Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 22 | Issue 3 Article 4

2006

The Negligent Enablement of Trade Secret Misappropriation

Michael L. Rustad

THE NEGLIGENT ENABLEMENT OF TRADE SECRET MISAPPROPRIATION

Michael L. Rustad†

INTRODUCTION

During the March 30, 2005 oral argument in the *Grokster* file swapping case, the attorney representing the entertainment industry urged the U.S. Supreme Court to brace up its test for contributory copyright infringement in order to restrain widespread peer-to-peer (P2P) copyright infringement.[1] The attorneys for the media moguls urged the Court to replace the *Sony* standard with a more rigorous secondary liability test that would make software providers legally

---

† Michael L. Rustad Ph.D., J.D., LL.M. is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at Suffolk University Law School in Boston, Massachusetts. Thanks to Professor Tyler Ochoa for his invitation to present this paper at the Conference on Third Party Liability in Intellectual Property Law held October 7, 2005 at the Santa Clara Law School. I appreciate the critical comments of Allen Hammond, Santa Clara University School of Law, Robert Bone, Boston University School of Law and Joseph Bauer, Notre Dame Law School. My thanks to Susan W. Brenner, the NCR Distinguished Professor of Law & Technology, University of Dayton School of Law who provided valuable suggestions and materials for this paper. I would like to thank John Hebb, a working law enforcement officer, Suffolk University Law School student, and research assistant. Shannon Downey, As'ad Hamad, Conway Kennedy, Anna-Karin Kuliga, and Danielle Bouvier also provided expert research and editorial suggestions. Michael Scott Fischer provided me useful examples of how software vulnerabilities are exploited in economic espionage cases. I also appreciate the assistance given to me by Diane D'Angelo, a reference librarian at Suffolk University Law School and the advice given to me by Andrew Beckerman-Rodau and Jerry Cohen. Chryss J. Knowles provided useful editorial suggestions and commentary.

1. In Metro-Goldwyn-Meyer Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005), the attorney for the recording industry contended that Grokster and the other file swapping services were "built on networks of infringing users and intentionally and directly promote illegal file swapping." *Supreme Court Hears Grokster Case; Pundits Predict Narrow Decision*, COMM. DAILY, Mar. 30, 2005, *available at* 2005 WLNR 4914200 (summarizing oral argument before the U.S. Supreme Court in *MGM v. Grokster*). Twenty-eight of the world's leading media and entertainment industry stakeholders filed suit against the owners of Morpheus, Grokster, and KaZaA software products used by Internet users around the globe for swapping copyrighted materials. *See generally* Benny Evangelista, *Music File-Sharing Case Before High Court Ruling Could Have Major Effect on Future of Entertainment Industry, Consumer Rights*, S.F. CHRONICLE, Mar. 28, 2005 at A1.

responsible for enabling P2P copyright infringement.[2] During the *Grokster* oral argument, Justice Stephen Breyer expressed skepticism about the long-term effects of expanding secondary copyright liability beyond the contours of the *Sony* case. Justice Breyer speculated that the Xerox copying machine and the Apple iPod would never have been brought to the marketplace if the inventors were subject to secondary liability because their invention enabled copyright infringement.[3]

In the Ninth Circuit opinion, the appellate court applied the *Sony* standard to the Streamcast and Grokster software, holding that the providers of these peer-to-peer (P2P) products could not be secondarily liable for copyright infringement since the software was capable of significant lawful use. The court held that neither P2P software developer "could be held liable, since there was no showing that their software, being without any central server, afforded them knowledge of specific unlawful uses."[4] In its groundbreaking *Grokster* opinion, the U.S. Supreme Court reversed the Ninth Circuit, holding that the P2P providers could be secondarily liable for copyright infringement by importing the novel theory of intentional inducement from patent law.

The *Grokster* Court unanimously held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement is liable for the resulting acts of infringement by third parties."[5] The Court decided the case on an "intentional inducement" theory, declining to rule on the continuing vitality of the *Sony* test for contributory infringement.[6] The signpost of *Grokster* is the greater willingness of the Court to approve imposing secondary liability on third parties that facilitate intellectual property crimes and infringement. The U.S. Supreme Court's decision in *MGM v. Grokster* also raises the possibility that in a future case courts may be more receptive to arguments based upon negligent enablement,[7]

2. *Grokster*, 125 S. Ct. at 2775. *See also* Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417 (1984) (holding that Sony, the manufacturer of the Betamax video cassette recorder was not liable for infringing uses of the VCR so long as the product was capable of substantial non-infringing uses).

3. *Grokster*, 125 S. Ct. at 2792.

4. *Id.* at 2778.

5. *Id.* at 2780.

6. *Id.*

7. *Id.* at 2765.

intentional inducement's "running mate," in order to impose secondary liability on software producers that pave the way for trade secret misappropriation.[8]

Over the past quarter century, "the American economy exploded with new technology and a proliferation of software and Internet companies."[9] Total revenue of the top 500 software companies for 2004 was an estimated $330.7 billion, a 14% increase from 2003.[10] Software is too often introduced into the marketplace with well-known software design defects that enable intruders to immediately gain privileged access to computer systems, enabling the theft of trade secrets or the leak of confidential business or personal data.[11] Substandard software costs businesses and consumers tens of billions of dollars because of defective design features or other vulnerabilities that enable cybercriminals.[12] This Article presents the case for expanding third-party liability for the misappropriation of trade secrets to safeguard American international competitiveness.

Three points are made in this article. The first point is that the manifest function of The Economic Espionage Act (EEA) was to punish and deter state-sponsored espionage.[13] While Congress also intended to punish and deter the misappropriation of trade secrets by

---

8. I borrow this phrase from Alfred Yen who was a commentator at Santa Clara University School of Law's Conference on Third-Party Liability in Intellectual Property Law.

9. Tanya Patterson, Heightened Securities Liability for Lawyers Who Invest in Their Clients: Worth the Risk?, 80 TEX. L. REV. 639, 639 (2002).

10. John P. Desmond, *2004 Software 500: Growth Came in Segments*, http://www.softwaremag.com/L.cfm?Doc=2004-09/2004-09software-500 (last visited Apr. 6, 2006).

11. *See, e.g.*, U.S.-CERT, UNITED STATES COMPUTER EMERGENCY READINESS TEAM, NATIONAL CYBER ALERT SYSTEM, CYBER SECURITY BULLETIN, SB05-264, SUMMARY OF SECURITY ITEMS FROM SEPTEMBER 14 THROUGH SEPTEMBER 20, 2005, http://www.us-cert.gov/cas/bulletins/SB05-264.html.

12. Quentin Hardy, *Saving Software From Itself*, FORBES, Mar. 14, 2005, at 60.

13. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839 (2000)) (hereinafter "EEA"). The legislative history for the EEA reveals two reasons for the federal criminalization of trade secret theft:

> (1) Foreign powers, through a variety of means, are actively involved in stealing critical technologies, data and information from U.S. companies or the U.S. Government for the economic benefit of their own industrial sectors. (2) Laws then on the books—including the Interstate Transportation of Stolen Property Act and the Mail Fraud and Fraud by Wire statutes—were of virtually no use in prosecuting acts of economic espionage.

Gerald J. Mossinghoff, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, *available at* http://www.oblon.com/Pub/mason-120.html (last visited Apr. 2, 2005).

domestic defendants, the thrust of the federal statute was directed to espionage by foreign agents, instrumentalities, and governments.

My second point is that the EEA has played almost no role in punishing and deterring the primary wrongdoers that misappropriate trade secrets from foreign governments, agents, or other entities. All but a few EEA prosecutions have been filed against domestic spies with the federal statute playing no role in punishing and deterring foreign agents and governments. Many of the domestic espionage suits were cases in which the investigation was completed by the victim corporations rather than the Justice Department or other federal law enforcement officials.

An empirical study of all EEA prosecutions from the federal criminal statute's enactment in 1996 to August 1, 2005 uncovered fewer than fifty economic or espionage prosecutions filed in federal courts; nearly every prosecution was for domestic rather than foreign economic espionage.[14]

The data on EEA defendant characteristics, targeted companies, the nature of trade secrets stolen, the method of misappropriation, and trends in cases prosecuted, reveals that the federal criminal statute is not punishing and deterring state-sponsored espionage. EEA prosecutors focus on domestic trade secret theft rather than foreign government involvement in industrial and economic espionage. Cybercriminals and other trade secret misappropriators are unlikely to be deterred with such a dismal record of detection and punishment of economic espionage by federal law enforcement officials.

My third point is that the EEA should be amended to give the corporate victims of espionage standing to file a statutory tort action against the primary wrongdoers as well as the software provider whose defective software frequently paves the way for economic or industrial espionage. Judge Jerome Frank used the term "private attorney general" to refer to "empowering any person, official or not, to institute a proceeding involving such a controversy, even if the sole purpose is to vindicate the public interest. Such persons, so

14. The principal sources for the sample of EEA prosecutions include: (1) DEPARTMENT OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION (CCIPS), CURRENT TABLE OF PROSECUTIONS FOR THE ECONOMIC ESPIONAGE ACT, http://www.usdoj.gov/criminal/cybercrime/eeapub.htm (last visited Apr. 5, 2006); (2) R. Mark Halligan, *Reported Criminal Arrests and Convictions Under the Economic Espionage Act of 1996*, http://my.execpc.com/~mhallign/indict.html (last visited Aug. 10, 2005); (3) CURNWS database of LEXIS/NEXIS and News file of WESTLAW; (4) ALLCASES file of LEXIS/NEXIS and (4) Internet-related searches on the EEA.

authorized, are, so to speak, private Attorneys General."[15] Another court expanded this concept to include the remedy of punitive damages where "[t]he plaintiff acts as a private attorney general to punish the culpable wrongdoer, thereby encouraging adherence to safety standards that benefit [society] generally . . . . [I]t is not the plaintiff's individual right, but society's as a whole, that is being defended."[16] The private attorney general is a litigant who files a private cause of action for a public purpose.[17] When plaintiffs' attorneys serve the public interest they are called "private attorneys general."[18]

Private enforcement is already well established in other branches of intellectual property law.[19] Trade secret protection is the only branch of intellectual property where there is not a private cause of action based upon federal statute.[20] The Software Publishers Association, for example, funds a private police force that actively detects and prosecutes copyright infringement and software piracy.[21] Software copyright cops routinely participate in raids on companies to confiscate unlicensed copies of software. The industry victims of corporate espionage are far more likely to have the resources and the resolve to prosecute wrongdoers than federal law enforcement personnel, who are already spread too thin in the wake of 9/11.

To maximize the private attorney general's role as an independent monitoring force in espionage cases, the EEA must be

---

15. Assoc. Indus. of N.Y. State, Inc. v. Ickes, 134 F.2d 694, 704 (2d Cir. 1943).

16. Thiry v. Armstrong World Indus., 661 P.2d 515, 518 (Okla. 1983); *see also* Kink v. Combs, 135 N.W.2d 789, 798 (Wis. 1965) (describing how punitive damages serve the public because the private individual acts as a prosecutor to punish harmful conduct).

17. *Thiry*, 661 P.2d at 518.

18. By private attorney general, I am referring to both the litigant and plaintiff, and plaintiff's attorney public interest role. Private attorneys general are critically needed to protect our nation's competitiveness.

19. Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 101 (2001).

20.

> Trade secrets law is one of the last areas of intellectual property that is not covered by a federal statute granting a private right of action to trade secret owners. Currently, federal statutes exist that provide private rights of action to protect patents (35 U.S.C. § 281), copyrights (17 U.S.C. §§ 101-22), and trademarks (15 U.S.C. §§ 1051-1129).

Andrew Beckerman-Rodau, *Trade Secrets – The New Risks to Trade Secrets Posed by Computerization*, 28 RUTGERS COMPUTER & TECH. L.J. 227, 233 n.34 (2002) (describing the greater difficulty of protecting trade secrets in the networked world of computers).

21. *Id.*

reconfigured to maximize private enforcement. The Economic Espionage Act is one of the few modern regulatory statutes that do not have a significant role for the private attorney general.[22] The revised EEA must make certain that the corporate spy is punished in addition to being forced to disgorge all profits made from illicitly obtained trade secrets. The EEA should be amended to permit causes of action against third parties that enable or facilitate misappropriation, such as vendors of software with known vulnerabilities that did not take prompt remedial measures to reduce the radius of the risk.[23]

A reformed EEA would not only give the victims of trade secret misappropriation a private cause of action against primary wrongdoers but also a private cause of action against software vendors that enable or pave the way for trade secret misappropriation because of defective software design. The expansion of secondary liability for defective software enabling trade secret theft can teach even the most powerful software vendor that software must be designed for its foreseeable environment of use.

---

22. A large number of federal statutes have bifurcated roles for the public regulators or law enforcement and private attorneys general: The Agricultural Adjustment Act of 1938, Bank Holding Company Act, Consumer Credit Protection Act, Fair Housing Act, Federal National Mortgage Association Charter Act, Federal Property and Administrative Services Act of 1949, Organized Crime Control Act of 1970 (RICO), Patent Act, Prevention of Unfair Methods of Competition in Import Trade, Regional Rail Reorganization Act of 1973, Trademark Act of 1946, Petroleum Marketing Practices Act, and the Commodity Futures Trading Commission Act of 1973. Thomas Koenig & Michael Rustad, *Crimtorts as Corporate Just Deserts*, 31 U. MICH. J.L. REFORM 289, 326 (1998). Wealth-based civil punishment is also found in the Racketeer Influenced and Corrupt Organization Act (RICO), the Resource Conservation and Recovery Act (RCRA), anti-insider trader statutes, and the False Claims Act. Section 1983 constitutional tort actions, civil forfeiture litigation, securities enforcement, antitrust enforcement, sexual harassment remedies, and whistleblower qui tam actions are just a few examples of federal statutes employing public and private enforcement. *Id.* at 305.

23. Third party liability for trade secret misappropriation is generally restricted:

> [T]o parties in privity with the trade secret owner who owe the owner a duty of confidence. . . . The general rule regarding third party liability for trade secret misappropriation is straightforward. One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if . . . he learned the secret from a third person with notice of the facts that it was a secret from a third person with improper means or that the third person's disclosure of it was otherwise a breach of duty to the other.

Steven D. Glazer, *Special Issues Relating to Third Party Liability for Trade Secret Misappropriation*, *in* PRACTICING LAW INSTITUTE, PATENTS, COPYRIGHTS, TRADEMARKS AND LITERARY PROPERTY COURSE HANDBOOK SERIES, PLI Order No. G0-011Q (Sept. 2002), *available at* 719 PLI/Pat 39 (Westlaw).

At present, the injured targets of trade secret theft have no federal civil remedy for the foreseeable consequential damages of economic espionage. Under the tort of negligent enablement, a third-party software vendor or other data intermediaries would only be civilly liable in federal court if they knew or should have known of vulnerabilities in software or network design facilitating espionage.[24] In the first decade of EEA prosecutions, no outside hacker was prosecuted for misappropriating trade secrets by exploiting known software defects. The new statutory tort of negligent enablement of trade secret theft is designed to supplement lax public enforcement of state-sponsored economic espionage.[25] Few cases of foreign espionage have been successfully prosecuted on the criminal side of the law because of several interrelated factors, including the problem of anonymity, jurisdictional issues, and the lack of resources in the law enforcement community. Economic espionage is frequently multi-national, requiring the development of new legal sanctions including private enforcement.

