *aff'd in part*, 36 F.3d 1147 (1st Cir. 1994); Avtec Systems, Inc. v. Peiffer, 805 F.Supp. 1312 (E.D. Va. 1992), *modified*, 21 F.3d 568 (4th Cir. 1994).

[51] A.R.S. §§ 44-402, 403.

[52] A.R.S. § 44-401(2).

[53] A.R.S. § 44-401(1). *See Restatement (Third) of Unfair Competition*, § 43 (1995); *Chanay v. Chittendon*, 115 Ariz. 32, 38, 563 P.2d 287, 293 (1977) (actual theft is "just one of the many improper means by which the disclosure, use or procurement might take place").

[54] *See, e.g.,* Economy Roofing & Insulating Co. v. Zumaris, 538 N.W.2d 641 (Iowa 1995). *Cf* Tracer Research Corp. v. National Environmental Service Co., 843 F.Supp. 568 (D. Ariz. 1993) (former licensee). Misappropriation need not involve physical copying. A trade secret can be misappropriated by memory. MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993), *cert. dism'd*, 510 U.S. 1033 (1994); Ed Nowogroski Ins., Inc. v. Rucker, 88 Wash. App. 350, 944 P.2d 1093 (Wash. App. 1997); *review granted*, 958 P.2d 313 (1998) *aff'd*, 971 P.2d 936 (1999); Stampede Tool Warehouse, Inc. v. May, 272 Ill. App.3d 580, 209 Ill. Dec. 281, 651 N.E.2d 209 (1995), *app. denied*, 657 N.E.2d 639 (1995).

[55] A.R.S. §§ 44-401(2)(B)(i), 402(B); Uniform Act § 2, Commissioners' Comment ("The notice suffices to make the third party a misappropriator thereafter. . . ."); *Restatement (Third) of Unfair Competition*, § 40(b)(3), comment d and reporters' note ("letters and other communications sent to the defendant by the trade secret owner can establish that the defendant knew its use or disclosure was wrongful"); Salsbury Laboratories, Inc. v. Merieux Laboratories, Inc., 908 F.2d 706, 713 (11th Cir. 1990); Conmar Products Corp. v. Universal Slide Fastener Co., 172 F.2d 150, 156-57 (2d Cir. 1949). IDS Life Ins. Co. v. SunAmerica, Inc., 958 F.Supp. 1258 (N.D. Ill. 1997), *aff'd in part*, 136 F.3d 537 (7th Cir. 1998). *See* Uniform Act § 3, Commissioners' Comment (If a person materially changes position without knowledge of misappropriation, damages "should not be awarded for past conduct that occurred prior to notice that a misappropriated trade secret has been acquired"). *Cf.* A.R.S. § 44-402(B) (injunction may also be denied after change of position prior to notice of misappropriation). An employer need not have actual notice of an employee's violation of trade secrets of a competitor. Constructive notice is sufficient. Computer Associates Intern., Inc. v. Altai, Inc., 982 F.2d 693 (2nd Cir. 1992).

1. Prosecution Under the Economic Espionage Act of 1996

The Economic Espionage Act ("EEA") criminalizes theft of trade secrets.[56] The EEA created federal protection for property previously protected only by state law. The legislative history states the EEA covers conduct as diverse as stealing competitor's bid proposals or leaving employment with computerized engineering schematics.[57] Since October 1996, theft, attempted theft, or conspiracy to steal trade secrets from an owner or licensee subjects defendants to federal prosecution.[58]

The EEA has separate provisions governing foreign espionage[59] and domestic trade secret theft.[60] For domestic theft:

> (a) Whoever, 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, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.
>
> (b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.[61]

---

56 18 U.S.C. §§ 1831-1839 (2000) (effective Oct. 11, 1996).

57 H.R. Rep. No. 104-778 (1996).

58 18 U.S.C. § 1832 (imposing fines of up to $250,000 [up to $5 million for organizations] and imprisonment for up to 10 years).

59 18 U.S.C. § 1831.

60 18 U.S.C. § 1832.

61 *Id.*

The definition of a trade secret is arguably broader in the EEA than under the Uniform Trade Secrets Act.[62] The EEA recognizes a trade secret if: (a) the owner thereof has taken responsible measures to keep such information secret; and (b) the information derives independent economic value, actual or potential, from not being generally known to, or not being readily ascertainable through proper means by, the public. . .[63]

The EEA protects:

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.[64]

There is no minimum jurisdictional value.

The prospect of tax dollars funding litigation with a misappropriator is appealing and the federal law provides for protection of trade secrets during prosecution.[65] Forfeiture of property and profits earned is also provided.[66]

There is a loss of control of the federal prosecution, however, and a potential loss of control of the underlying trade secrets. In *U.S. v. Hsu,*[67] the District Court denied a strong protective order for Bristol-Myers trade secrets. The court concluded the defendant's constitutional right to access the incriminating evidence is paramount. The Third Circuit reversed, thereby providing some comfort to trade secret owners, but only because the crimes charged—attempt and conspiracy—do not require the existence of actual trade secrets.[68]

---

62 G. Dilworth, *The Economic Espionage Act of 1996: An Overview*, U.S. ATTORNEYS BULLETIN (May 2001) available at www.cybercrime.gov/usamay2001_6.htm; *See* U.S. v. Martin, 228 F.3d 1, 11 (1st. Cir. 2000).

63 18 U.S.C. § 1839(3).

64 *Id.*

65 18 U.S.C. § 1835.

66 18 U.S.C. § 1834.

67 982 F.Supp. 1022 (E.D. Pa. 1997), *reversed* 155 F.3d 189 (3d Cir. 1998).

68 155 F.3d 189 (3d. Cir. 1998).

Federal prosecutions have been pursued in connection with technologies owned by a range of companies.[69] Approximately 35 cases have been brought under the Economic Espionage Act.[70]

In *United States v. Martin,* a classic example of bumbling theft, conspiratorial e-mail was inadvertently distributed to other employees of the victim.[71] The co-conspirator (who entered into a plea agreement in return for testimony against the defendant) sent a series of e-mail acknowledging "I feel like a spy", "they know I've been stealing, so to speak, from the company in sending info to someone" and received encouragement to "absorb as much information, physically and intellectually, as you can."[72] The court upheld the conviction under the Economic Espionage Act, "which applies to attempts or conspiracies to steal trade secrets."[73] A reasonable jury could conclude that the co-conspirator had formed an agreement to convey information to the defendant in violation of the statute.