Finally, the enactment of an international convention or extradition treaty will also be needed to reach foreign spies living on another continent or operating in an offshore haven. The long-term impact of federal statutory private remedies for economic and industrial espionage will improve global competitiveness for American industry.

I. THE ECONOMIC ESPIONAGE ACT: THE LAW-IN-THE-BOOKS

A. Economic Espionage and the American Experience

This part of the Article confirms that the Economic Espionage Act has been a gross failure in punishing and deterring the widespread practice of economic espionage by foreign states. Today's

24. Negligent enablement claims will not excuse a company that has not taken reasonable efforts to protect the secrecy of an alleged trade secret. *See* Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823, 849 (10th Cir. 1993) (applying Colorado law). A company's failure to protect its trade secrets through nondisclosure agreements, restricted covenants in licenses and other reasonable measures will preclude any misappropriation action.

25. "The EEA prosecutorial record also reveals that the Government has not brought prosecutions when trade secrets have been disclosed unintentionally, i.e. through mere negligence or inadvertence." Mark D. Seltzer & Angela A. Burns, *Criminal Consequences of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete?*, 1999 B.C. INTELL. PROP. & TECH. F. 52501, http://www.bc.edu/bc_org/avp/law/st_org/iptf/articles/content/1999052501.html.

Hobbesian-like economic competition was prefigured by our Founding Fathers' unofficial policy of condoning the wholesale theft of technology from England and other European states according to a provocative new historical study by Doron S. Ben-Atar.[26] When Georgia planters stole a prototype for Eli Whitney's cotton gin and began to disseminate that invention throughout the South, their defense to patent infringement claims was that the cotton gin was not patentable and had in fact been in use in England and Ireland for decades.[27]

During the Revolutionary War, America's Founding Fathers routinely employed spies to learn about the techniques and processes of English industry.[28] Thomas Jefferson, John Adams, and other U.S. diplomats in Europe recruited artisans and "were also not averse to promoting industrial espionage."[29] Jefferson, for example, sought to acquire wool carding and spinning machinery built by English artisans in France.[30] Both Madison and Jefferson incorporated the "acquisition of European technology into their larger vision of American diplomacy."[31] In Jefferson's first State of the Union address, he noted how he intended to jump start the U.S. economy by the introduction of "new and useful inventions from abroad."[32]

Fast forward to the twenty-first century. The world is still divided into intellectual property "haves" and "have-nots," but the intellectual property shoe is now on the other foot. Many developing countries, including America's allies, use legal or illegal means to acquire critical technologies from the United States.[33] U. S. firms own the crown jewels of the information society whereas less developed competitors, such as China, Taiwan, and Korea have inexpensive raw materials and a low-wage labor force.[34]

---

26. DORON S. BEN-ATAR, TRADE SECRETS: INTELLECTUAL PIRACY AND THE ORIGINS OF AMERICAN INDUSTRIAL POWER (Yale University Press) (2005).

27. *Id.* at xiv.

28. *Id.* at 34.

29. *Id.* at 123.

30. *Id.* at 124.

31. *Id.* at 159.

32. *Id.* at 157.

33. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (1998), *available at* http://www.fas.org/irp/ops/ci/docs/fy98.htm (last visited Apr. 5, 2005).

34.

> The smartest companies are looking far field for innovation as well. . . . Other companies on FORTUNE's Global 500 list, such as Boeing and Microsoft and Pfizer, are collaborating with engineers and scientists in India and China and

Empirical evidence on the extent of economic espionage is unknown and perhaps, unknowable. China, like the United States in the eighteenth century, has a concerted policy of jump-starting its economy through misappropriating the trade secrets of the software, pharmaceutical, and financial services industries, as well as other industries employing advanced information technologies.[35] The assistant director of the FBI's counterintelligence division rates China as the "biggest [espionage] threat to the [United States] today."[36] The FBI estimates that 3,000 Chinese "front companies" have been set up for the sole purpose of acquiring U.S. military or industry technologies.[37]

Chinese nationals studying in U.S. universities or working for U.S. defense contractors "are contacted by Chinese government officials or one of more than 3,000 Chinese front companies . . . to specifically acquire military or industrial technologies illegally."[38] Today's greatest threat may be from Far Eastern countries, but tomorrow's trade secret thieves may be engaged in state-sponsored

---

> Russia. Why reach out to incubate ideas? Says Forrester Research CEO George Colony: "There's simply not enough qualified talent at home for global companies to keep pace."

Patricia Sellers, *Where do good ideas come from? For Global 500 companies, the answer could be anyplace.*, FORTUNE, July 25, 2005, at 127.

35. Editorial, *Chinese Cook Books*, INVESTOR'S BUSINESS DAILY, June 20, 2005, at A18 (contending that 90% of China's technology is stolen from more developed countries).

36. Jay Solomon, *Phantom Menace: FBI Sees Big Threat from Chinese Spies: Businesses Wonder*, WALL ST. J., Aug. 10, 2005, at A1.

37. *Wall Street Journal: FBI Sees Big Threat From Chinese Spies; Businesses Wonder*, CENTRAL NEWS AGENCY, Taiwan (Aug. 10, 2005). Chinese espionage generally uses employees or ex-employees to transmit trade secrets to Chinese government-related companies.

> The FBI recently arrested two ex-employees of Metaldyne Corporation of Plymouth, Michigan, on charges that they stole Metaldyne's trade secrets to enable a Chinese business to produce exact replicas of products at a reduced price. . . . One defendant, Fuping Liu, worked at Metaldyne as an engineer until quitting in April 2004 to work for a competitor, while his co-defendant, Anne Lockwood, was a former vice president of sales at Metaldyne.

The FBI documented that the defendants made multiple trips to meet with potential Chinese business partners transmitting numerous purloined documents about the target company's proprietary production methods. *Combating Organized Piracy, Hearing Before the Subcomm. On Oversight of Government Management, The Federal Workforce, and the District of Columbia of the S. Committee on U.S. Homeland Security and Governmental Affairs*, June 14, 2005, (statement of Laura H. Parsky, Deputy Assistant Attorney General) 2005 WL 1396295 (Westlaw).

38. *Wall Street Journal: FBI Sees Big Threat From Chinese Spies; Businesses Wonder*, CENTRAL NEWS AGENCY, Taiwan (Aug. 10, 2005).

espionage originating in India, Pakistan, Ukraine, Kazakhstan, Rumania or other less developed countries.[39]

Modern China and other developing countries have a great incentive to use illicit means to transfer advanced technologies from the United States to jump-start their economies. Just as England lost its competitive edge because of state-sanctioned espionage, U.S. global hegemony is endangered by economic espionage in the twenty-first century. The United States will be unable to maintain its international competitiveness unless it finds some means to protect its trade secret information.[40]

Economic espionage may be broadly defined as "the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies."[41] "Economic crimes have a serious impact on a wide variety of U.S. industries and businesses and therefore upon the economic well-being of the [United States]."[42] At present, the victims of trade secret theft have no federal cause of action and must file parallel civil suits in state or federal courts in diversity actions. Parallel civil suits in different courts not only impede successful prosecutions by the Department of Justice but subject material governmental and non-governmental witnesses to "searching and protracted depositions and interrogatories even before the Government can present testimony to a jury."[43] The next part of the article proposes that Congress amend the EEA to provide the victims of economic espionage with new tort remedies against primary wrongdoers and software licensors whose defective products and services enable trade secret theft.

B. Economic Espionage Act of 1996 (EEA)

1. Purpose of the EEA

The EEA, signed into law by President Clinton on October 11, 1996, was enacted to punish and deter foreign and domestic spies

39. Rob Lever, *Security Experts Warn of Chinese Cyberattacks for Industrial Secrets*, AFX-ASIA, July 24, 2005, at 1.

40. Kent B. Alexander & Kristen L. Wood, *The Economic Espionage Act: Setting the Stage for a New Commercial Code of Conduct*, 15 GA. ST. U. L. REV. 907, 909 (1999).

41. Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2001), http://www.ncix.gov/publications/reports_speeches/reports/fecie_all/FECIE_2001.pdf.

42. *Id.*

43. Seltzer & Burns, *supra* note 25.

threatening America's economic well-being.[44] The annual losses due to economic espionage are estimated to be between $130 billion and $330 billion.[45] "The National Counterintelligence Center and the U.S. State Department found that seventy-four U.S. corporations reported more than 400 incidents or suspected incidents of *economic espionage* by foreign companies."[46] Until 1996, there was no federal criminal statute punishing industrial spying by foreign governments and agents.[47] The prosecution of trade secret theft as a criminal offense is a fairly recent development.[48] Prior to the EEA, prosecutors pursued the theft of trade secrets by using existing law such as the 1934 National Stolen Property Act, which was intended to punish thieves who also fled across state borders in automobiles.[49]

---

44. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839 (2000)). The EEA was enacted to fill a gap in the law. "Other federal statutes, such as the National Stolen Property Act, 18 U.S.C. § 2314, and the Mail and Wire Fraud statutes, 18 U.S.C. § 1341 and 18 U.S.C. § 1343, were also of limited use in combating the problem of economic espionage." J. Michael Chamblee, *Validity, Construction, and Application of Title I of Economic Espionage Act of 1996*, 177 A.L.R. FED. 609, 617-18 (2005).

45. Richard Krantz, *Industrial Espionage Becomes Favorite Way to Achieve Quick Gains*, Voice of America Broadcast, Voice Am. Press Releases & Documents, Apr. 29, 2005, http://www.voanews.com/english/archive/2005-04/2005-04-29-voa1.cfm (quoting an industrial espionage expert).

46. Information Security, http://www.idsemergencymanagement.com/emergency_management/us/Risk_Decisions/Security_Risk_Protection_Espionage/29_0/g_supplier_4.html (last visited Apr. 5, 2006).

47. "Until 1996 there was no federal statute that explicitly criminalized the theft of commercial trade secrets." United States Department of Justice Intellectual Property Manual, http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm (last visited Apr. 6, 2006) (discussing enforcement of the Economic Espionage Act). *See also* Joseph N. Hosteny, *The Economic Espionage Act: A Very Mixed Blessing*, http://www.hosteny.com/articles/espionage.html (last visited Apr. 5, 2006).

48. "However, the misappropriating party has not normally been exposed to criminal liability for wrongfully taking a trade secret. In the 1960's a number of states enacted statutes making it a crime to wrongfully misappropriate a trade secret." Donald M. Zupanec, *Criminal Liability for Misappropriation of Trade Secrets*, 84 A.L.R.3d 967, 971-72 (2005).

49. R. Mark Halligan noted that prior to the EEA federal prosecutors "relied primarily upon the National Stolen Property Act and the wire and mail fraud statutes to commence criminal prosecutions for trade secret theft." The National Stolen Property Act was enacted by Congress in 1934 to prevent criminals from evading state prosecutions by fleeing in automobiles across state lines with stolen property. Prosecutions under 18 U.S.C. § 2314 require the government to prove that "goods, wares or merchandise" were transported in "interstate or foreign commerce" and that the defendant knew that they were "stolen, converted or taken by fraud." "Trade secret prosecutions under this Act have been difficult because some courts have held that the theft of 'purely intellectual property' does not constitute the theft of 'goods, wares or merchandise' as required by 18 U.S.C. § 2314.31." R. Mark Halligan, *The Economic Espionage Act of 1996: The Theft of Trade Secrets is Now a Federal Crime*, http://my.execpc.com/~mhallign/crime.html (last visited Apr. 5, 2006).

The National Stolen Property Act applied to tangible goods but was not clearly applicable to the unauthorized transfer of intangibles such as intellectual property.[50] Another statute, the Federal Mail Fraud Act, required proof that economic espionage used the U.S. Postal Service.[51] Similarly, the Wire Fraud statute "requires intent to defraud as well as the use of wire, radio or television."[52] "The only federal statute explicitly targeting the theft of trade secrets was limited to government employees' unauthorized disclosure of trade secrets, and offenders were subject only to misdemeanor penalties."[53] The EEA was enacted to bridge a gap in trade secret law by creating two new federal crimes for trade secret misappropriation:

> Section 1831 covers misappropriation by foreign governments or their agents, which is punishable by fines up to $500,000 or imprisonment of up to fifteen years. Offending organizations may be subject to fines of up to $10,000,000. Section 1832 covers misappropriation that is intended to benefit individuals and corporations. Under Section 1832, individuals are subject to fines and up to ten years of imprisonment, while organizations are subject to fines of up to $5,000,000.[54]

In hearings that led to the passage of the 1996 Economic Espionage Act, FBI Director Louis J. Freeh testified, "[e]conomic espionage is the greatest threat to our national security since the Cold War."[55] He observed that "[t]he end of the Cold War sent government spies scurrying to the private sector to perform illicit work for businesses and corporations and by 1996 studies revealed that nearly $24 billion of corporate intellectual property was being stolen each year."[56] The 2002 Annual Report to Congress on Foreign

---

50. *See, e.g.*, Dowling v. United States, 473 U.S. 207, 216 (1985).

51. Gerald J. Mossinghoff, J. Derek Mason & David A. Oblon, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, http://www.oblon.com/Pub/mason-120.html (last visited Apr. 5, 2006).

52. *Id.*

53. George "Toby" Dilworth, *The Economic Espionage Act of 1996: An Overview*, http://www.usdoj.gov/criminal/cybercrime/usamay2001_6.htm (last visited Apr. 5, 2006).

54. KINNEY & LANGE P.A., INTELL. PROP. L. BUS. LAW § 12.11 (2005).

55. Alan Gathright & Vanessa Hua, *Tech Theft Rises Amid China Ties*, S.F. CHRON., Feb. 10, 2003, at A1.

56. United States. v. Hsu, 155 F.3d 189, 194 (3rd Cir. 1998). Freeh also testified that:

> [The FBI's] investigations of economic espionage cases had doubled in the previous year from 400 to 800, and that 23 countries had been involved. According to Freeh, foreign governments are actively targeting U.S. industry and the U.S. government to steal critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage.

Economic Collection and Industrial Espionage estimated that "economic espionage and loss of critical information cost American companies more than $300 billion a year."[57] An FBI report concluded that "losses related to high-tech crimes in the United States are $10 billion to $15 billion per year."[58] One observer describes business espionage as the new battleground for global hegemony:

> Since the end of the Cold War, the focus of intelligence and counterintelligence efforts has shifted from military and political targets to technological and economic ones. Nations have been reshaping their intelligence agencies and investigative resources to be more responsive to the competitive and global needs of businesses. The Cold War has been replaced by the Economic War. The increase in trade secret theft has placed the technologies of U.S. companies, ranging from simple textile formulas to complex defense technology, at great risk.[59]

The EEA provides criminal sanctions and civil damages for the misappropriation of trade secrets. The Congressional purpose of the EEA was to enhance trade secret protection:

> For many years federal law has protected intellectual property through the patent and copyright laws. With this legislation, Congress will extend vital federal protection to another form of proprietary economic information – trade secrets. There can be no question that the development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interest.[60]

Congress passed this statute against "a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage."[61]

Sorojini J. Biswas, *The Economic Espionage Act of 1996*, http://www.myersbigel.com/ts_articles/trade_secret4.htm (last visited Apr. 5, 2006) (quoting FBI Director Louis Freeh's testimony).

57. Richard B. Isaacs, *How Not to Tell All: Find out How to Preserve the Company's Competitive Edge by Preventing Proprietary Information from Being Given Away*; 5 SECURITY MGMT. 102 (May 1, 2004).

58. Tony Aeilts, *Defending Against Cybercrime and Terrorism: a New Role for Universities*, 74 THE FBI L. ENFORCEMENT BULL. 14, 15 (Jan. 1, 2005).