> A careful reading of the 7-month e-mail communication between Dr. Steven Martin and Karyn Camp could lead to the conclusion that Martin and his counsel urge—that this is simply a pen-pal relationship between a lonely Maine lab technician and a reclusive California scientist. However, the evidence could also lead a reader to the conclusion that something far more sinister was afoot: that an originally harmless communication mushroomed into a conspiracy to steal trade secrets and transport stolen property interstate, and that the electronic mail and U.S. mails were used to further a scheme to defraud IDEXX. Because we find there was sufficient evidence for a reasonable jury to conclude the later beyond a reasonable doubt, we affirm the defendant's conviction on all counts.[74]

Dr. Martin served about 1 year in prison (January to November 2000).[75]

---

[69] *See, e.g.,* E. Herman, *Kodak Under Cover,* CORP. COUNSEL MAGAZINE, (Dec., 1997) at 53, 62; D. Osborne, *Trading Secrets*, AM LAW TECH, (Winter, 1998) at 45; *Protecting Trade Secrets Requires Many Approaches*, CORP. LEGAL TIMES (Oct., 1998); R. Deger, *Grand Jury Indicts Avant Executives*, THE RECORDER (Dec. 18, 1998), J.D. Mason, G. Mossinghoff & D. Oblon, *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets* 16 THE COMPUTER LAWYER 14 (March 1999). Hosteny & Kamp, *Corporate Espionage: Protecting Trade Secrets*, ACCA DOCKET (Jan./Feb. 1999) at 18.

[70] V. Slind-Flor, *Trade Secrets in the Age of Terrorism*, IP WORLDWIDE at 12 (July 2002); www.cybercrime.gov/eeapub.htm (chart of cases). For the first five years (until October 2001) every prosecution had to be approved by the Department of Justice. 28 CFR § 50.64-5; U.S. Attorney's Manual § 9-59-100 (Sept. 1997).

[71] 228 F.3d 1 (1st Cir. 2000).

[72] Id. at 10

[73] 228 F.3d at 10-11.

[74] 228 F.3d at 19.

[75] P. Toni, *Perils of E-Mail*, *at* http://abcnews.go.com/sections/business/TechTV/techtv_emailespionage020327.html.

In *U.S. v. Yang*[76] the defendants were also convicted based upon the testimony of a co-conspirator cooperating with the prosecution. The misconduct was originally disclosed by an employee of the defendants seeking employment from the victim. On appeal the imposition of the maximum fine against the defendant corporation ($5 million) was vacated.[77] In addition to the criminal prosecution, a civil action was filed by the victim. The court in the civil action reportedly froze the assets of the defendants. After the criminal conviction, the victim, Avery Denison, reportedly obtained a civil judgment of $10 million for misappropriation of trade secrets and $30 million in punitive damages.[78]

Thus, criminal and civil sanctions can be substantial.

2. *Prosecution Under State Law*

Arizona has not criminalized trade secret misappropriation as such.[79] At least 17 states do have Criminal Code provisions referring to theft of trade secrets, including California.[80]

The California courts have considered several state law trade secret prosecutions. Cadence Design Systems, Inc. ("Cadence") claimed trade secret misappropriation by Avant! Corp. . Cadence pursued a civil action against Avant! while the Santa Clara County district attorney pursued a parallel state criminal complaint.[81] Controversy ensued over the role of the victim in assisting the prosecution.[82] The criminal action was resolved after four years with guilty

---

[76] 74 F. Supp.2d 724 (N.D. Ohio 1999), *aff'd in part vacated in part*, 281 F.3d 534 (6th Cir. 2002).

[77] *Id.*

[78] James Repass, Michael McCoy, *The Economic Espionage Act: How Companies Can Use it on the Offensive*, 7 THE INTELLECTUAL PROPERTY STRATEGIST, 1, 3 (Dec. 2000).

[79] ARIZONA REV. STAT. ANN. § 13-1801 (B) 2003 (Liability . . .theft). §13-2310 (a scheme or articulate to defraud), § 13-2316 (A), (E) (or computer fraud). §13-105(32) (Protection extends to intellectual property). §13-2301(D)(4)(v), (xx) (Theft . . . statute).

[80] DRATLER, INTELLECTUAL PROPERTY LAW: COMMERCIAL, CREATIVE & INDUSTRIAL PROPERTY, § 13.04(3)(c); CAL. PENAL CODE § 499c (1999).

[81] *See* Cadence Design Systems, Inc. v. Avant! Corp., 125 F.3d 824 (9th Cir. 1997), *cert. denied*, 118 S.Ct. 1795 (1998), *after remand*, 189 F.3d 472 (9th Cir. 1999) (table), *question certified to Cal S. Ct.*, 253 F.3d 1147 (9th Cir. 2001).

[82] The California Supreme Court had previously dismissed a state indictment because of the involvement of the victim in providing expert testimony and financial support to the prosecution. People v. Eubanks, 927 P.2d 310 (1997). *But see* IBM Corp. v. Brown, 857 F. Supp. 1384 (C.D. Cal. 1994). In *U.S. v. Yang*, 281 F.3d 534, 545 (6th Cir. 2002), the Sixth Circuit noted Avery made available to the prosecutors "the same loss evaluation experts Avery intended to use in the parallel civil case." This participation was "wholly irrelevant to either the defendant's guilt or the nature or extent of his sentence" and consideration of the victim's participation was an abuse of discretion. *Id.* at 546.

plea, payment of fines totaling over $30 million and restitution to Cadence totaling $195 million.[83]

In an opinion ordered not officially published, the California Court of Appeals reversed a conviction of misappropriating a trade secret under California State Law, Penal Code Section 499c. The technology was circuitry for an electronic testing device. The prosecution was based on a "crumbled paper containing a . . . simplified block diagram of the IQ modulator". The definitions of trade secret in the penal code and civil code are identical.[84] The court found there was no evidence that the technology derived value from its secrecy.[85] The court also found that there was no specific intent to deprive the owner of the trade's secret value for personal gain or competitive advantage.[86] The defendant used the diagram in a job interview with a company that did not compete with his former employer.[87]

California has also ruled that theft of trade secrets worth more than $50,000 triggers a minimum sentence statute requiring at least 90 days in County jail as a condition of probation.[88] Therefore, an engineer employed at Digital Equipment Corporation was required to serve the minimum sentence upon pleading guilty to theft of trade secrets in an amount exceeding $100,000. The court noted that the purpose of the minimum sentence statute was to vigorously prosecute white-collar crime and ensure restitution to victims. Those purposes would not be served by excluding theft of property that had substantial value, but was not cash or a cash equivalent.

C. Copyright Infringement

Copyright protection, unlike trade secrets or trademarks, is exclusively the province of federal law.[89] Copyright protection exists for any "original works of authorship" reduced to a tangible form.[90] The copyright owner has the exclusive right: (1) to reproduce the work, (2) to prepare derivative works, (3) to distribute copies to the public, (4) to perform the work publicly, and (5) to display the work pub-

---

[83] Victoria Slind-Flor, *Did Cadence Get Short-Changed in Criminal Trade Secrets Case?* IP WORLDWIDE (Oct. 2001); Shannon Lafferty, *Avant Success May Give Prosecutor Ammunition in Trade Secrets Case,* THE RECORDER, May 23, 2001, at 1.

[84] *People v. Hsieh*, 103 Cal. Rptr. 2d 51, 56 n.4 (Ct. App. 2000). *Compare* Cal. Civil Code § 3426.1(d) *and* Cal. Penal Code § 499c(a)(9). Both conform to the definition in the Uniform Trade Secrets Act. *Hsieh,* 103 Cal. Rptr. 2d at 55 n.4.

[85] *Id.* at *58.*

[86] *Id.* at 60-61.

[87] *People v. Hsieh*, 103 Cal.Rptr.2d 51 (Ct. App. 2000).

[88] Penal Code § 1203.044 (People v. Farell, 28 Cal. 4th 381, 384 (2002)).

[89] *See infra* note 160.

[90] 17 U.S.C. § 102 (1976).

licly.[91] The software, music and movie industries rely heavily on copyright protection of their intellectual property.

The elements of a prima facie case for copyright infringement are: (1) Ownership of a valid copyright; and (2) Copying of protected expression.[92] Copyright ownership is usually established by proving registration.[93] Copying can be inferred through circumstantial evidence of access, if the works are "substantially similar."[94] Unauthorized copying constitutes copyright infringement subject to civil and criminal liability.[95]

Certain uses which works otherwise constitute infringement are within the statutory fair use defense.[96] To the extent there is a reasonable licensing procedure available, however, copying without a readily available license may not be deemed fair use.[97] Licensing programs are available through the Copyright Clearance Center[98] and UMI Article Clearing House for printed material and through BMI and ASCAP[99] for music.

Recent controversies have required the courts to apply copyright law to Internet use and peer-to-peer file transfer technologies.[100] One Arizona corporation agreed to a $1 million out of court settlement with Recording Industry Association of America ("RIAA"), resulting from employee use of a corporate file server to distribute MP3 files over the Internet.[101] The RIAA recently sent a warning letter to For-

---

91 17 U.S.C. § 106.

92 *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 361 (1991). *See also* Apple Computer, Inc. v. Microsoft Corp., 35 F.3d 1435, 1442 (9th Cir. 1994), *cert. denied*, 513 U.S. 1184 (1995); registration is *prima facie* evidence of copyright ownership and validity. 17 U.S.C. § 410(c). Civil remedies for copyright infringement include injunctive relief (§ 502), damages (§ 504) and costs and attorneys fees (§ 505).

93 Johnson Controls, Inc. v. Phoenix Control Sys., Inc., 886 F.2d 1173, 1175 (9th Cir. 1989).

94 Apple, 35 F.3d at 1442.

95 *See* American Geophysical Union v. Texaco, Inc., 60 F.3d 913 (2d Cir. 1994), *cert. denied*, 516 U.S. 1005 (1995) (civil liability for duplication of published scientific articles). *See also supra* note 11.

96 17 U.S.C. § 107.

97 *See* American Geophysical Union, 60 F.3d at 913.

98 www.copyright.com.

99 www.bmi.com, www.ascap.org.

100 *See* A&M Records, Inc. v. Napster, Inc., 114 F.Supp.2d 896 (N.D. Cal. 2000), *aff'd in part*, 239 F.3d 1004 (9th Cir. 2001); Universal City Studios v. Reimerdes, 111 F. Supp.2d 294 (S.D.N.Y. 2000), *aff'd*, 273 F.3d 429 (2d Cir. 2001); UMG Recordings, Inc. v. MP3.com, Inc., 92 F.Supp. 2d 349, 54 U.S.P.Q.2d 1376 (S.D. N.Y. 2000). *See also* David Goldstone & Michael O'Leary, *Novel Criminal Copyright Infringement Issues Related to the Internet*, US ATTORNEY'S BULLETIN (May 2001), *available at* http://www.cybercrime.gov/usamay2001_5.htm.

101 *RIAA Collects $1 Million From Company Running Internal Server Offering Thousands Of Songs* (April 9, 2002), *available at* http://www.riaa.org/news/newsletter/040902_2.asp.

tune 1000 companies and 2000 University presidents regarding use of powerful network computers to support illegal "warez" sites that share copyrighted software, music and video.[102] Corporations can be held liable for vicarious or contributory copyright infringement based on the conduct of employees.[103]

Software industry groups, such as the Business Software Alliance, have been formed to combat software piracy. The Sixth Annual Business Software Alliance Global Software Piracy Study estimated worldwide software piracy losses at $11.75 billion in 2000 (one third of all business software applications).[104] These organizations are increasing their efforts to combat software piracy, both domestically and internationally.

1. Criminal Prosecution for Copyright Infringement

To prove misdemeanor copyright infringement: the prosecution must show: (1) that someone other than the defendant owned the copyright at issue; and (2) that the defendant violated one or [sic] more of the copyright owner's exclusive rights under Section 106.[105]

Although willful copyright infringement for profit has technically been a misdemeanor since 1909, there have been few prosecutions.

Until 1992, only copyright infringements involving sound recordings or motion pictures constituted felonies (punishable by more than one year in jail). Software Publishers Association ("SPA," now known as Software and Information Industry Association) was active in obtaining legislation (PL 102-561) expanding criminal penalties to cover any copyrighted work, including software. To prove felony copyright infringement, "the defendant must have violated the copyright owner's reproduction or distribution right; mere violation of the right of adaptation (preparation of derivative works), public performance, or public display is not enough."[106] The felony criminal sanctions were originally imposed only if the infringement was committed "will-

---

[102] John Borland, *Studios, RIAA Warn CEOs on File Trading*, CNET News.com (Oct. 24, 2002), *available at* http://zdnet.com.com/2102-1106-963208.html; John Borland, *Hollywood Chases Down Campus Pirates*, CNET News.com Oct. 10, 2002 *available at* http://zdnet.com.com/2102-1106-961637.html.