59. Thierry Oliver Desmet, The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?, 22 HOUSTON J. INT'L L. 93, 96-97 (1999).

60. H.R. REP. NO. 104-788, at 4 (1996).

61. United States v. Hsu, 155 F.3d at 194.

2. EEA Definition of Trade Secrets

The EEA draws heavily upon the common law but is broader than the misappropriation tort.[62] The federal criminal statute is based primarily upon property concepts as opposed to wrongful conduct.[63] Any tangible property and intangible information is potentially classifiable as a trade secret so long as the owner "has taken reasonable measures to keep such information secret,"[64] and the information "derives independent economic value . . . from not being generally known to . . . the public."[65] The theft of trade secrets is criminalized if the defendant: (1) stole, or without authorization of the owner, obtained, destroyed or conveyed information; (2) knew or believed that this information was a trade secret; and (3) the information was in fact a trade secret.[66]

3. Reasonable Measures to Protect Trade Secrets

No EEA prosecution may be initiated unless "the owner thereof has taken reasonable measures to keep such information secret."[67] If a company fails to implement reasonable computer security, the consequence is that proprietary information is not treated as a trade secret.[68] The U.S. Attorney General has the discretion to institute civil enforcement actions and obtain injunctive relief for violations.[69] The EEA provides for protective orders to protect trade secrets during litigation.[70] In addition, the court has broad powers to protect the

62. Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 860 (2002).

63. *Id.*

64. 18 U.S.C. § 1839(1)(3)(A) (2000). *See also* Rockwell Graphic Sys., Inc. v. Dev Indus., Inc., 925 F.2d 174, 179-80 (7th Cir. 1991) (discussing reasonable measures to protect trade secrets under Illinois' Uniform Trade Secrets Act).

65. 18 U.S.C. § 1839 (2000) (defining the term "trade secret" to include "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, or codes, whether tangible or intangible, and whether or how stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing," as long as the "reasonable measures" and "independent economic value" tests are met).

66. 18 U.S.C. § 1832 (2000).

67. 18 U.S.C. § 1839(3)(a) (2000).

68. Weigh Sys. South, Inc. v. Mark's Scales & Equip., Inc., 68 S.W.3d 299 (Ark. 2002) (holding that inadequate computer security resulted in the loss of trade secret protection).

69. 18 U.S.C. § 1836 (2000).

70. U.S. DEPARTMENT OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION (CCIPS), INTELLECTUAL PROPERTY CRIMES VIII.B9,

confidentiality of trade secrets during litigation.[71] A trade secret does not lose its protection under the EEA "if it is temporarily, accidentally, or illicitly released to the public, provided it does not become generally known or readily ascertainable through proper means."[72] The modern standard is that the trade secret owner implements reasonable standards.

Reasonable efforts to protect the secrecy of alleged trade secrets include compliance with mandatory export control laws imposed on the export of data and goods that implement or reveal technology.[73] The EEA requires that courts take such actions as necessary to preserve the confidentiality of the trade secret.[74] The EEA also contains a provision designed to preserve the confidentiality of trade secrets during criminal prosecutions. Title 18 U.S.C. section 1835 states that a court:

> shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.[75]

4. Value

EEA prosecutions also require proof that a trade secret has value. If reasonable measures are not taken by the trade secret owner, value can be destroyed. The EEA requires that the information must derive "independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through

---

http://www.usdoj.gov/criminal/cybercrime/ipmanual/08ipma.htm. (last visited Apr. 5, 2006) (discussing procedures for seeking protective order protecting trade secrets).

71. 18 U.S.C. § 1835 (2000).

72. United States v. Genovese, No. 05 CR.04 (WHP), 2005 U.S. Dist. LEXIS 11947, at *9-10 (S.D.N.Y. June 21, 2005).

73. I am grateful to Jerry Cohen for pointing out that voluntary reasonable efforts are complemented by a large number of federal statutes to protect trade secrets in government contracts or grants. In addition, a company's reasonable methods includes private license agreements from third parties included in the goods and services of value added resellers or licensees.

74. 18 U.S.C. § 1835 (2000).

75. *Id.*

proper means by, the public."[76] The statute does not specify any *de minimis* value in trade secrets that triggers EEA prosecutions.[77]

5. Two Types of EEA Trade Secret Theft

The EEA criminalizes two types of offenses: (1) economic espionage that benefits foreign governments or entities (Section 1831) and (2) the theft of trade secrets that benefit any person but the true owner (Section 1832).[78] Section 1831 criminalizes the theft of trade secrets when the defendant, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly:

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of . . . (1) through (3); or (5) conspires with one or more persons to commit any offense described in any of . . . (1) through (3), and one or more of such persons [does] any act to effect the object of the conspiracy.[79]

---

76. 18 U.S.C. § 1839(3)(b) (2000).

77. One of the conceptual difficulties in trade secret law is the degree to which value and reasonable measures form a circular system.

78. Section 1832 was enacted as part of the Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488.

> In relevant part, the statute applies to anyone who, 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 . . . without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information.

United States v. Genovese, No. 05 CR.04 (WHP), 2005 U.S. Dist. LEXIS 11947, at *4 (S.D.N.Y. June 21, 2005). "The first offense, 'economic espionage,' arises only when the theft benefits a foreign government. This carries higher penalties than the second offense, 'theft of trade secrets,' which is more sweeping, and concerns theft benefiting any person but the true owner." Sylvia N. Albert, Jason A. Sanders & Jessica M. Mazzaro, *Twentieth Survey of White Collar Crime: Intellectual Property Crimes*, 42 AM. CRIM. L. REV. 631, 634 (2005).

79. 17 U.S.C. § 1832 (2000).

In contrast, Section 1832 applies to domestic trade secret theft. Section 1832 is a broader provision applying "to anyone who knowingly engages in the theft of trade secrets, or an attempt or conspiracy to do so."[80] The vast majority of prosecutions were filed under Section 1832, which classifies "attempt" and "conspiracy" as distinct offenses from those acts that constitute completed crimes under the statute.[81]

A large number of EEA prosecutions have been for attempt or conspiracy to steal trade secrets.[82] The government has used Section 1832 rather than 1831, even when the defendant is a foreign national or representing a foreign entity, because of the difficulty of proving the involvement of a foreign government or entity beyond a reasonable doubt.

Section 1832, sanctioning the "theft of trade secrets," is of more general application than Section 1831, but nonetheless includes several limitations not found in Section 1831:

> The three prosecutorial limitations not present in the "economic espionage" offense: (i) the intended benefit realized must be economic in nature; (ii) the thief must intend or know that the offense will injure the rightful owner; and (iii) the stolen information must be related to or included in a product produced for or placed in interstate or foreign commerce.[83]

The government's burden under Section 1831 is proof beyond a reasonable doubt that: (1) the defendant stole, or without the owner's authorization obtained, destroyed, or conveyed information; (2) the defendant knew or believed that this information was a trade secret; (3) the information was a trade secret; and (4) the defendant intended or knew that the offense would benefit a foreign government, instrumentality, or agent.[84] Section 1831 was "designed to apply only

---

80. United States v. Hsu, 155 F.3d at 195.

81. "It has been held that to establish that a defendant is guilty of conspiracy under 18 U.S.C. § 1832(a)(5), the prosecution must prove that an agreement existed, that it had an unlawful purpose, and that the defendant was a voluntary participant." J. Michael Chamblee, *Validity, Construction and Application of Title I of Economic Espionage Act of 1996*, 177 A.L.R. Fed. 609, 625 (2005)

82. *See, e.g.*, *Hsu*, 155 F.3d at 197 (noting that the EEA "defendants are charged only with attempting to steal, and conspiring to steal, trade secrets under § 1832.").

83. Sylvia N. Albert, Jason A. Sanders & Jessica M. Mazzaro, *Twentieth Survey of White Collar Crime: Intellectual Property Crimes*, 42 AM. CRIM. L. REV. 631, 636 (2005).

84. The term "foreign instrumentality" means "any agency, bureau, component, institution, association, or any legal, commercial, or business organization, firm, or entity that is

when there is 'evidence of foreign government sponsored or coordinated intelligence activity.'"[85]

6. Criminal Penalties Under the EEA

Under the foreign section of the EEA, a violator is subject to a fifteen-year prison term and a $500,000 fine.[86] The domestic trade secret theft section subjects violators to a ten-year prison term and a $250,000 fine. Organizations found guilty under the EEA can be fined up to $10 million for foreign espionage or $5 million for trade secret theft.[87] The EEA criminalizes the knowing theft of trade secrets, as well as attempts and conspiracies to steal trade secrets.[88]

The Sixth Circuit, in *United States v. Yang*,[89] held that legal impossibility was not a defense to a charge of attempt and conspiracy to steal a trade secret under the EEA's domestic trade secret section.[90] The EEA statute also provides for the criminal forfeiture of any property or proceeds derived from a violation of the statute.[91]

---

substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1) (2000).

85. *Hsu*, 155 F.3d at 195.

86. 18 U.S.C. § 1831 (2000).

87. *Id.*; 18 U.S.C. § 1832 (2000).

88. EEA prosecutions have been based on the misappropriation of, or on attempts or conspiracies to misappropriate, various types of trade secrets including: proprietary corporate documents (as has been alleged in the case with Branch and Erskine); technical reports (United States v. Yang, 281 F.3d 534 (6th Cir. 2002), *cert. denied*, 537 U.S. 1170 (2003)); documents reflecting the processes, methods and formulas for manufacturing the drug Taxol (*Hsu*, 155 F.3d at 191-92); computer data detailing the specifications for aircraft replacement parts (United States v. Lange, 312 F.3d 263, 264-65 (7th Cir. 2002)); proprietary pricing information (United States v. Morris, No. 02-CR-120 (D. Del.)); and proprietary customer information. (United States v. Chang, No. 00-CR-20203 (N.D. Calif.)). David W. Simon, *Prosecution of IP Theft Increases*, Nat'L L.J., Aug. 11, 2003, at 15.

> Section 1831, "economic espionage," requires that the theft of trade secrets benefit a foreign government, instrumentality, or agent in some manner. This type of misappropriation of trade secrets not only covers outright theft or unauthorized duplication, but also includes trafficking in stolen trade secrets, as well as the attempt and conspiracy to commit these offenses. Section 1831 includes an intent component requiring that the misappropriation be "knowingly" committed.

Albert, Sanders & Mazzaro, *supra* note 83, at 636.

89. *Yang*, 281 F.3d at 534; *See also Hsu*, 155 F.3d at 200 (holding that "Congress did not intend to allow legal impossibility to be asserted as a defense to attempt" EEA offenses).

90. 18 U.S.C. § 1832 (2000).

91. 18 U.S.C. § 1834 (2000).

7. Extraterritorial Reach of the EEA

The EEA has an expansive jurisdictional reach to punish and deter the theft of domestic trade secrets and "economic espionage that occurs overseas, so long as federal law binds the offender or an 'act in furtherance of the offense was committed in the United States.'"[92] Section 1837 of the EEA imposes criminal fines on a foreign corporation that sells a product within the United States.[93] The EEA's long arm reaches U.S. citizens and corporations "for actions occurring abroad, even when there is no other connection with the United States."[94] Prosecutors may pursue trade secret thieves outside the country "so long as some part of the activity is connected to the United States."[95]

II: THE ECONOMIC ESPIONAGE ACT: THE LAW-IN-ACTION

The future of American society depends upon our ability to compete in the global economy. "The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor . . . the companies are training the armies and the unemployed are the casualties."[96]

The underpinning of American competitiveness in the worldwide economy depends upon shielding U.S. trade secrets. The 1998 Annual Report to Congress on Foreign Collection and Industrial Espionage reported $44 billion in losses from a survey of Fortune 1,000 companies and the 300 fastest growing U.S. companies.[97] The explanation for the astonishing rise in economic espionage and its colossal cost to business is simple: "mountainous accumulations of tempting trade secrets that constitute to vast intellectual property achievements of U.S. companies."[98] One of the foremost security

92. Albert, Sanders & Mazzaro, *supra* note 83, at 637.

93. 18 U.S.C. § 1837 (2000).

94. Albert, Sanders & Mazzaro, *supra* note 83, at 637.

95. *Id.*

96. Bernard Esambert, President of the French Pasteur Institute, Paris Conference on Economic Espionage, quoted by IWS Cybercrime and Economic Espionage, http://www.iwar.org.uk/ecoespionage/ (last visited Apr. 6, 2006).

97. "Despite an overall 12-percent response rate, responding companies reported $44 billion in known and suspected losses over a 17-month period during 1996-97." Annual Report, *supra* note 33.

98. STEVEN FINK, STICKY FINGERS: MANAGING THE GLOBAL RISK OF ECONOMIC ESPIONAGE 7 (Dearborn Trade) (2002).

threats is the capacity of foreign spies to steal crucial confidential information.

The next part of the article presents findings from an empirical study that describes what the first decade of EEA prosecutions tell us about the federal criminalization of trade secret protection.

A. FINDING #1: THE CASES TELL US THAT THE EEA IS ADDRESSING GNATS, NOT CAMELS.

> For years now, there has been mounting evidence that many foreign nations and their corporations have been seeking to gain competitive advantage by stealing the trade secrets, the intangible intellectual property of inventors in this country. The Intelligence Committee has been aware that since the end of the Cold War, foreign nations have increasingly put their espionage resources to work trying to steal American economic secrets. Estimates of the loss to U.S. business from the theft of intangible intellectual property exceed $100 billion. The loss in U.S. jobs is incalculable.[99]

The EEA is not effectively punishing and deterring economic and industrial espionage. Table One reveals that less than fifty prosecutions have been pursued under the EEA since its enactment in 1996.[100] Forty-seven percent of the EEA prosecutions were filed in 2001 or 2002 (twenty-three out of forty-eight). In the period 2003-2005, the number of EEA prosecutions has dropped precipitously.[101] As of August 1, 2005, only one EEA prosecution has been filed, a case in which a former officer of a Michigan-based automobile parts manufacturer and another ex-employee were charged with being part of a conspiracy to sell trade secrets belonging to two Michigan

---

99. U.S. Dept. of Justice, Legislative History – Economic Espionage Act of 1996, *available at* http://www.usdoj.gov/criminal/cybercrime/EEAleghist.htm (last visited Apr. 6, 2006) (*quoting* Sen. Arlen Specter, R-PA) (hereinafter Legislative History).

100. "As of 2002, 92 EEA cases had been referred for prosecution. Compare this with the 210 referrals for copyright offenses and the 103 referrals for trademark crimes during the same period. And copyright and trademark cases were more likely actually to be prosecuted." Susan W. Brenner & Anthony C. Crescenzi, State-Sponsored Crime: The Futility of the Economic Espionage Act, at 73 n.161 (internal citations omitted) (unpublished manuscript, on file with author).

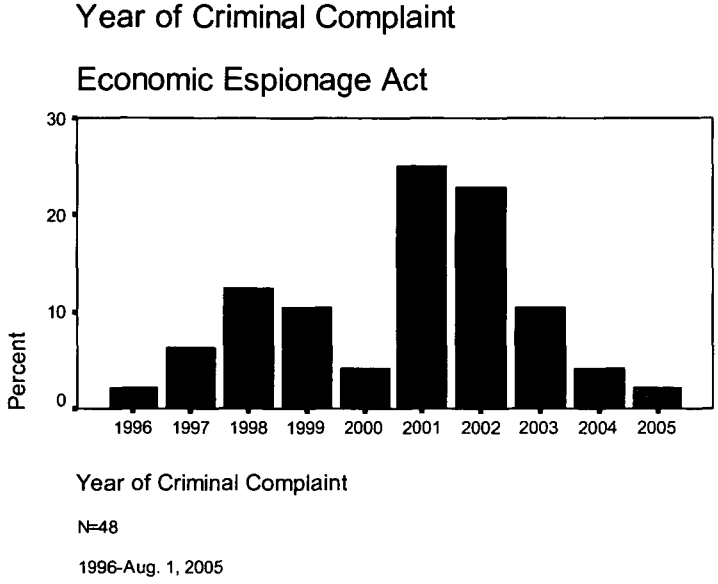
101. The Wall Street Journal recently reported that the "government is currently prosecuting about a dozen cases against individuals alleged to have sent technology, sometimes designs, sometimes software, sometimes high-tech equipment, in China illegally. FBI officials say at least three more cases will likely go ahead in the coming months." Solomon, *supra* note 36. It is unclear at this time whether these cases will result in prosecutions.

automobile parts manufacturers to a Chinese company.[102] The Chinese firm sought the trade secrets "in an effort to undercut the price the [Michigan] supplier charges for a sophisticated metal rod used in truck engines."[103]

102. *FBI Arrests Industrial Spies*, INDUS. MAIN. & PLANT OPERATION, Mar. 1, 2005, at 6 (reporting a Detroit News story in which a Michigan company's trade secrets about "profitable powdered-metal connecting rods used in truck engines was alleged to be used by Chongqing Huafa Industry Co. to undercut Metaldyne's prices").

103. David Shepardson & Brett Clanton, *FBI: Local Execs Stole Secrets for Chinese*, DETROIT NEWS, Feb. 2, 2005, at 1A, *reprinted in* 2005 WLNR 1494752.

Table One



In addition to the low overall quantity of EEA prosecutions, the fraction of cases filed against foreign governments or their agents under Section 1831 is negligible (see Table Two below). This empirical fact, seen in the light of Congress's purpose in enacting the EEA, shows how far the statutory apple has fallen from the legislative tree.

"When Congress was considering the Economic Espionage Act, Louis Freeh, then director of the FBI, testified that foreign governments 'actively target U.S. persons, firms, industries, and the U.S. government itself' to steal trade secrets, endangering the U.S. economy and national security."[104] There are justifiable reasons why few cases may be brought. The U.S. government may be detecting foreign spying but unwilling to disclose its counterspy methods, which would occur in an EEA investigation. Another reason for few cases is that U.S. intelligence agencies are seeking the same trade secret from other countries as other countries are seeking from us—

104. Daniel Sorid, *Economic-Spying Case May Signal Crackdown*, CHICAGO TRIBUNE, Nov. 23, 2003, at C1.

hence, they may want to avoid retaliatory legal actions against U.S. companies in foreign countries.[105]

Since 1996, only two of the forty-eight espionage cases have been prosecuted under the foreign espionage section of the EEA since 1996.[106] It is unlikely that law enforcement will receive international cooperation because of the very nature of state-sponsored espionage. Foreign governments simply do not have the incentive to prosecute or even extradite companies or individuals that misappropriate the trade secrets of U.S. companies. In general, the United States receives very little cooperation from our allies in prosecuting foreign spies.[107] Further, prosecution of state-sponsored espionage by allies is improbable during a period in which the United States needs backing in the war against terrorism.[108]

The first U.S. indictment under the foreign espionage section of the EEA charged two Japanese researchers with the larceny of confidential medical information from a research institute of the Cleveland Clinic Foundation on behalf of The Institute of Physical and Chemical Research (Riken), a Japanese company. The only other foreign espionage case arose out of a massive Chinese scheme to steal trade secrets in a number of Silicon Valley computer companies. In *United States v. Ye*, the defendants were indicted for trade secret theft, conspiracy, and foreign transportation of stolen property.[109]

The charges arose out of a conspiracy to steal trade secrets from four Silicon Valley companies for the People's Republic of China (PRC), although the PRC was not named in the criminal complaint.[110] The trade secrets were stolen from four high-tech companies in Silicon Valley: Transmeta Corporation (Transmeta), Sun

105. Andy Beckerman-Rodau suggested these alternative hypotheses for the failure of the EEA in actions against foreign agents, entities, or governments.

106. Albert, Sanders & Mazzaro, *supra* note 83, at 637 (discussing Section 1832 EEA prosecutions).

107. *See* Brenner & Crescenzi, *supra* note 100 (citing example of French school that basically trains experts in economic espionage).

108. I am indebted to Susan Brenner for her point that prosecutors may be reluctant to name foreign governments as accomplices in EEA crimes because it will raise serious foreign policy or diplomacy issues.

109. Press Release, U.S. Dept. of Justice, Pair from Cupertino and San Jose, California, Indicted for Economic Espionage and Theft of Trade Secrets From Silicon Valley Companies (Dec. 4, 2002), *available at* http://www.usdoj.gov/criminal/cybercrime/yeIndict.htm.

110. *Id.*

Microsystems, Inc. (Sun), NEC Electronics Corporation (NEC), and Trident Microsystems, Inc. (Trident).[111]

Both defendants were employees of Transmeta and one co-defendant also worked at Sun and NEC. The purpose of the espionage in *Ye* was to lend a hand to China whose goal was to develop a super-integrated circuit design "and form a powerful capability to compete with worldwide leaders' core development technology and products in the field of integrated circuit design."[112] Federal prosecutors were hesitant to file Section 1831 charges against the Chinese government, preferring to file a complaint under Section 1832, the domestic espionage section of the EEA.

The first decade of EEA cases demonstrates the ineffectiveness of law enforcement in stemming the tide of economic espionage. In general, EEA prosecutions are filed in cases where avaricious individuals have misappropriated trade secrets from their employer. Few of the prosecutions were against sophisticated state actors infiltrating U.S. companies or hacking into computer systems. In general, state-sponsored espionage is carried out with impunity with a trivial chance of being detected let alone prosecuted under the EEA.[113] While the EEA defendant class is highly educated, a few of the schemes to steal trade secrets are based upon blind stupidity coupled with cupidity.[114] In *United States v. Martin*, the hapless defendant was caught when she inadvertently transmitted a smoking-gun e-mail containing purloined trade secrets to a manager in the

---

111. *Id.*

112. *Id.*

113.

> On December 7, 1996, the first arrest under the EEA was made in Pittsburgh, Pennsylvania. Patrick Worthing and his brother, Daniel, were arrested by FBI agents after agreeing to sell Pittsburgh Plate Glass ("PPG") proprietary information for $1,000 to a FBI undercover agent posing as a representative of Owens-Corning. The Government alleged that Worthing solicited Owens-Corning's CEO under an assumed name in a letter that stated: "Would it be of any profit to Owens-Corning to have the inside track on PPG?"

Mark D. Seltzer & Angela A. Burns, *Criminal Consequences of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete*, 1999 B.C. INTELL. PROP. & TECH. F. 052501 (discussing United States v. Worthing, Crim. No. 97-9 (W.D. Pa, Crim. Complaint filed Dec. 9, 1996)), http://www.bc.edu/bc_org/avp/law/st_org/iptf/articles/content/1999052501.html; *see also* United States v. Davis, Crim. No. 97-CR-124 (M.D. Tenn. 1997), *Id.* (discussing case in which a contractor for Gillette contacted Schick, Wilkinson and Bic offering to sell information about Gillette's new shaving system).

114. This pattern is not confined to EEA arrests and prosecutions. Most criminals are caught because they are either stupid or they do stupid things.

targeted corporation.[115] In *United States v. Hsu*, the would-be spy was caught when he approached an undercover FBI agent mistakenly believing he was a technological information broker.[116] All but a small number of the EEA prosecutions grew out of poorly thought-out schemes to steal and attempt to sell this stolen information on the open market or to competitors. The criminal prosecutions described in Table One and Table Two are overwhelmingly routine domestic trade secret misappropriations rather than theft by foreign governments and their agents. By focusing on run-of-the-mill domestic espionage and side-stepping far more injurious foreign espionage, the EEA is straining at gnats and swallowing camels.

B. FINDING #2: THERE ARE SUBSTANTIAL BARRIERS TO IMPLEMENTING THE CURRENT REGIME

While the EEA law-in-the-books may be reasonable, the EEA law-in-action has been not easy to implement in practice. One reason is that criminal law enforcement inevitably lags behind rapidly developing technologies. Spyware, for example, is an increasing security threat ranked by the business community ahead of spam, hackers, and cyberterrorism. Corporate spies routinely use diagnostic tools to intercept their competitors' messages.[117] None of these activities have yet been the subject of an EEA prosecution.

Another stumbling block resulting in a low number of EEA prosecutions is the reluctance of federal law enforcers to assign a high priority to economic-based crimes. In the first months after the EEA was enacted, the FBI filed no cases, although they investigated approximately 800 incidents of possible economic espionage.[118] In addition, federal law enforcement officers have given a higher priority to enforcing federal criminal penalties for copyright and trademark infringement than trade secret theft.[119]

---

115. United States v. Martin, 228 F.3d 1 (1st Cir. 2000).

116. United States v. Hsu, 982 F. Supp. 1022 (E.D. Pa. 1997).

117. "Forbes said about a dozen versions of Myfip may have been in circulation and used to steal sensitive documents including mechanical designs and circuit board layouts." Rob Lever, *U.S.–Sino Cyber War*, GEELONG ADVERTISER, July 27, 2005, at 21.

118. Mossinghoff, Mason & Oblon, supra note 51.

119. The federal government has made trademark and copyright infringement a priority. "'Operation Buccaneer,' a collaborative effort by the U.S. Customs Service and the Department of Justice . . , and the 'Joint Anti-Piracy Initiative' which, additionally, involves the FBI, is evidence of the government's ongoing commitment to prosecute intellectual property crimes." Albert, Sanders & Mazzaro, *supra* note 83, at 633.

These barriers to effective statutory enforcement are explored below, along with other problems such as lack of cooperation by espionage victims, jurisdictional issues, and the special difficulties of tackling foreign governments and their instrumentalities.

1. Previously Targeted Companies Fear Revictimization

The chief obstacleto EEA prosecutions is the self-inflicted wound of cover-ups by corporate victims or the refusal to report trade secret theft to federal law enforcement agencies.[120] Corporations often fear the adverse publicity that accompanies punitive damages and other forms of civil punishment far more than the monetary costs.[121] Companies victimized by defective software will not report these crimes because they are concerned about the loss of public confidence in their products or services. Many companies victimized by industrial or economic espionage do not file complaints with federal law enforcement authorities because they may be revictimized by adverse publicity, lower stock prices,[122] and waning public confidence.[123]

Customers and business partners will think twice about sharing trade secrets with a trading partner or joint venturer that has inadequate computer security to prevent computer hacking or the theft of confidential information. Once the Department of Justice enters into a case, the corporate victim is no longer in control of the investigation. A company may incur costs by opening up its internal records to federal law enforcement. Since the EEA has no private

120. I am indebted to Susan Brenner for suggesting that the risk of revictimization is a real deterrent against reporting economic espionage and could be greatly reduced by reforming the discovery provisions of the EEA.

121. Andrea A. Curcio, *Painful Publicity - An Alternative Punitive Damage Sanction*, 45 DEPAUL L. REV. 341, 361-62 (1996).

122. *See generally* Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 BUS. LAW. 25, 29 (2001) (documenting that companies suffer from declining stock prices after reporting an EEA offense).

123.

> Perhaps the biggest adjustment business executives will have to make concerns the shift of power from the victimized business to the prosecutor. In all criminal prosecutions the prosecutor—not the victim—is in control. Consequently, victim businesses will lack the power to direct the prosecution, engage in negotiations, or even dismiss the case.

J. Derek Mason, Gerald J. Mossinghoff & David A. Oblon, *The Economic Espionage Act: Federal Protection for Corporate Trade Secrets*, http://www.oblon.com/Pub/economicespionageactII.html (last visited Apr. 5, 2006).

cause of action, the corporate victim will be unable to recoup any of their losses. Companies will often find the cost of cooperating with law enforcement to far outweigh any potential gain.

2. Lack of Federal Law Enforcement Resources

Law enforcement agencies are far less prepared to address sophisticated espionage by foreign governments than other law enforcement priorities. While industrial espionage has always been a part of the American experience, economic espionage in the age of information poses a greater menace because of the greater vulnerability of trade secrets in a networked world where a company's crown jewels may be transported around the world at the click of the mouse. In addition, many schemes to steal trade secrets go undetected and unprosecuted because these crimes are difficult to trace because of the greater anonymity possible by computer hackers.

Crime on the streets receives greater consideration than corporate crime hatched in the suites. More successful enforcement of the EEA requires federal law enforcement officers who have a highly developed command of computer-based technologies and the computer expertise to track foreign spies in the cross-border environment of the Internet.[124] Another difficulty is that there are far too few federal law enforcement officers with proficiency in computer crime or cybercrime investigations, and these officers have to deal with many other serious crimes as well.[125] Cybercrime prosecutors also face enormous logistical and operational difficulties. "The ability to track criminals in multiple jurisdictions, as well as specialized knowledge of vast varieties of hardware, software, applications, foreign languages, and other related issues, requires regional, state, and national multiagency cooperation."[126] Fear of violating laws against racial profiling in the federal law enforcement community may be another barrier.[127]

---

124. *See, e.g.*, Beckerman-Rodau, *supra* note 20, at 234 (describing the greater difficulty of protecting trade secrets in the networked world of computers).

125. Susan Brenner was the first to make this point.

126. Tony Aeilts, *Defending Against Cybercrime and Terrorism: a New Role for Universities*, THE FBI LAW ENFORCEMENT BULLETIN, Jan. 2005, at 14.

127. The Wall Street Journal reported that Asian-Americans in Silicon Valley are concerned about FBI overreaching with a "new wave of racial profiling . . . reminiscent of the 2000 case of Wen Ho Lee, a Taiwan-born American scientist who was fired from his job at Los Alamos National Laboratory and was prosecuted for allegedly giving away nuclear secrets to Beijing." Solomon, *supra* note 36. It is unclear at this time whether these cases will result in prosecutions.

Economic and industrial espionage is difficult to detect without elaborate sting operations because many of these white-collar crimes produce no traditional crime scene. Online spies, current employees, or ex-employees leave few of the digital footprints that DNA evidence, fingerprints, or other personally identifiable information used to catch most criminals leave behind. Digital trade secrets may be copied within seconds and are easier to transport than containers of proprietary documents.

Electronic trade secret thieves that commit financial crimes also leave fewer clues than white-collar criminals who alter checks or intercept promissory notes. The use of false e-mail headers, offshore sites, and anonymous e-mailers also make catching foreign spies more difficult. In a cybertheft case, for example, an information security expert might need to reconstruct e-mails or other electronic smoking guns that document attempted or completed misappropriations of trade secrets.

The FBI and other federal enforcers have taken a reactive rather than proactive approach.[128] To date, federal law enforcement has been ineffective in deterring the spread of spyware used to steal data or launch "zombie attacks" on corporate computers.[129] Spyware or system monitors are used to steal trade secrets by running in the background, recording what is typed in a keyboard, and sending that information to another location.[130]

In most investigations, the targeted companies hire private investigators after receiving competitive intelligence about attempts to misappropriate their trade secrets.[131] In order to effectively act against misappropriators, the targeted company must have the resources to conduct their own private investigations before

128. Susan W. Brenner and Anthony C. Crescenzi argue that a paradigm shift from reactive to proactive law enforcement is necessary to prevent espionage. *See* Brenner & Crescenzi, *supra* note 100, at 55.