[103] Fonovisa v. Cherry Auction, 76 F.3d 259 (9th Cir. 1996); CoStar Group, Inc. v. LoopNet, Inc., 164 F. Supp. 2d 688 (D. Md. 2001).

[104] SIXTH ANNUAL BSA GLOBAL SOFTWARE PIRACY STUDY 2 (May 2001), *available at* www.bsa.org/resources2001-05.21.55.pdf.

[105] JAY DRATLER, JR., INTELLECTUAL PROPERTY LAW: COMMERCIAL CREATIVE AND INDUSTRIAL PROPERTY § 13.04[1][a], (1994-2003).

[106] *Id.*

fully and for purposes of commercial advantage or private financial gain."[107]

> In enacting the enhanced criminal penalties, Congress recognized that the term "willfully," although used in copyright statutes since 1897 for criminal violations, has never been defined.[108]

Making at least ten copies of a copyrighted work, with a retail value of more than $2,500, during a six-month period, is required for a felony.[109] In determining the threshold for felony copyright infringement:

> The term "retail value" is deliberately undefined, since in most cases it will represent the price at which the work is sold through normal retail channels . . . In [appropriate] cases, the courts may look for the suggested retail price, the wholesale price, the replacement cost of the item, or financial injury costs of the copyright owner.[110]

In *U.S. v. Manzer,*[111] the defendant was ordered to pay $2.7 million in restitution after a criminal conviction and was also required to pay a civil judgment of $2 million. Software companies and their policing organizations are actively encouraging United States Attorneys to pursue wrongdoers aggressively. In the last four years, over 30 cases of criminal copyright infringement have been prosecuted.[112]

2. *Prosecution Under the No Electronic Theft Act of 1997*

In a well-publicized case, a student posting software on the Internet caused over $1 million in damage but did not commit a crime because the student did not intend to profit from his conduct.[113] The No Electronic Theft ("NET") Act eliminated the requirement of "commercial advantage or private financial gain" by substituting

---

[107] 17 U.S.C. § 506(a). Use or removal of a copyright notice with fraudulent intent, or knowingly making a false representation of material fact in a copyright registration application shall result in a fine of not more than $2,500. 17 U.S.C. § 506(c)-(e).

[108] H.R.REP. No. 102-997 at 5 (1992), *reprinted in* 1992 U.S.C.C.A.N. at 3573. *See* U.S. v. Manzer, 69 F.3d 222 (8th Cir. 1995) (copyright notice in program read through use of a common debug program or "DUMP" file sufficient to prove willful infringement).

[109] Felony copyright infringement is subject to imprisonment for not more than five years and a fine of up to $250,000 for individuals and $500,000 for corporations. 18 U.S.C. §§ 2319(b)(1), 3571. Enhanced penalties for repeat offenders extend to 10 years imprisonment. In January 2001, a domain name (www.software-inc.com) was forfeited in connection with a guilty plea for unauthorized sale of computer software. 61 PTCJ 260 (1/12/01).

[110] H.R.REP. No. 102-997, at 6-7 (1992), *reprinted in* 1992 U.S.C.C.A.N. at 3574-75. *See* U.S. v. Larracuente, 952 F.2d 672, 674 (2nd Cir. 1992) (using the normal retail price rather than the lower bootlegged price paid for illegitimate copies).

[111] 69 F.3d 222 (8th Cir. 1995).

[112] www.cybercrime.gov/ipcases.htm (chart of cases). These cases include NET Act and DMCA cases, see part 2 and 3 *infra*.

[113] United States v. LaMacchia, 871 F.Supp. 535 (D. Mass. 1994).

proof of reproduction or distribution of one or more copyrighted works with a total retail value of over $1000 in a 180 day period.[114] This change allows prosecution of bulletin board operators who willfully copy and distribute works (typically software) worth more than $1,000.

On November 23, 1999, a 22-year-old Oregon college student, Jeffrey Levy, pled guilty posting software, videos and music to his Web site.[115] This was the first conviction under the NET Act. In 2001, seventeen "Pirates with Attitude" (5 former Intel employees and 12 others), were indicted under the NET Act in Chicago.[116] On May 15, 2001, after 13 defendants had plead guilty to copyright conspiracy, one defendant was convicted at the first trial under the NET Act.[117] By October 2002, Operation Buccaneer resulted in 16 felony copyright infringement convictions in the United States with sentences imposed of up to 46 months in federal prison.[118]

3. *The Impact of the Digital Millennium Copyright Act of 1998*

a. *Safe Harbors for Internet Service Providers*

Potential liability for copyright infringement has been seen as an impediment to the growth of electronic commerce. Internet Service Providers ("ISPs")[119] can now be shielded from liability for damages arising from copyright infringement if they register with the U.S. Copyright Office and designate an agent to receive notifications of claimed infringement.[120] The Digital Millennium Copyright Act

---

114 PL 105-147. 111 Stat. 2678. *See also* 17 U.S.C. § 506(a)(1)-(2).

115 U.S. Dep't of Justice press release, *First Criminal Conviction Under the "No Electronic Theft" (NET) Act for Unlawful Distribution of Software on the Internet* (Aug. 20, 1999), at http://www.cybercrime.gov/netconv.htm.

116 Darryl van Duch, *Eyes on 'Pirates' Trial in Chicago Can Prosecutors Succeed if Defendants Didn't Gain Financially*, NAT'L L.J., Mar. 26, 2001; U.S. Dep't of Justice press release, U.S. Indicts 17 in Alleged International Software Piracy Conspiracy (May 4, 2000), at http://www.cybercrime.gov/pirates.htm.

117 U.S. Dep't of Justice press release, *Software Pirates Guilty of Copyright Infringement Under NET Act* (May 15, 2001), *at* http://www.cybercrime.gov/pwa_verdict.htm; Business Software Alliance press release, First Guilty Verdict Under NET Act Draws Praise (May 15, 2001), at http://www.bsa.org/usa/press/newsreleases/2001-05-15.553.phtml.

118 *See* U.S. Dep't of Justice, Operation Buccaneer (last updated Oct. 7, 2002), *at* http://www.cybercrime.gov/ob/OBMain.htm.

119 "A service provider generally includes an entity offering the transmission, routing or connections for digital online communications, [including (except for transmission without modification)] a "provider of online services or network access, or the operator of the facilities therefore." 17 U.S.C. § 512(k)(1). The broad definition will include many companies providing Internet access.