129. A computer that has been hijacked by a backdoor Trojan is known as a zombie. Sophos estimates that "as much as 40% of spam is being sent from zombie computers without the user's knowledge." *Looking at. . .Spyware*, SOPHOS NEWS, (Sophos Inc., Lynnfield, M.A.), Nov. 2004, at 3.

130. *Id.*

131. Andy Beckerman-Rodau reminded me that private policing is not limited to trade secret investigations. The private investigator is also used to investigate trademark infringement, counterfeit goods, gray goods importation and related unfair competition. It is arguable that in such cases that it is the initial responsibility of the property owner to protect his or her property and after all intellectual property is a species of property.

contacting federal law enforcement authorities.[132] Hardly any cases of industrial spying have therefore been pursued even if overwhelming evidence of espionage was collected by the corporate victim and supplied to law enforcement.[133]

Another obstruction to successful prosecutions against foreign governments is the requirement that the U.S. Department of Justice receive prior approval from the U.S. Attorney General prior to filing Section 1831 actions. The Department of Justice has inserted "a requirement in the U.S. Attorney's Manual that prosecutions continue to be approved and strictly supervised by the Executive Office of the United States Attorney."[134] The U.S. Attorney General or other high-level Deputy or Assistant Attorneys General in the Criminal Division supervise prosecutions.[135] Few cases are filed because of the fear that a given EEA prosecution against a state actor or their affiliated agents may precipitate a foreign policy crisis.

3. Displacement of EEA Cases by Other Priorities

Federal law enforcement needs more technical and human resources to detect foreign governments spying on U.S. industries. Federal law enforcement officers are less likely to devote substantial human and economic capital to pursuing state-sponsored espionage because of the greater priority of international terrorism. After 9/11, the number of EEA prosecutions has fallen off significantly. An expert in information security observes:

> Law enforcement is stretched too thin fighting terrorism, and the bad guys . . . see that it's open season on U.S. businesses. They can come in and just cherry pick the trade secrets they want.[136]

---

132. Joseph N. Hosteny, *The Economic Espionage Act: A Very Mixed Blessing*, http://www.hosteny.com/articles/espionage.html (last visited Apr. 6, 2006).

133.

> Thus, to make out an offense under the economic espionage section, the prosecution must show in each instance that the perpetrator intended to or knew that his or her actions would aid a foreign government, instrumentality, or agent. Enforcement agencies should administer this section with its principle purpose in mind and therefore should not apply section 1831 to foreign corporations when there is no evidence of foreign government sponsored or coordinated intelligence activity.

Legislative History, *supra* note 99.

134. *Id.*

135. Mossinghoff, Mason & Oblon, *supra* note 51.

136. Gathright & Hua, *supra* note 55.

Economic espionage prosecutions are often displaced by other law enforcement priorities, which fluctuate between offices:

> In Chicago, where I live, gang prosecutions have become a high priority. Prosecutions involving narcotics and other controlled substances are also important, and consume a large proportion of the resources of any United States Attorney. Chicago is famous too for the many prosecutions of public officials, including a former governor, state representatives, and many judges in the Circuit Court of Cook County, law enforcement officers, aldermen, and many others.[137]

4. Limits to Extraterritorial Reach of EEA

The EEA protects against theft that occurs either (1) in the United States, or (2) outside the United States and (3) an act in furtherance of the offense was committed in the United States, or (4) if the violator is a US person or organization.[138] Extradition has proven to be an obstacle in economic espionage cases. The Tokyo High Court rejected the U.S. request that a Japanese scientist be extradited to the United States to face charges of economic espionage.[139] The Japanese scientist was charged with the pilfering of genetic materials related to Alzheimer's disease conducted at the Cleveland Clinic Foundation.[140] The Japanese court held that the scientist had no probable cause to benefit his new employer, which was an institute funded by the Japanese government.[141] A new treaty or convention requiring countries to extradite trade secret thieves is thus necessary.

---

137. Hosteny, *supra* note 132.

138. Federal Bureau of Investigation, Investigative Programs: Counterintelligence Division, http://www.fbi.gov/hq/ci/economic.htm (last visited Apr. 6, 2006).

139. Tetsuya Morimoto, *First Japanese Denial of U.S. Extradition Request: Economic Espionage Case*, 20 INT'L ENF. L. RPTR. 288 (2004).

140. *Id.* at 289.

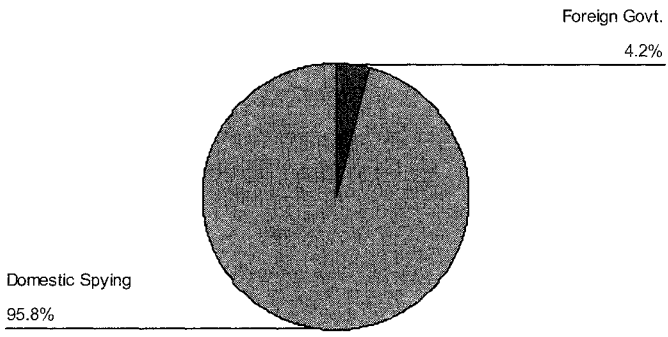
141. *Id.* at 290.

5. Additional Difficulties in Prosecuting Foreign Governments and Agents

Table Two

Foreign Government Prosecutions

Economic Espionage Act, Section 1832



N=48

1996-Aug. 1, 2005

Table Two confirms that the EEA has proven an unproductive tool in the war against state-sponsored espionage. Criminal activity involving foreign governments is almost never prosecuted even though the chief statutory purpose of the EEA is to punish spying by foreign nations, agents, and their closely connected corporate entities. From 1996 to 2005, U.S. prosecutors implicated foreign governments or agents in only two EEA prosecutions. Federal prosecutors rarely charge foreign governments or agents with crimes, even though there is overwhelming evidence of widespread state sponsored economic espionage.

Under the same period, thirty-three out of the forty-eight defendants charged with economic espionage were Americans. One in four EEA defendants were foreign nationals from countries of the Far East: Peoples Republic of China (N=5), Taiwan (N=4), Malaysia (N=2), and Japan (N=1). In many of these cases, the corporate spy

was affiliated with a foreign company closely connected to a foreign government. Yet, the U.S. government has declined to charge foreign governments or entities, choosing to try each case under EEA's domestic trade secret section.

It is often difficult to discover the identity of foreign spies, who frequently operate in countries that fund their activities. Economic and industrial espionage on the Internet crosses national borders, creating the need for international cooperation in law enforcement. "Protecting trade secrets after they've been posted online is a bit like locking the barn door after the horse is stolen."[142] The intellectual property "have nots" have little motivation to protect the intellectual property rights of U.S. companies.

Federal prosecutors have been reluctant to prosecute foreign governments, agents, or entities for economic or industrial espionage because prosecutions may have foreign policy implications. A possible explanation is that overburdened federal prosecutors fear foreign policy repercussions from naming other governments in criminal complaints.

Another hypothesis is that the U.S. Attorney General overrides the filing of criminal charges against foreign governments, closely connected corporate entities, or agents. One of the difficulties facing the law enforcement community is also the lack of know-how in information technologies necessary to detect espionage. U.S. intelligence agencies may be more effective in dealing with foreign trade secret theft cases than are criminal agencies like the Federal Bureau of Investigation.

Even when prosecutors have adequate technical and scientific expertise to trail a devious foreign spy, they may be impeded by the warrant requirements, cross-border jurisdictional concerns and the possibility that a foreign arrest will precipitate a diplomatic crisis. Federal prosecutors are likely to fear the foreign policy repercussions that will be inevitable when naming a foreign government, instrumentality, or agent in a criminal complaint assuming that approval is granted by the U.S. Attorney General's Office.

C. FINDING #3: BIOMEDICAL, SOFTWARE AND HIGH TECHNOLOGY INDUSTRIES ARE THE PRIME

142. Mark D. Rasch, *Can You Keep A Secret? As the Apple Case Demonstrates, the Internet Makes Trade Secret Protection a Challenge*, IP LAW & BUSINESS, May 2005, at 24.

TARGETS OF ECONOMIC AND INDUSTRIAL ESPIONAGE.

Table Three

1. High Technology as Target of Trade Secret Espionage

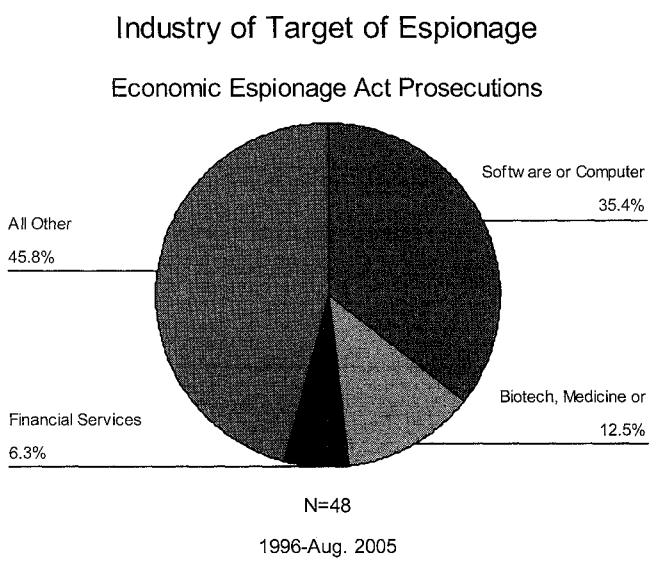


Table Three confirms that targets in most cases of economic espionage and other collection activities are the computer software, biotechnology and medical industries. However, traditional manufacturing, defense and aerospace, telecommunications, engine technologies, manufacturing processes, and media have also been targets. Source code, software, or other computer-related proprietary information was purloined in nineteen out of forty-eight cases (40%).[143] Project information, pricing information, or research on products or processes was stolen in 19% of the EEA prosecutions (N=9). Customer and business information was taken in 15% of the cases leading to prosecutions (N=7). Engineering or schematic drawings of products were the target of 10% of EEA cases (N=5). Biogenetic materials (N=2), drug delivery systems (N=2), and

143. ROGER MILGRIM, MILGRIM ON TRADE SECRETS § 1.09[5][b] (2005) (stating that the "single most important 'product' eligible for trade secret protection is computer software.").

competitor's business plans (N=2), access card or control information thefts accounted for the remaining cases. This empirical finding suggests that small or medium-sized companies simply do not have the resources to do the groundwork necessary to gather evidence needed by prosecutors.

2. Software or Computer Industry

Several of the most publicized foreign espionage cases were filed against perpetrators stealing computer chip design and source code from Silicon Valley companies.[144] In *United States v. Genovese*,[145] the defendant was found to be responsible for his unauthorized Internet sale of the source code for the computer programs Microsoft Windows NT 4.0 and Windows 2000, software that had been stolen by third parties.[146] In that case, "portions of Microsoft Corporation's source code for two of its computer operating systems, Windows NT 4.0 and Windows 2000, appeared on the Internet."[147] Microsoft hired a private online security firm that downloaded the purloined code after transferring twenty dollars to the defendant through an online payment service.[148] After the defendant provided access to the source code through his FTP server, Microsoft alerted the FBI.[149] An undercover FBI agent then contacted Genovese and purchased the Microsoft source code.[150] The sting operation resulted in the arrest of the defendant for unlawfully downloading and selling a trade secret.[151] In another stolen computer-related technology case, two defendants placed an Internet

144. John R. Wilke, *Two Silicon Valley Cases Raises Fears of Chinese Espionage*, WALL ST. J., Jan. 15, 2003, at A4, *available at* http://www.economicespionage.com/WSJ.htm (last visited Apr. 5, 2006); *See, e.g.*, Press Release, United States Department of Justice, San Jose Man Indicted for Theft of Trade Secrets and Computer Fraud (Apr. 2, 2003), http://www.usdoj.gov/criminal/cybercrime/murphyIndict.htm (reporting arrest of San Jose defendant for stealing his employer's chip features, and wireless computer networks specifications).

145. Press Release, United States Department of Justice, U.S. Arrests Connecticut Man on Charge of Selling Stolen Microsoft Windows Source Code (Nov. 9, 2004), http://www.usdoj.gov/criminal/cybercrime/genoveseCharge.htm.

146. United States v. Genovese, 2005 U.S. Dist. LEXIS 11947 (S.D.N.Y., June 21, 2005).

147. "Genovese posted a message on his Website offering the code for sale: "win2000 source code jacked . . . and illmob.org got a copy of it . . . im [sic] sure if you look hard you can find it or if you wanna buy it ill give you a password to my ftp." *Id.* at *1.

148. *Id.*

149. *Id.*

150. *Id.*

151. *Id.*

advertisement offering stolen prototype Intel Central Processing Units (CPU) for "Slot II" computers.[152] The victims of software or computer-related trade secret theft in the EEA database included well-known companies such as C & D Semiconductor Services, Cisco, IBM, Intel, Jasmine Networks, Lucent Technologies, Sun Microsystems, Varian, and Smart software.

3. Prosecutions for Biomedical and Genetic Piracy

During the first decade since the federal trade secret statute was enacted, EEA prosecutions were initiated for trade secrets stolen from a number of important companies in the biotechnology/medical or pharmaceutical sector of the economy. Biomedical targets included the Harvard Medical School, Zirmed, Bristol-Myers, and the Cleveland Clinic. The first EEA prosecution against a foreign national was filed in 1997 against Taiwanese spies who attempted to steal research on the anti-cancer drug "Taxol" from Bristol-Myers Squibb Co.[153] In the Taxol trade secret theft case, the prosecution was filed under Section 1832, rather than Section 1831 which was reserved for prosecutions against foreign governments, entities, or agents. The Taxol case was prosecuted for attempted theft of trade secrets and conspiracy to steal trade secrets.[154]

In July of 2005, a Japanese scientist and her Chinese husband "pleaded not guilty to charges that they transported stolen genetic information from a Harvard Medical School laboratory where they once worked."[155] The charges arose out of the alleged theft of certain trade secrets belonging to Harvard Medical School, including reagents used to develop new immunosuppressive drugs to control organ rejection.[156] Thirteen out of the forty-eight EEA prosecutions (27%) from 1996 to 2005 were outright thefts of proprietary or confidential information from traditional manufacturers. The remaining targeted industries were mining, telecommunications, media, engineering, petroleum, and service sectors.

---

152. *See* Halligan, *supra* note 14 (discussing Criminal Case No. 4: 98M37 (E.D. Texas, Feb. 26, 1998)).

153. United States v. Hsu, 155 F.3d 189, 202 (3d Cir. 1998).

154. 18 U.S.C. § 1832(a)(4) (2000).

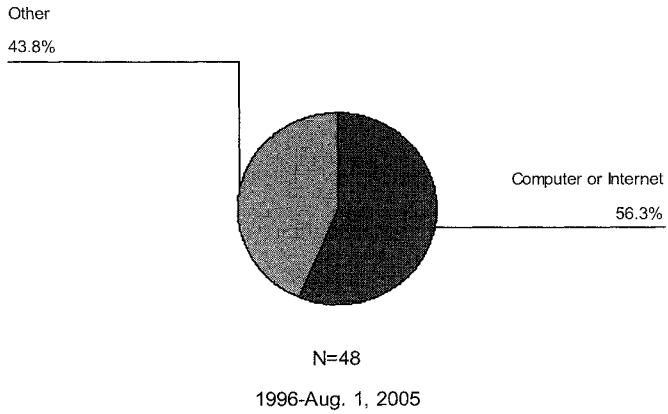
155. *Japanese Scientist, Husband Plead Not Guilty in DNA Theft*, JAPAN SCIENCE SCAN, July 18, 2005, *available at* 2005 WLNR 11272094.