120 A summary of the regulations is available on the Library of Congress website *at* http://lcweb.loc.gov/copyright/onlinesp/. *See* Annot. 2001 ALR Fed.2 (Validity, Construction and Application of DMCA).

("DMCA")[121] limits the copyright owner to injunctive relief (removal of the infringing material) against an ISP unless the ISP: (1) initially placed the material on-line; (2) generates, selects, or alters the content of the material; (3) determines the recipients of the material; (4) receives a financial benefit directly attributable to a particular act of infringement; (5) sponsors, endorses, or advertises the material; or (6) knows, or is aware by notice or other information indicating that the material is infringing.

ISPs are generally protected if they merely operate as a conduit ("transmission . . . without modification"),[122] if material provided by a third party is automatically cached,[123] or if the ISP stores or links to infringing material without knowledge of the infringement or a financial benefit attributable to the infringing activity.[124] The ISP must adopt, implement and notify subscribers of a termination policy for repeat infringers.[125] Knowledge is imputed if the ISP is, "aware of facts or circumstances from which infringing activity is apparent".[126]

The ISP must "respond expeditiously to remove, or disable access to, material" made available online by a person other than the service provider "that is claimed to be infringing"[127] in order to claim, the exemptions for (1) system caching[128] and (2) lack of benefit and control.[129] Even if the material or activity is ultimately determined not to be infringing, an ISP is not liable for disabling access to or removing material in a good faith response to: (1) a notice of infringement[130] or (2) "facts or circumstances from which infringing activity is appar-

121 Digital Millennium Copyright Act, Pub. L. No. 105-304; (codified as amended at 17 U.S.C. § 1201 - 05).

122 17 U.S.C. § 512(a).

123 *Id.* § 512(b).

124 *Id.* § 512(c)-(d).

125 The service provider must adopt, implement and inform subscribers of a policy that provides for termination of repeat infringers and accommodates "standard technical measures." Standard technical measures means technical measures used by copyright owners to identify or protect copyrighted works that have: (1) developed "pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process"; (2) are available on reasonable and non-discriminatory terms; and (3) do not impose "substantial costs on service providers or substantial burdens on their systems or networks". *Id.* § 512(i).

126 § 512 (d)(1)(B).

127 § 512(b)(1), § 512(b)(2)(E).

128 § 512(b)(1), § 512(b)(2)(E).

129 § 512(c)(1)(c), § 512(d)(3).

130 The registrar of copyrights maintains a current directory of designed agents for receipt of notice. *See* http://www.loc.gov.copyright/onlinesp. The designation must be accompanied by a $20 fee. *See* 37 CFR 201.38.

ent".[131] Substantial compliance with the notice provision is sufficient.[132]

The ISP must "take reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material."[133] The source of the material can than have access reinstated by serving a counter notification. The ISPs replacement or removal of disabled material in response to a counter notification will not subject the ISP to liability for copyright infringement.[134]

No obligation is imposed on ISPs to seek information indicating materials infringe. Liability for direct infringement against a passive service provider is precluded by the legislative history of the DMCA, but the ISP can be liable for contributory infringement after receiving actual or constructive notice under the DMCA.[135] Cases such as *Playboy Enterprises, Inc. v. Webbworld, Inc.*[136] would still result in liability for website operators who sell infringing material and profit from the infringement—even in the form of a fixed monthly fee. Peer to peer distribution of copyrighted material does not meet the safe harbors available under the Digital Millennium Copyright Act.[137]

EBay and its employees have been held immune from liability under the DMCA safe harbor provisions.[138] The same District Court recently held that America Online was also within the safe harbor provision,[139] but an adult website age verification service was not.[140]

b. Civil Liability

The DMCA technically does not define "copyright infringement." Instead the DMCA creates liability in "a niche distinct from

---

131 17 U.S.C. § 512(g)(1).

132 ALS Scan Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001) (ISP could be liable for failure to take down infringing photographs by 2 news groups).

133 17 U.S.C. § 512(g)(2)(A).

134 *Id.* § 512(g)(4).

135 ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619 (4th Cir. 2001).

136 991 F. Supp. 543 (N.D. Tex. 1997).

137 *See* A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000), *aff'd in part*, 239 F.3d 1004 (9th Cir. 2001), *on remand*, 2001 WL 227083 (N.D. Cal. Mar. 5, 2001) (Judge Patel ordered Napster to remove songs identified by the plaintiffs within 3 days); Thomas E. Barako, *Finding. . .Liability*, 42 JURIMETRICS J. 1 (2001).

138 Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (the copyright owner did not comply with the requirements of the statutory written notice).

139 Ellison v. Robertson, 189 F. Supp.2d 1051 (C.D. Cal. 2002).

140 Perfect 10, Inc. v. Cybernet Ventures, Inc., 2002 WL 731721 (C.D. Cal. Apr. 22, 2002); *See* Costar Group, Inc. v. LoopNet, Inc., 164 F. Supp. 2d 688 (D. Md. 2001) (genuine issues of material fact found to exist regarding protection under the DMCA).

copyright infringement".[141] The impact of the DMCA on copyright related issues, however, merits discussion.

The DMCA prohibits manufacturing or trafficking in any technology, product, service or device primarily designed: (1) for the purpose of circumventing a technological measure to control access to a protected work (i.e. descrambling a scrambled work, decrypting an encrypted work),[142] or (2) for the purpose of circumventing copy protection[143] afforded by a technological measure.[144] Opponents argued the provision against circumventing copy protection would limit the statutory fair use doctrine and prevent access to material not protected by copyright. A variety of exemptions to the prohibition on circumventing technological measures are contained in the statute.[145]

In addition, the DMCA provides that no person shall provide false copyright management information[146] or intentionally remove or alter any copyright management information.[147] Copyright management information includes: (1) the title and other information identifying the work; (2) the name and other identifying information about the author, (3) the copyright owner, or the performer; (4) the terms and conditions for use of the work or such other information as the Register of Copyrights may prescribe by regulation.[148] Again, certain exemptions are provided, for example, to preserve fair use[149] to insure that the design or selection of components for any consumer electronics, telecommunications or computer product does not need to "provide for a response to any particular technology measure"[150] and to protect privacy.[151]

Civil libertarians have argued that the DMCA goes too far in protecting the rights of copyright owners.[152] The fair use defense (17

---

141 RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D. Wash. Jan. 18, 2000), (*quoting* 1 NIMMER COPYRIGHT § 12.A17[B].)