156. *Id.*

Table Four

Computer or Internet Instrumentality

Method of Trade Secret Theft or Attempt



Computers are not only the target of espionage, but also the instrumentality that enables most trade secret or data theft. A recent U.S.-CERT study uncovered high or medium vulnerabilities in the most popular versions of both Windows and UNIX/LINUX operating systems.[157] Microsoft's Internet Explorer, for example, does not properly display the location of HTML documents in the status bar. This known vulnerability lulls some users into revealing sensitive information such as credit card numbers.[158] Table Four reveals that 56% of the EEA defendants used computers as the principal instrumentality to steal trade secrets. The computer and the Internet permit "new forms of potentially criminal behavior that would not have been possible without the use of computer technology."[159] The

157. High-risk vulnerabilities were ones that will allow an intruder to immediately access a computer system or to allow an intruder to execute virulent code or allow unauthorized users to send sequences of instructions to computer systems. Medium-risk vulnerabilities were defined as ones that allow intruders privileged access. U.S.-CERT, *supra* note 11.

158. *See* United States Computer Emergency Readiness Team—Vulnerability Note #652278, http://www.kb.cert.org/vuls/id/652278.

159. RALPH D. CLIFFORD, CYBERCRIME; THE INVESTIGATION, PROSECUTION, AND DEFENSE OF A COMPUTER-RELATED CRIME 2-3 (2001).

perpetrator used a computer and the Internet to transfer data as opposed to physically carrying away trade secrets from a firm.

In 54% of the cases, the defendant was charged only with violation of the EEA. Federal prosecutors also filed ancillary charges of the Computer Abuse and Fraud Act in 10% of the cases (N=5).[160] A count for Mail Fraud or Wire Fraud was found in another 8% of the cases prosecuted (N=4). The Interstate Transportation of Stolen Property Act was an additional charge in five other cases (10%) whereas federal criminal conspiracy was charged in another six cases (13%). Overall, these findings confirm the widespread use of computers and the Internet to transfer stolen trade secrets.

This empirical study of economic espionage in the private sector parallels findings that computers were frequently the instrumentality for computer intrusion cases where federal agencies were victimized. The study by the U.S. Department of Justice concluded that most cases prosecuted were for attacks on government computer networks, not private corporate networks.[161] Federal prosecutors were unable to prosecute a single case in which software vulnerabilities resulted in computer intrusions because most prosecuted cases involved knowledgeable insiders. This finding is critically important evidence that EEA prosecutors are failing to detect, let alone punish, the most sophisticated state-sponsored economic espionage that preys upon software vulnerabilities.[162]

---

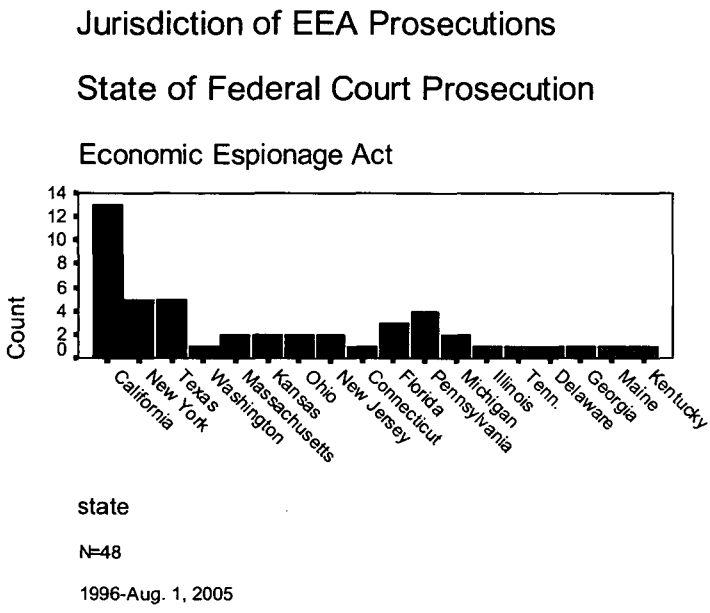
160. The Computer Fraud and Abuse Act (CFAA) is the single most important federal statute governing computer crime. The CFAA punishes and deters hacking, creating viruses, and other forms of computer crime, and extends to all computers involved in interstate commerce. The CFAA was enacted in 1984 and has been amended several times. Its jurisdiction includes the Internet. The CFAA prohibits any person from knowingly causing the transmission of information that intentionally damages a protected computer. It is a violation of the CFAA for persons to obtain unauthorized access to the computer networks of government agencies and financial institutions, as well as computers used in interstate or foreign commerce. Michael L. Rustad, *supra* note 19, at 89 (footnotes omitted).

161. *Id.* at 65 (describing prosecutions in intrusions into NASA Jet Propulsion Lab and U.S. Postal Service computers, and a hack attack on American and Israeli computers).

162. I am, of course, making reference to the famous Sherlock Holmes story in which Holmes found relevance in the fact that the dog kept in the stables did not bark during a nighttime intrusion. The fact that the dog did not bark created an inference that the intrusion was by a trusted insider. In this case, the absence of software defect cases reveals that federal law enforcers lack the resources and expertise to detect intrusions exploiting software vulnerabilities. *See*, ARTHUR CONAN DOYLE, SILVER BLAZE, THE COMPLETE SHERLOCK HOLMES 143 (Random House 2002). (describing the "The Simpson incident in which the dog kept in the stables did not bark.").

D. FINDING #4: THE SILICON VALLEY AND OTHER HIGH TECHNOLOGY AREAS WERE TARGETED BY INDUSTRIAL AND ECONOMIC ESPIONAGE

Table Five



The new battleground for economic espionage concentrates on information technology, biotechnology, and traditional manufacturing.[163] Only eighteen out of the fifty-one U.S. jurisdictions had one or more EEA prosecutions. Table Five shows that three states, California, New York, and Texas, accounted for nearly half of all EEA prosecutions for 1996 to 2005. Twenty-seven percent of the EEA prosecutions were filed in California (N=13), followed by New York (N=5), and Texas (N=5), each accounting for 10% of the prosecutions. Most states did not have a single federal court criminal case arising out of an EEA prosecution during the past decade. A total of only eighteen jurisdictions had one or more prosecutions in that time period. Most EEA prosecutions were filed

163. HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING 19 (2004).

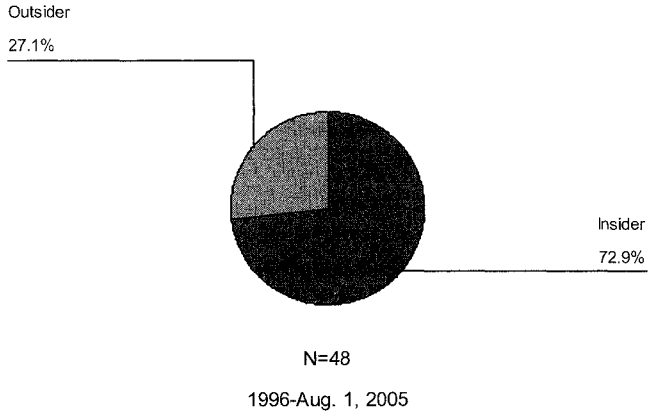
in high technology centers of innovation though there was a smattering of cases filed in other states. This finding reveals that economic espionage is targeting our country's most sophisticated technologies.

E. FINDING #5: WHAT WE KNOW ABOUT PERPETRATORS: HIGHLY EDUCATED MALES WHO TEND TO BE THE ENEMY WITHIN

Table Six

EEA Defendant's Role

(Insiders vs. Outsiders)



The greatest threat of corporate espionage is not the hacker, but the enemy within. Employees, ex-employees, and insiders were the primary wrongdoers in 73% of the EEA prosecutions. Economic espionage cases are no exception to the rule that insiders are more likely to misappropriate trade secrets. In *Kissane v. United States*, the defendant worked as a release engineer on a software package marketed to large telecommunications companies abroad.[164] The defendant sent e-mail messages to two of his employer's competitors

164. *See* Halligan, *supra* note 14 (discussing United States v. Thomas Kissane, No. 1:02CR626 (S.D.N.Y. 2002)).

offering source code for sale.[165] In another industrial espionage case, two former Boeing Company managers were charged with the theft of Lockheed Martin trade secrets for a U.S. Air Force rocket program.[166] Table Nine reveals that federal law enforcement officials participated in sting operations in slightly more than one in four EEA cases prosecuted (27%).[167] This finding suggests that the government will only infrequently "devote significant resources to the investigation, prosecution and enforcement of the EEA."[168]

In *United States v. Tse Throw Sun*, a 31-year old Singapore national was arrested in an FBI sting operation.[169] The sting began after an unidentified person called a California translation business offering to sell customer lists and detailed billing information stolen from his or her Chicago competitor. The California firm reported being approached to the FBI and a sting operation was organized. Masquerading as a company official, an FBI agent purchased material that included an online profit-and-loss statement, billing summaries, call counts, and an e-mail message discussing Language Line for $5,000.[170]

In ten of the forty-eight EEA prosecutions since 1996, a trade secret owner's competitor reported being approached by an insider seeking to sell purloined documents. In *United States v. Hsu*, a technical director of a Taiwanese firm contacted an undercover FBI agent in an attempt to steal trade secrets about anti-cancer drugs from a pharmaceutical company.[171] The defendant told an undercover FBI agent that his company would pay $400,000 in cash, stock, and royalties to employees willing to give them documents about the drug. Most EEA cases were initiated by the targeted company who

---

165. *Id.*

166. Press Release, U.S. Dept. of Justice, Two Former Boeing Managers Charged in Plot to Steal Trade Secrets from Lockheed Martin (Jun. 25, 2003), http://www.usdoj.gov/criminal/cybercrime/branchCharge.htm (discussing United States v. Branch and Erskine, No. 03-M-1453 (C.D. Calif.)).

167. *See, e.g.*, United States v. Yang, 74 F. Supp.2d 724 (N.D. Ohio 1999) (involving a defendant who was caught through joint collaboration of the FBI and the corporate victim); United States v. Hsu, 155 F.3d 189, 189 (3d Cir. 1998) (discussing EEA investigation spearheaded by an undercover FBI agent whom the defendant mistakenly believed to be a technological information broker).

168. NASHERI, *supra* note 163, at 168.

169. Press Release, U.S. Dept. of Justice, Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter's Information (Apr. 11, 2003), http://www.usdoj.gov/criminal/cybercrime/sunPlea.htm.

170. *Id.*

171. *Hsu*, 155 F.3d at 189.

learned of the theft of trade secrets through their own investigations. During the first decade of EEA cases, the Department of Justice initiated complaints generally only after the corporate victim of espionage had completed the bulk of the investigation.

In *United States v. Serebryany*, a nineteen-year-old insider stole access card control information for DirectTV.[172] In *United States v Kissane*, the defendant worked as a release engineer on a software package marketed to large telecommunications companies abroad.[173] The defendant sent e-mail messages to two of his employer's competitors offering source code for sale.[174] The finding that nearly three out of four EEA defendants were insiders, employees, or ex-employees is consistent with an earlier study, which concluded:

> that the significant threat to electronic data comes from disgruntled employees with intimate knowledge of a company's highly sensitive intellectual property, trade secrets, computer software, business, financial and customer information, and even DOS prevention programs.[175]

The EEA defendant was an outsider in only thirteen out of forty-eight federal criminal prosecutions (27%). Corporate spies tend to be well-educated insiders who are generally professionals or technicians rather than low-level functionaries.

172. Press Release, U.S. Dept. of Justice, L.A. Man Sentenced for Stealing Trade Secrets Pertaining to 'Smart Card' Technology (Sept. 8, 2003), http://www.usdoj.gov/criminal/cybercrime/serebryanySent.htm.

173. *See* Halligan, *supra* note 14 (discussing United States v. Kissane, No. 1:02CR626 (S.D.N.Y. 2002)).

174. *Id.*

175. Rustad, *supra* note 19.

Table Seven

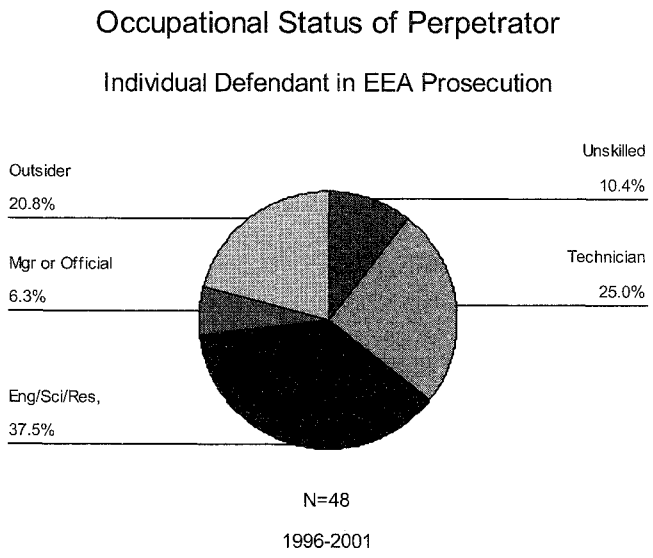


Table Seven illustrates that three out of four EEA perpetrators were single individuals. More than one individual defendant was charged in approximately 19% of the cases (N=9). A corporation was charged with industrial espionage in only 6% of the cases (N=3). Thirty-eight percent of the perpetrators charged with violating the EEA were engineers, scientists or researchers. Another 25% of the EEA defendants had occupations classifiable as technicians. The median EEA defendant is a forty-year-old white-collar male. In 77% of the cases (N=37) a male was charged. In another 10% of the EEA cases in the sample, more than one male defendant was named in the indictment. Females were never perpetrators apart from being named as co-defendants with male accomplices (N=6). Eight in ten of the EEA perpetrators were employees, ex-employees, or otherwise classified as insiders.

F. FINDING #6: MOST EEA PERPETRATORS WERE AMERICAN CITIZENS BUT ONE IN FOUR WAS FROM COUNTRIES OF THE FAR EAST.

Table Eight

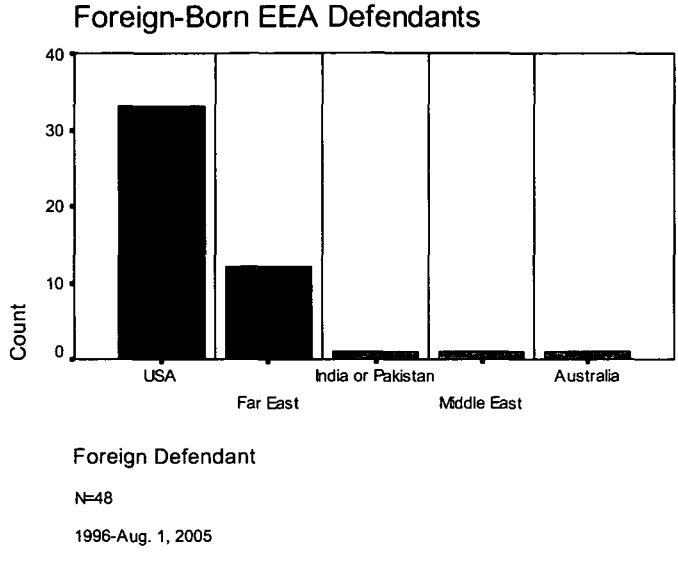


Table Eight demonstrates that only a small percentage of foreign spies are prosecuted under the EEA. The database documents only one reported case of a computer hacker or virus planter being sued for espionage under the EEA. Yet, several Chinese companies use economic espionage to steal computer code from U.S. companies.[176] Trojan horses are used to infect U.S. companies' personal computers to gather "sensitive documents, like CAD/CAM files used to store, say, mechanical designs, electronic circuit board schematics and layouts."[177] In May of 2005, the Israeli police arrested twenty-one persons for using Trojan horse software to steal documents and images for pending patents from their rivals.[178]

176. Nathan Vardi, *Chinese Take Out*, FORBES, July 25, 2005, at 54.

177. *Id.*

178. *Israeli Corporate Spy Scandal, Top Execs Arrested for Allegedly Using Spyware to Sniff Out Rivals' Strategies*, RED HERRING, May 31, 2005, *available at*

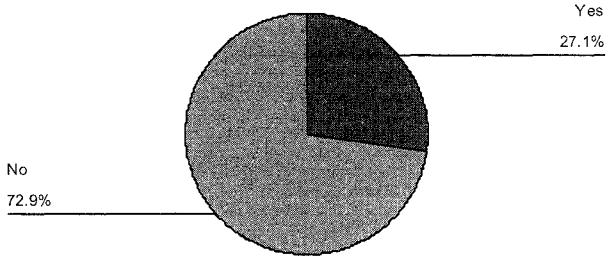
Chinese industrial spies steal data by linking Internet protocol addresses to an Internet domain name in Tianjin, China.[179] The incident is just the "start of a wave of China-sponsored cybercrime that will seek out vital trade secrets."[180] The EEA is playing no role in detecting, let alone punishing, this type of computer-related espionage.

G. FINDING #7: EEA INVESTIGATIONS ARE GENERALLY DONE BY THE VICTIM OF TRADE SECRET THEFT OR ATTEMPTED THEFT.

Table Nine

Economic Espionage Prosecutions

Law Enforcement Use of Sting Operations



N=48

1996 to Aug. 1, 2005

H. FINDING #8: THE EEA IS PEA SHOOTER, NOT A POWERFUL WEAPON IN PUNISHING AND DETERRING ECONOMIC ESPIONAGE.

The EEA law-in-the-books prescribe fines of up to $500,000 for individuals and corporate fines of up to $5 million for domestic

---

http://www.redherring.com/Article.aspx?a=12214&hed=Israel+Corporate+Spy+Scandal (last visited Apr. 5, 2006).

179. *See* Vardi, *supra* note 176.

180. *Id.*

espionage. Trade secret theft performed for a foreign government, entity, or agent can result in fifteen years of jail time.[181] In addition to fines and jail time, a defendant may have his or her assets forfeited under the EEA's criminal forfeiture section.[182] As of August 1, 2005, the defendant in twenty-two out of forty-eight EEA prosecutions had not been sentenced or fined. For the twenty-six cases where sentencing did take place, defendants received home detention or probation in 19% of the cases (N=5).[183] Another 19% were sentenced to federal prison for a period up to one year (N=5).[184] The median criminal sentence was one to three years in federal prison (N=12 or

---

181.

> Persons convicted of violating Section 1831 may be fined up to $500,000 or imprisoned up to 15 years, or both, while any organization that commits any offense prohibited by Section 1831 may be fined up to $10,000,000. A person convicted of violating Section 1832 faces a fine of up to $500,000 or a prison sentence of up to 10 years, or both, while any organization that commits any offense described in Section 1832 may be fined up to $5,000,000.

Sorojini J. Biswas, The Economic Espionage Act of 1996, http://www.myersbigel.com/ts_articles/trade_secret4.htm (last visited Apr. 5, 2006).

182.

> Section 1834 [of the EEA] provides for the criminal forfeiture of property obtained or used in the process of violating Sections 1831 or 1832. The section provides for criminal forfeiture to the United States of any property constituting or derived from the process of violation of the act, and the forfeiture of any property used or intended to be used in the furtherance or commitance of the act. This section may allow, for example, prosecutors and enforcers to dismantle internet espionage schemes and seek criminal forfeiture of all computers and devices used to commit the offenses prohibited by the Act.

Id.

183. *See, e.g.*, U.S. Dept. of Justice, Computer Crime and Intellectual Property Section (CCIPS) Economic Espionage Act (EEA) Cases, http://www.usdoj.gov/criminal/cybercrime/eeapub.htm (last visited Apr. 5, 2006) (reporting five months of home detention and a thirty-six month probation for theft of engineering plans by company insider in United States v. Daddonna (D. Conn. Mar. 12, 2002)); *Id.* (reporting that ex-employee received a sentence of twenty-four months probation for the theft of computer source code in United States v. Dai (W.D.N.Y. Aug. 23, 2001); reporting that ex-employee of California software company received sentence of thirty-six months probation for the theft of software design documents in United States v. Morch (N.D. Cal. Mar. 21, 2001); and documenting that outsider received a sentence of sixty months probation for trade secret theft of software in United States v. Corgnati (S.D. Fla.)).

184. *See, e.g.*, Sorojini J. Biswas, The Economic Espionage Act of 1996, http://www.myersbigel.com/ts_articles/trade_secret4.htm (last visited Apr. 5, 2006) (reporting sentence of twelve months and a $60,000 fine in EEA case where insider stole customer information in United States v. Chang (N.D. Cal. Dec. 4, 2001)).

46%).[185] Four EEA perpetrators received sentences of between four and six years (15%).

Fines were imposed in only fourteen out of forty-eight cases. Fines and forfeitures ranged from $200 to $12,000,000. The median fine was $50,000. This data drawn from a decade of EEA prosecutions confirms that the federal statute is a mouse trap, not a bear trap.[186] The data reveals that EEA convictions result in sanctions typically given to other white-collar criminals. An alternative hypothesis is that problems with discovery in a substantive case mean that federal prosecutors frequently default to lesser crimes such as attempt or conspiracy.[187]

The empirical studies confirm that domestic corporate gnats outnumber state-sponsored camels by a large margin in the first decade of EEA prosecutions. The vast majority of the EEA prosecutions has not been the byproduct of proactive investigations but is the product of foiled plans to sell trade secrets to competitors. Most corporate spies caught by federal law enforcement officers were knowledgeable insiders such as employees, ex-employees, and consultants, not foreign spies.

Fewer than twenty-five federal district or appellate cases even mention the EEA in the first decade of prosecutions.[188] Cyberspace is only the newest economic espionage battleground. "At least one 'Trojan horse' program used to steal files from infected computers has been traced to servers in China, providing further evidence that U.S. companies may be targets, say analysts."[189]

Federal law enforcement has focused on domestic trade secret theft instead of espionage sponsored by our allies. In all but a few

185. *See, e.g., id.* (reporting ex-employees' theft of computer source code was punished by a two year sentence in federal prison in United States v. Kissane (S.D. N.Y. Oct. 15, 2002); reporting that insider and ex-employee was punished by a fourteen month sentence for stealing drug delivery system formula in United States v. Rector (M.D. Fla. Jan. 28, 2002); and imposing two year sentence on ex-employee for stealing micro-process or research in United States v. Ow (N.D. Cal. Dec. 11, 2001)).

186. *See* Chris Carr, Jack Morton & Jerry Furniss, *The Economic Espionage Act: Bear Trap or Mousetrap?*, 8 TEX. INTELL. PROP. L.J. 159 (2000).

187. Susan Brenner suggests that lesser sentences in EEA cases may be explained by the tendency of prosecutors to default to lesser EEA offenses such as attempts or conspiracies. In addition, sentences may be reduced because the value of the loss will be non-existent in the case of a failed attempt to steal trade secrets.

188. A LEXIS/NEXIS search of all cases conducted on July 20, 2005 revealed only twenty-three cases in which the term Economic Espionage Act was mentioned.

189. Lever, *supra* note 117.

cases, large multinational U.S. corporations have been victimized by trade secret theft. This trend may partially be explained by the fact that only large companies have the resources to conduct private investigations. The research findings from the first decade of EEA cases confirm that high technology, including software and biomedical industries, are the most common targets for industrial espionage. The next section proposes that the EEA be amended to encourage private attorneys general to bridge the enforcement gap in the present law.

III. REFORMING THE ELECTRONIC ESPIONAGE ACT BY BRINGING IN THE PRIVATE ATTORNEY GENERAL

> Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened.[190]

In this part of the article, I argue that data intermediaries such as software vendors should be secondarily liable for economic espionage when they "'facilitate' the realization of an independently created risk by doing something that they knew or should have known would 'pave the way' for a third party to harm the victim."[191] The software industry will vigorously oppose this expansion of liability, arguing that secondary liability will stifle innovation, punish the wrong entity, and not be feasible because it is impossible to produce bug-free software.[192]

Increasingly, the justification for third-party liability for misappropriation must shift from intentional tort actions to the negligent enablement of trade secret theft.[193] Expanded third-party liability against software providers would help bridge the enforcement gap left by weak EEA enforcement. The most efficient solution to this wrongdoing is the "prevention of crime rather than trying to cope afterwards with the damage it has done."[194] A fence at the top of the

---

190. E.I. DuPont deNemours & Co., Inc. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

191. Aaron Twerski & Anthony J. Sebok, *Liability Without Cause? Further Ruminations on Cause-in-Fact as Applied to Handgun Liability*, 32 CONN. L. REV. 1379, 1383 (2000).

192. Harris Miller, *Penalizing Vendors Brings Consequences*, NETWORK WORLD, Apr. 22, 2002, *available at* http://www.networkworld.com/columnists/2002/0422faceoffno.html.

193. *See, e.g.*, Micro Data Base Sys., Inc. v. Dharma Sys., Inc., 148 F.3d 649, 654 (7th Cir. 1998) (holding "misappropriation of a trade secret is an intentional tort").

194. GRAEME R. NEWMAN & RONALD V. CLARKE, SUPERHIGHWAY ROBBERY: PREVENTING E-COMMERCE CRIME xiv (2003).

cliff is far more efficient than deciding who pays for consequential damages once trade secrets are misappropriated. The software industry is just beginning to recognize the importance of building in security solutions into its products.[195] Despite this promising development, corporate computer networks are presently at great risk. A study by an international accounting found that 83% of the officers at leading financial institutions reported that their computer systems had been compromised within the past year as compared to only 39% in 2003. A 2003 CSS/FBI survey of cybercrime concluded that corporations frequently suffer from the "theft of proprietary information with the average reported loss of $2.7 million per incident."[196] In the law of negligence, the greater the risk the greater the duty and this principle applies equally well to defective software that enables trade secret theft.

The *prima facie* case for the EEA statutory tort of negligent enablement of economic espionage consists of four elements: (1) Software licensors must have owed their licensees a duty to implement adequate security in their products and services;[197] (2) the

---

195. Microsoft, for example, has recently improved the security of its products by building security related updates into the post-marketing period. Microsoft now automatically sends security related updates to users rather than requiring users to download patches. Windows XP automatically checks for fixpacks on the Microsoft Web site, and if it finds them offers to download them gratis to all users. Most software now automatically checks for updates, at least when it is installed if not on a schedule after installation. Windows XP, for example, automatically checks for updates on a regular basis.

196. John B. McCormick, *2003 CS/FBI Survey Cybercrime Survey Shows Reduced Losses*, TECH REPUBLIC, June 23, 2003, http://techrepublic.com.com/5100-6264-5054396.html. Cybercrime may be divided into many categories, including the illegal use of cryptography, stock manipulation, offshore scams, e-mail threats, computer viruses, forged e-mail postings, illegal copying of software, and cyber-terrorism. Daniel P. Schafer, Comment, *Canada's Approach to Jurisdiction over Cybertorts: Braintech v. Kostiuk*, 23 FORDHAM INT'L L.J. 1186, 1190 (2000) (noting cybercrime categories include credit card fraud, unauthorized access to computer systems, child pornography, software piracy, and cyberstalking and acknowledging that new crimes are evolving). The harm caused by cybercrime includes financial injuries, invasion of privacy, compromising of sensitive information, information theft, destruction of trade secrets, meltdown of computer hard drives, or even threats to public health or security. U.S. Dept. of Justice, Computer Crime and Intellectual Property Section, Computer Intrusion Cases, http://www.cybercrime.gov/cccases.html (last visited Apr. 5, 2006). "The San Francisco-based Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad have conducted the CSI/FBI survey annually since 1996." Michael Fickes, *Behind the Numbers: The FBI Cyber-Crime Survey Results*, GOVERNMENT SECURITY, Aug. 1, 2004, http://govtsecurity.com/mag/behind_numbers_fbi/.

197. Whether the duty is based upon products liability, premises liability or a general enabling tort, courts must find a duty before the law will recognize Internet security claims. Next, they must establish that the online intermediary breached that duty and proximately

software licensor must have breached the standard of reasonable computer security either by acts or omissions that created vulnerabilities or that enabled the theft of trade secrets;[198] (3) the trade secret's theft or economic espionage must have been negligently enabled by the software vendor's negligence.[199] In other words, the defective software products or service was both a cause in fact and a proximate cause of the plaintiff's harm;[200] and (4) the software vendor's failure in producing products or services with adequate security must have caused economic losses to the trade secret owner.[201]

---

caused harm to the plaintiff. Any duty to protect computer users from the cybercrimes of third persons must be predicated on a high degree of known, preventable risk.

198. To qualify as a protectible trade secret, the "promise" software, customer list and prospects list: (1) must be information such as a formula, pattern, compilation, program, device, method, technique or process; (2) have independent economic value, available from only one source; and (3) is the subject of reasonable efforts to maintain its secrecy. *See* Leske v. Leske, 539 N.W.2d 719, 721-22 (Wis. Ct. App. 1995). In bricks and mortar tort law, courts frequently turn to custom to determine best practices in a given field. Custom provides the floor, but not necessarily the ceiling, of reasonable care. A threshold question for setting the standard of care for the Internet is to examine whether compliance to custom should be a defense against a negligence claim. In the traditional law of negligence, the greater the risk the greater the likelihood a court will impose a duty of care. Like preventive medicine, the purpose of preventive law is to avoid or reduce the risky conditions leading to negligence liability. Yet, few companies have even a basic understanding of how to protect their computer systems against the known risks of foreign and domestic data theft. A company has a legal duty to develop and maintain a computer system that is available, reliable and protects data from hackers and other intruders.

199. In a negligent enablement of economic espionage case, the corporate victim must present facts and circumstances that will convince a jury that the data theft or trade secret misappropriation that caused plaintiff's injury was foreseeable and that the software vendor or online intermediary was in the best position to reduce the radius of the risk. Foreseeability is the sine qua non of duty. The greater the risk, the greater the duty of care owed software licensees.

200. It may be difficult to determine whether a software bug, security hole, or misconfiguration was a "substantial factor," where the security breach was connected to multiple problems. Courts will grapple with the "cause-in-fact" problem where third party intruders exploit a variety of security holes on numerous different networks in order to harm Internet users. Even if the plaintiff establishes actual cause, there may not be recovery if the causal relationship between the defendant's breach and the plaintiff's losses to cybercrimes are too remote.

> Proximate cause rules are among those rules that seek to determine the appropriate scope of a negligent defendant's liability. The central goal of the proximate cause requirement is to limit the defendant's liability to the kinds of harms he risked by his negligent conduct. . . . The proximate cause issue, in spite of the terminology, is not about causation at all but about the appropriate scope of responsibility.

DANN B. DOBBS, THE LAW OF TORTS 443 (2000).