142 17 U.S.C. § 1201(a)(2) (2003).

143 Copy protection is used here as shorthand for protection of all rights of the copyright owner under 17 U.S.C. § 106 (2003).

144 17 U.S.C. § 1201(b)(1) (2003). *See* RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

145 In October 2000, the Copyright Office granted additional exemptions from liability for circumventing a technological measure to control access to 2 classes of works: compilations of websites blocked by filtering software; and access control mechanisms failing due to malfunction, damage or obsolescence. 37 C.F.R. § 201.40(b)(1)(2). For other matters circumvention of access control measures exposes the user to infringement liability.

146 17 U.S.C. § 1202(a)(1).

147 *Id.* § 1202(b)(1).

148 *Id.* § 1202(c)(1)-(4), (6), (8).

149 *Id.* § 107.

150 *Id.* § 1201(c)(3).

151 *Id.* § 1201(i).

152 *See e.g.* ELEC. FRONTIER FOUND, *at* http://www.eff.org.

U.S.C. § 107) applies only to copyright infringement, not violations of the DMCA anticircumvention provisions.[153]

A Princeton professor claims he elected not to present his research into the secure digital music initiative (SDMI) copyright protection technology due to threats of a lawsuit. The professor filed a declaratory judgment action to establish his right to publicize his research.[154] Again, overbroad potential liability is viewed as detrimental to the growth of electronic commerce and related research.

c. Criminal Liability

Criminal penalties apply to the manufacture of devices to circumvent data management and database protection systems.[155] A criminal proceeding must be commenced within 5 years after the cause of action arose.[156]

The argument over the scope of the DMCA intensified when a Russian citizen, Dmitry Sklyarov, was arrested while attending a convention in Las Vegas.[157] Mr. Skyarov allegedly authored software that decrypts security measures on e-book Reader software provided by Adobe Systems. His employer ElcomSoft failed to respond to cease and desist letters from Adobe. He was arrested the day after he gave a speech on electronic book security at the Defcon Hackers Conference. Mr. Skyarov became the first person indicted under the DMCA in Northern California on August 28, 2001 along with his employer.[158] Interestingly, Adobe Systems withdrew support for the prosecution prior to the indictment because on the software was no longer availa-

---

153 Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 323 (S.D.N.Y. 2000), *aff'd*, 273 F.3d 429 (2nd Cir. 2001).

154 Felten v. Recording Industry Association of America, No. CV-01-2669 (GEB) (D. NJ June 6, 2001).

155 A violation, if willful and for purposes of commercial advantage or private financial gain, results in a fine of not more than $500,000 or imprisonment for not more than 5 years for a first offense. Those penalties are doubled for any subsequent offense. The criminal sanctions do not apply to a non-profit library, archive or educational institution. 17 U.S.C. § 1204 (2003).

156 *Id.*

157 Brenda Sandberg, *FBI Arrest of Russian Developer May Trigger Copyright Fight*, THE RECORDER (California), July 20, 2001. *See* U.S. v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

158 Press Release, U.S. Department of Justice, *First Indictment Under Digital Millennium Copyright Act Returned Against Russian National, Company, in San Jose, California* (Aug. 28, 2001), *available at* www.cybercrimes.gov/sklyarovindictment.htm. The first person was convicted under the DMCA in Nebraska in 2002. *See* Press Release, U.S. Department of Justice, First Digital Millennium Copyright Act (DMCA) Criminal Conviction in California and Second Known DMCA Conviction in the Country (Mar. 28, 2002) (*available at* http://www.cybercrime.gove/mynofplea.htm).

ble in the U.S.[159] Defenses based on free speech and fair use have been rejected by the District Court,[160] but the prosecution was unable to establish the requisite criminal intent in the trial of Elcom late last year.

In February 2003, federal prosecutors seized a website used to distribute mod chips designed to circumvent security features in the Microsoft XBox and Sony Playstation 2 game consoles. The prosecution asserted violation of the DMCA anticircumvention provisions. The site content was replaced with information about prosecution of online piracy under the terms of a plea agreement.[161]

Congressional leaders recently sent a letter to the Department of Justice urging criminal enforcement to deter peer-to-peer online theft of copyrighted works. The letter asserts prosecution is appropriate to protect the copyright based industries, which account for 5% of GDP.[162] Political pressure to deter copying of software, music and videos can be expected to continue. Continued prosecution based on legislation already enacted is inevitable.

4. Protection of Performers' Rights and Data Bases

There is now a statute criminalizing unauthorized fixation of live musical performances.[163] Other proposed legislation which would provide criminal penalties for use of proprietary databases has not yet been enacted in the United States.[164] Pressure will continue to expand protection of databases under U.S. law.

---

159 *Copyrights: Arrangement Delayed as Opposing Lawyers Negotiate in Russian Software Case* PTD, August, 27, 2001at d2.

160 U.S. v. Elcom, 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

161 *See*, 20 COMPUTER AND INTERNET LAWYER 30 (May 2003); www.iSONEWS.com (now linking to www.cybercrimes.gov). *Cf.* Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D.Ky. 2003)(civil liability analysis under DMCA); Chamberlain Group, Inc. v. Skylink Technologies, Inc., 2003 WL 22038638 (N.D.Ill. Aug 29, 2003)(same).

162 Letters from Joseph Biden, Denator, Chairman of Senate Judiciary Subcommittee on Crime and Drug, *et al.*, to John Ashcroft, Attorney General, Department of Justice (July 25, 2002) (*available at* http://www.politechbot.com/docs/congress.p2p.letter.081002.pdf).

163 18 U.S.C. § 2319A (1982). *See,* U.S. v. Moghadam, 175 F.3d 1269 (11th Cir. 1999), *reh'g. denied*, 193 F.3d 525 (11th Cir. 1999), *cert. denied*, 529 U.S. 1036 (2000).

164 A Directive on Legal Protection of Databases became effective for the European Union in 1998. Directive 96/9/EC of the European Parliament of the Council of 11 March 1996 (*available at* http://europe.eu.int/eurlex/en/lif/det/1996en_396L0009.html). The Council of Europe also adopted a convention on cybercrime (ETS No. 185) which would govern production of information from Internet service providers, the collection of Internet content and the extradition of cybercriminals. (*available at* http://conventions.coe.int/treaty/EN/cadreprincipal.htm).

5. *Prosecution Under State Law*

State copyright legislation is preempted by federal law.[165] Preemption, however, does not bar a state law conviction for destroying data through use of a "time bomb" installed in computer software.[166] Thus a Wisconsin statute criminalizing willful destruction of computer data was upheld.[167] Copyright law does not preempt criminal prosecution for destruction of noncopyrighted data owned by the victim. Commentators have argued that virtually every state has imposed a computer crimes law that may permit state court prosecution in matters potentially subject to federal copyright preemption.[168]

II.
DESIGNING AN EFFECTIVE COMPLIANCE PLAN TO PREVENT, DETECT AND MITIGATE INTELLECTUAL PROPERTY OFFENSES.[169]

A. Criminal Corporate Liability

The risk of a business inadvertently receiving and using stolen property is greatly enhanced by the nature of intellectual property. A company may not easily be able to detect that an employee is using information that he or she misappropriated from another company. In addition to the significant civil liabilities that have traditionally resulted from an infringement or misappropriation of another's intellectual property,[170] today a business may also be criminally prosecuted and sentenced.

Criminal liability is a serious threat to a company with a rogue employee. Under federal law, a corporation may be held criminally liable for the illegal acts of an employee, regardless of the employee's position within the corporation,[171] if the employee's actions: (i) were within the scope of his duties, and (ii) were intended, at least in part,

---

165 17 U.S.C. § 301. NBA v. Motorola Inc., 105 F.3d 841 (2d Cir. 1997); *See also* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989); State v. Perry, 697 N.E.2d 624 (Ohio 1998).

166 Corcoran v. Sullivan, 112 F.3d 836 (7th Cir. 1997).

167 *Id.*

168 *See* Note, Corcoran v. Sullivan, 13 BERKLEY TECH. L. J., 55 at 64 nn.71-73 (1998) (citing Xan Raskin & Jeannie Schaldach-Pavia, *11th Survey of White-Collar Crime: Computer Crimes* 33 AM. CRIM. L. REV. 541 (1996)).

169 For a discussion of Arizona corporate compliance planning, see James Burgess & Lee Stein, *Carrots, Sticks and Criminal Penalties,* ARIZONA ATTORNEY, Feb. 2001, at 30-35.

170 *See, e.g.*, Data General Corp. v. Grumman Sys. Support Corp., 825 F. Supp. 340 (D. Mass. 1993) ($24,417,000 jury award for misappropriation of trade secrets; judge increased this award by $9,000,000 for willfulness), *aff'd.* 36 F.3d 1147 (1st Cir. 1994).

171 New York Cent. & Hudson River R.R. v. United States, 212 U.S. 481, 491-95 (1909); United States v. Route 2, Box 472, 60 F.3d 1523, 1527 (11th Cir. 1995) (holding corporation liable for acts of one of its agents committed in scope of employment); United States v. Bank of New England, N.A., 821 F.2d 844, 856 (1st Cir. 1987) (same).

to benefit the corporation.[172] Under Arizona law, a corporation may be held criminally liable for conduct undertaken on its behalf if the offense was "engaged in, authorized. . .or recklessly tolerated by the directors of the enterprise in any manner or by a high managerial agent acting within the scope of employment."[173]

The illegal knowledge or intent necessary for many felony violations can be inferred from the collective conduct of the company's executives and employees.[174] The corporation does not need to profit from its employee's illegal conduct to be held liable.[175] Even though an employee was acting primarily to benefit himself, the corporation may be criminally liable if any part of his motivation was to benefit the corporation.[176]

Businesses that fail to take the steps necessary to prevent and detect intellectual property offenses are subjecting themselves to an unnecessary risk of criminal prosecution and penalties, as well as civil liability.

Effective programs to prevent or detect violations are specifically recognized as a mitigating factor under the Federal Sentencing Guidelines.[177] If the government prosecutes or the victim sues, the existence of an effective compliance plan may mitigate the assessment of criminal penalties[178] and undermine any punitive damage claims based on willful misconduct.[179]

---

172 United States v. Cincotta, 689 F.2d 238 (1982); United States v. One Parcel of Land, 965 F.2d 311, 316 (7th Cir. 1992) (agent's knowledge of illegal act may be imputed to corporation if agent was "acting as authorized and motivated at least in part by an intent to benefit the corporation.").

173 A.R.S. § 13-305(A)(2).

174 Bank of New England, 821 F.2d at 855 (imputing to corporation various employees' collective knowledge obtained within the scope of their employment).

175 United States v. American Medical Laboratories, 770 F.2d 399, 407 (4th Cir. 1985).

176 Automated Medical Laboratories, 770 F.2d at 407 (affirming corporation's conviction for actions of subsidiary's employee despite claim that employee was acting for his own benefit, namely his desire to ascend the corporate ladder; "Partucci was clearly acting in part to benefit AML since his advancement within the corporation depended on AML's well-being and its lack of difficulties with the FDA.").

177 18 USCS Appx. § 8A1.2 (2003). *See id.* § 2B5.3.

178 United States Sentencing Comm'n, 18 USCS Appx. § 8C2.5 (providing for significantly reduced criminal fines if corporate defendant had "an effective program to prevent and detect violations of law," i.e. a compliance plan); A.R.S. § 13-822 (providing for a 25% reduction in criminal fines if corporate defendant had an effective compliance plan).

179 Kolstad v. American Dental Ass'n, 527 U.S. 526 (1999) (employer may not be vicariously liable in punitive damages for discriminatory employment decisions of managers when those decisions are contrary to employer's good-faith efforts to comply with anti-discrimination laws).

B. Compliance Planning

1. Establish Compliance Standards Through a Code of Conduct

Generally, a company's Code of Conduct should inform employees that they must respect the copyrights, patents, licenses, trade secrets and confidential information of others, including the company's competitors, suppliers, and customers. The Code should provide enough information so that employees will be able to recognize potential problems. The Code should also direct employees as to where they can obtain further guidance if they are concerned about how to handle a particular issue or how to avoid a potential violation.

The Code of Conduct should educate employees about how to avoid violations that may occur because of the nature of the company's business. For instance, a company that uses software under licenses from other companies should: (1) inventory the licenses and review the restrictions they impose, and (2) use the Code of Conduct to educate employees about the company's restrictions under the licenses. The Code of Conduct may discuss the restrictions the software licenses impose. Alternatively, if the company does not want its Code of Conduct to go into that level of detail, the Code may simply state that all software must be licensed, that such licenses restrict the company's use of software, and that employees can take specific steps to obtain more information from specific sources about what they can and cannot do under the licenses.

The Code of Conduct should emphasize that employees have a duty to report any questionable conduct, that such reporting will be kept in confidence to the extent possible, and that employees will not suffer any detriment or retaliation for reporting a potential violation in good faith.[180]

2. Communicate the Compliance Standards Effectively

Producing a Code of Conduct is of little value unless employees understand what conduct is required of them. The company must train all employees in what the standards mean. With respect to intellectual property issues, the training should provide employees with a basic understanding of trade secrets, patents, copyrights and other forms of intellectual property. The training should raise employees' awareness of misappropriation of intellectual property, especially for

---

[180] Anne C. Flannery & Kristine Zaleskas, *The Case for Implementing a Corporate Compliance Program*, THE METROPOLITAN CORPORATE COUNSEL, Feb. 1998, at 4.

employees who formerly worked for competitors.[181] The training program should use examples to illustrate how the standards apply to specific workplace situations. The goal should be to train each employee to identify ethical and compliance problems and to seek appropriate assistance in resolving such issues.

3. *Establish Procedures to Achieve Compliance, Including Monitoring and Regular Audits*

An effective compliance plan requires that a company establish: (1) avenues by which employees can report potential compliance problems; (2) procedures for the company to investigate reports of potential violations, and if necessary, take remedial action; and (3) procedures by which the company will regularly monitor and test its compliance program to make sure it is working as it should.

A company should establish specific procedures designed to prevent employees from misappropriating confidential information from other companies or infringing on patents, trademarks, and copyrights.

a. Preventing Misappropriation of Confidential Information

A company faces a heightened risk of being accused of trade secret misappropriation when it hires employees who formerly worked for competitors or whose prior employers utilized written confidentiality agreements. In interviewing job applicants, a company should require the applicants to disclose whether they signed a non-disclosure, non-compete or confidentiality agreement with any of their former employers. If they did, the company should require them to provide the agreement so that the company can ascertain what restrictions apply. A company should not hire an employee who cannot perform the new position's duties without violating the rights of a former employer. All new hires should be required to sign a statement acknowledging that they understand that the company does not want them to disclose any confidential information they obtained from former employers.[182]

A company should monitor new hires closely, especially if they formerly worked in a position where they could have taken confidential information that would be of use in their new position. Also, a company should apprise appropriate employees of confidentiality provisions in the company's agreements with vendors or suppliers, and

---

[181] Stanley S. Arkin & Michael Colosi, *The Criminalization of Theft of Technology and Trade Secrets*, 5 BUSINESS CRIMES BULLETIN: COMPLIANCE AND LITIGATION, June 1996, at 4.

[182] Alan J. Sternstein et al., *Designing an Effective Intellectual Property Compliance Program*, § 3:132, in 8 CORPORATE COMPLIANCE SERIES (West 1998).

monitor employees' adherence to those confidentiality provisions. If a company accepts advice or ideas from external sources, it should establish idea submission procedures to protect itself from those who might submit an idea and later claim that the company stole it.[183]

When an employee terminates his or her employment, the company should conduct an exit interview. Ask the employee whether he or she is aware of any potential misappropriation of confidential information or other violations by the company. Document the employee's answers and investigate any reported potential violations.

b. Preventing Patent Infringement[184]

To avoid liability for patent infringement, a company should establish a review process for all new products and improvements to existing products, and new processes and equipment used to manufacture products.[185] The review should occur before the new development is made, used or sold. The review should determine whether the new development infringes on an existing patent. The review may include conducting a patent search and obtaining an opinion from patent counsel if any infringement issues need to be addressed.

c. Preventing Trademark Infringement

To avoid infringing on the trademark rights of others, a company should establish a review process for each mark the company contemplates using.[186] The review should include state and federal trademark searches to determine whether the mark is registerable and available for use. The company's trademark counsel should evaluate any marks listed in the search reports to determine whether the proposed mark might infringe them by being confusingly similar.

d. Preventing Copyright Infringement

A common source of copyright liability is use of unlicensed software. At least two industry groups (BSA and SIIA) actively pursue enforcement of copyright protection of member software providers. Both provide sample compliance policies and employee notices.[187]

Use of the Internet has accelerated copyright risks for software and

---

183 Sternstein, *supra* n. 177 § 3:132.

184 There are no statutes specifically criminalizing patent infringement. DRATLER, INTELLECTUAL PROPERTY LAW: COMMERCIAL, CREATIVE AND INDUSTRIAL PROPERTY § 13.04 (1999).

185 Sternstein, *supra* n. 177 § 3:122.

186 Sternstein, *supra* n. 177 § 1:13.

187 www.siia.net/privacy.html, www.bsa.org/usa/policy/privacy/.

website content. Employers should monitor employee Internet use and notify employees they are subject to monitoring.

4. If an offense is detected, take all reasonable steps to respond appropriately and prevent future offenses.

If a company discovers unlawful conduct, it must take all reasonable steps to remedy the violation. In addition to disciplining the employees involved, the company may need to make restitution to anyone injured by the unlawful conduct, report the conduct to law enforcement or other government agencies, and modify its compliance plan to prevent similar recurrences in the future.

The value of self-reporting and taking remedial measures is illustrated by a recent prosecution under the Economic Espionage Act.[188] David Kern joined Radiological Associates of Sacramento ("RAS") after he was fired from his job at Varian Medical Systems. RAS was a customer of Varian. According to court documents, Kern allegedly stole information after a Varian technician accidentally left a laptop computer at a hospital. Kern's co-workers reported the suspected theft to RAS's management, which in turn disclosed it to Varian. Varian sued Kern, but not RAS, and was awarded $3.5 million. Federal prosecutors also criminally charged Kern under the Economic Espionage Act. Kern is awaiting trial and faces a prison term of up to ten years.

RAS's disclosure paid off. It avoided the $3.5 million liability in the suit Varian brought for theft of the trade secret information. RAS also avoided criminal prosecution under the Economic Espionage Act.

III.
CONCLUSION

Businesses that depend on intellectual property to compete (virtually all businesses) risk corporate criminal liability if an employee misappropriates intellectual property belonging to others. Today's legal climate demands that businesses establish compliance programs to prevent their employees from infringing or misappropriating others' intellectual property, and to detect and remedy such offenses if they do occur. An effective compliance plan serves these functions and is a company's best investment to protect against criminal and civil liability.

---

188 *See* Torri Still, *A Lesson for the Valley: Thou Shalt Not Steal*, THE RECORDER, Oct. 7, 1999.