201. A telecommunications company, for example, could be held liable for providing insecure software enabling a computer hacker to steal trade secrets. Compensatory damages

Software providers should be secondarily liable only if they fail to reasonably secure software through readily available means such as building automatic security updates into their products and services. Providers that do not undertake prompt remedial measures in plugging known security vulnerabilities should be liable for consequential damages in the form of trade secret theft. Similarly, vendors that market products with known vulnerabilities frequently pave the way for state-sponsored economic espionage.[202] Greater secondary liability imposed against the software vendor will result in more secure software that prevents economic espionage. The problem with the Economic Espionage Act is that federal prosecutors are frequently unable to prosecute primary wrongdoers in a cross-border legal environment. Suing the intermediary for failing to prevent the exploitation of known vulnerabilities would largely solve the cross-border enforcement problem.[203]

A. The Impenetrable Jungle of Trade Secrets Law

The muddled state of the Economic Espionage Act lies in part because of the conceptual uncertainty about the nature of trade secrets. The law of trade secrets was prefigured in Roman law, a legal regime that protected slave owners against competitors who

---

may be awarded for lost profits incurred because of trade secret misappropriation. The law of torts also provides for punitive damages to punish and deter software gatekeepers that fail to secure computer software with known vulnerabilities and prior similar misappropriations or data theft.

202. Courts frequently use the concept of proximate cause to limit liability for negligently enabling the crimes of third parties. *See, e.g.*, McCarthy v. Olin Corp., 119 F.3d 148, 169 n.21 (2d Cir. 1997) (Calabresi, J., dissenting) ("In other words, could the defendant be held liable for the criminal acts of an intervener absent any direct relationship with the plaintiff? Historically, a majority of jurisdictions answered this question in the negative, finding either no duty or no proximate cause.").

203. Professor Joseph Bauer notes that my proposal to lengthen the EEA lasso by recognizing private causes of action against primary wrongdoers does not mean we will see better cross-border enforcement if the foreign government is unwilling to enforce civil actions. It is expected that private attorneys general will have even greater difficulty obtaining jurisdiction or enforcing judgments against foreign agents, instrumentalities and governments than the current regime of criminal law enforcement. An American company will not have the means to enforce civil actions against primary wrongdoers when espionage claims are brought against foreign nationals and foreign corporations for conduct taking place abroad. A multilateral treaty would be required to reach conduct beyond the borders of the United States. The private cause of action against the primary wrongdoer will not lead to appreciably more enforcement in the cross-border environment in the absence of an Economic Espionage Convention or specific remedies of extradition for economic espionage be made part of the TRIPS Agreement. The private cause of action for negligent enablement will be against the available intermediary therefore bypassing many of these problems.

induced their slaves to disclose confidential information.[204] It is quite likely that Roman trade secret protection was too different from modern trade secret protection to offer much guidance.[205] Today, the formula for Coca-Cola is perhaps the best known example of a trade secret, having been a closely guarded secret since the company's founding in 1892.212

The current law of trade secrets requires that the "the appropriator must have acquired, disclosed, or used the information in a wrongful manner."[207] The law of trade secrets is the bastard stepchild of the common law that is alternatively classified as a tort, contract, property or even the breach of a confidential relationship. Professor Bone describes trade secrets as an anomalous branch of intellectual property because "it does not impose liability for mere appropriation."[208]

1. Trade Secret Misappropriation as Tort Action

Trade secret misappropriation, whether direct or contributory, is essentially a tort and implies the invasion of some legally protected right of the owner. The common law of trade secrets was first conceptualized as a business tort in the nineteenth century.[209] Since then, trade secret protection has been reconceptualized to provide protection on not only a tort theory, but also on a contract or property theory. Trade secret protection is "one of the last areas of intellectual property that is not covered by a federal statute granting a private right of action to trade secret owners."[210] While the general contours of trade secrets law are governed by state law, federal issues are frequently found in trade secrets litigation.[211]

---

204. A. Arthur Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti*, 30 COLUM. L. REV. 837 (1930); Herbert David Klein, *The Technical Trade Secret Quadrangle: A Survey*, 55 NW. U. L. REV. 437, 437 (1960-1961).

205. Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 244 (1998) (contending that Roman law prefiguring trade secret protection is not comparable to modern trade secret law).

206. Coca-Cola Bottling Co. v. Coca-Cola Co., 269 F. 796, 799 (3d Cir. 1920).

207. Bone, *supra* note 205.

208. *Id.*

209. *Id.* at 245.

210. Beckerman-Rodau, *supra* note 20.

211. *See* Jerry Cohen, Federal Issues in Trade Secret Law, Trade Secret Seminar, Suffolk University Law School Center for Advanced Legal Studies, Co-Sponsored with Boston Patent Law Association, (Mar. 14, 2003) at 29-30 (unpublished paper on file with author) (discussing numerous federal statutes having relevance to trade secret practice including the Federal Employees Trade Secret Act, Government Procurement Regulations, Freedom of Information

The First Restatement of Torts, published in 1939, extracted a relatively clear definition and a set of liability rules from a confusing body of precedent.[212] The Restatement (First) Torts section 757, still followed by important states such as Massachusetts and New York, states that:

> [o]ne who discloses or uses another's trade secret, without a privilege to do so, is liable to another if. . .(c) he learned the secret from a third person with notice of the fact that it was secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of his duty to another.[213]

The Restatement of Torts section 757 comment b (1939) provides the following factors in determining what information is protected as a trade secret:

> An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: the extent to which the information is known outside of his business; the extent to which it is known by employees and others involved in his businesses; the extent of measures taken by him to guard the secrecy of this information; the value of the information to him and to his competitors; the amount of effort or money expended by him in developing the information; the ease or difficulty with which the information could be properly acquired or duplicated by others.[214]

The American Law Institute approved the Restatement (Third) of Unfair Competition in 1995. The Restatement (Third) defines trade

---

Act (FOIA) Trade Secret Exceptions to Sunshine Government and Federal Agencies' Responsibilities and Options re Trade Secrets, Wiretap Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Economic Espionage Act, and the Interstate Transport of Stolen Property Act).

> At the time of the passage of Title I of the Economic Espionage Act of 1996, the only federal statute prohibiting the misappropriation of trade secrets was the Trade Secrets Act, 18 U.S.C. §1905, which was of limited utility because it did not apply to private sector employees and it provided only minor criminal sanctions.

J. Michael Chamblee, *Validity, Construction, and Application of Title I of Economic Espionage Act of 1996*, 177 A.L.R. Fed. 609, 617 (2005) . "The EEA's broad definition of trade secrets represents the first time federal legislation has specifically protected intangible property without additional requirements, such as transmission of such property through the mail or through a wire transmission." Albert, Sanders & Mazzaro, *supra* note 83, at 635.

212. Beckerman-Rodau, *supra* note 20, at 233.

213. RESTATEMENT (FIRST) OF TORTS § 757 (1939).

214. *Id.*

secrets broadly to include "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."[215] The tort of misappropriation requires plaintiffs to prove three elements: (1) the existence of a trade secret, (2) the acquisition of the secret as a result of a confidential relationship, and (3) unauthorized use of the secret.[216]

2. Trade Secret as Breach of Contract or Confidential Relationship

Employers, ex-employees, and other insiders who have breached a nondisclosure agreement, a fiduciary or confidential relationship are the most likely defendants in trade secret cases. As Professor Bone explains, "The relational focus of trade secret's liability rules aligns trade secret law more closely with the law of contract than with the law of property."[217] A growing number of U.S. companies require their employees, consultants, independent contractors, joint venturers, and other insiders to enter into signed nondisclosure agreements (NDAs), an agreement to protect the secrecy of trade secrets and other confidential business information.

A NDA is a contract in which an employee or other person expressly promises to keep a trade secret unless there is express authorization or approval from the owner. Contract is the principal legal device that trade secret owners use to demonstrate that information is secret and to bind employees and others by a confidential relationship or duty. By definition, the wrongdoer is liable for trade secret misappropriation for breach of a duty of confidence, breaching a contractual duty, or otherwise acquiring the information by misrepresentation or outright thievery.[218]

The Uniform Trade Secrets Act (UTSA) is based largely upon a relational theory of contracts and confidential relations defining "improper means" for acquiring trade secrets as encompassing "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other

215. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

216. Lemmon v. Hendrickson, 559 N.W.2d 278, 279 (Iowa 1997); *See also* Hudson Hotels Corp. v. Choice Hotels Int'l, 995 F.2d 1173, 1176 (2d Cir. 1993).

217. Bone, *supra* note 205, at 244.

218. *Id.* at 244.

means."[219]Similarly, UTSA defines misappropriation as using improper means to acquire a trade secret where the protected information was acquired by breaching a duty to maintain secrecy.[220]

The U.S. Supreme Court in *Kewanee Oil Co. v. Bicron Corp.*[221] held that trade secret law was not preempted by patent law and "encourage[s] invention in areas where patent law does not reach."[222] The Court stated that trade secret law contributed to "commercial ethics and the encouragement of invention,"[223] and adumbrated the principle of "good faith and honest, fair dealing [which] is the very life and spirit of the commercial world."[224] The underlying jurisprudence behind trade secret protection is that an owner should have a remedy if the essential element of secrecy is lost due to a breach of confidence by someone obligated to keep information secret.

3. Trade Secrets as Intellectual Property

In *Ruckelshaus v. Monsanto Co.*, the U.S. Supreme Court held that trade secrets were classifiable as property protected under the Takings Clause of the U.S. Constitution.[225] In *Ruckelshaus*, Monsanto filed suit claiming that data disclosures about its insecticides to the Environment Protection Agency amounted to a taking without just compensation by the Environment Protection

---

219. UNIF. TRADE SECRETS ACT § 1(1) (amended 1985).

220.

> Misappropriation means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
>
> (A) used improper means to acquire knowledge of the trade secret; or
>
> (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his position, knew or had reason to know that it was a trade secret ad that knowledge of it had been acquired by accident or mistake.

Id. § 1(2).

221. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

222. *Id.* at 485.

223. *Id.* at 481.

224. *Id.*

225. Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).

Agency. The Federal Environmental Pesticide Control Act of 1972 contained a provision for mandatory public disclosure of information learned through the EPA's pesticide-registration procedure.[226] The 1972 Amendments "did not specify standards for the designation of submitted data as 'trade secrets or commercial or financial information.'"[227]

Monsanto was one of a handful of companies that invented and developed "new active ingredients for pesticides and conduct most of the research and testing with respect to those ingredients."[228] The Court had little difficulty holding that trade secrets were protected by the Takings Clause of the United States Constitution as well as by Missouri's takings clause.[229] Richard Epstein views the *Monsanto* case as the linchpin for his argument that trade secrets are property.[230] Professor Epstein sees much common ground between trade secrets and the other branches of intellectual property law:

> [T]he logic for protecting trade secrets parallels that for protecting patents and copyrights. People will not develop certain forms of information at private cost if the benefits of that information can be immediately socialized by the unilateral actions of others. Patents grant the right to exclude only to individuals who disclose their information. This disclosure can, especially with processes and know-how, undermine its value to the owner because of his inability to monitor its use by others. So long as a product may be made in multiple ways, the owner cannot learn of the misappropriation of his invention from the mere appearance of that product on the market. Trade secrets offer both an alternative to patent protection for inventions, and an exclusive source of protection for matters as diverse as know-how, recipes, and customer lists.[231]

Richard Epstein acknowledges one major difference between trade secrets and other intellectual property. Once a trade secret is disclosed to the public, the value of the intellectual property evaporates.[232] The unprotected disclosure of a trade secret will cause

---

226. *Id.* at 992.

227. *Id.* at 993.

228. *Id.* at 997.

229. *Id.* at 1003-04.

230. Richard A. Epstein, *The Constitutional Protection of Trade Secrets Under the Takings Clause*, 71 U. CHI. L. REV. 57, 61 (2004).

231. *Id.* at 57.

232. *Id.*

the information to forfeit its trade secret status, since "[i]nformation that is generally known or readily ascertainable through proper means by others . . . is not protectible as a trade secret."[233] Once trade secrets are made public they may not be rescued, which is not true of any other branch of intellectual property law. Other scholars question the classification of trade secrets as property:

> In trade secrecy law, as in the information privacy law contemplated in this article, there is no need to say that a property right exists in the protected information. Although courts have sometimes loosely referred to trade secrets as the "property" of the firm that licensed them and have on occasion held trade secrets to be property for certain purposes, the more appropriate way to characterize the firm's interest in a trade secret is to say that the law protects the firm against breaches of contracts and confidential understandings.[234]

One of the basic attributes of property is the right of possession. Trade secrets are the one branch of intellectual property law where rights may be granted to the owner even if he or she has no exclusive rights of possession. The owners of a copyright, trademark, or patent have exclusive rights, whereas trade secrets may be shared because of the right of reverse engineering. As the drafters of the Uniform Trade Secret Act observe:

> Under both the Act and common law principles, for example, more than one person can be entitled to trade secret protection with respect to the same information, and analysis involving the "reverse engineering" of a lawfully obtained product in order to discover a trade secret is permissible.[235]

Finally, trade secrets are private and by definition kept from the public view so there is not the same exchange of a limited monopoly to advance science or public knowledge. The public interest is advanced in every branch of intellectual property save trade secrets. Trade secrets are unlike other intellectual property in that there is no engineered consensus as to whether protection should be classified as a branch of the law of torts, contracts, intellectual property, or whether the action should be for breach of fiduciary duty or an implied covenant of good faith and dealing.

---

233. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

234. Pamela Samuelson, *Cyberspace and Privacy: A New Legal Paradigm? Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1153 (2000).

235. UNIF. TRADE SECRETS ACT, Prefatory Note (amended 1985).

B. Third-Party Liability for Misappropriation

As the last section demonstrates, trade secrets lack the conceptual cohesiveness of other branches of intellectual property law. This section hypothesizes the reasons why secondary liability has been so late to develop in trade secrets law whereas the doctrine is well developed in every other branch of intellectual property law.[236] In the formative era of the software industry, the law of trade secrets was the preferred means to protect code because of the uncertainty whether copyright or patent protection were available. Yet, no case law ever developed making a software producer liable for enabling or inducing trade secret theft. The next subsection briefly summarizes the developed nature of secondary liability in patent and copyright law in contrast to the undeveloped secondary liability doctrine in the law of trade secrets.

1. Secondary Liability in Patent Law

Direct infringement of copyrights, patents, and trademarks is a strict liability offense with no requirement of proving the infringer's state of mind, while trade secret misappropriation is often conceptualized as an intentional business tort.[237] In contrast, contributory infringement often centers on a negligence-like standard of knowledge of infringement as well as proof of direct infringement in every branch of intellectual property law except trade secrets. Under patent law, for example, contributory infringement has been codified to apply to sellers who incorporate "a component . . . constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in a [direct]

236. Robert Bone made this point in a conversation we had just prior to the Santa Clara University School of Law Conference on Third-Party Liability in Intellectual Property Law, Oct. 7, 2005. Professor Bone also made this argument in his commentary on my paper presented at the Symposium. Professor Bone contends that trade secret is the only branch of intellectual property law without a strong secondary liability tradition. *See, e.g.*, Inwood Lab., Inc. v. Ives Lab., Inc., 456 U.S. 844, 854 (1982) (holding that secondary trademark liability may be imposed "if a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement") (trademarks); Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005) (expanding the theory of contributory liability to encompass inducement theory in addition to contributory and vicarious infringement) (copyright law); and 35 U.S.C. § 271 (incorporating contributory infringement into the 1952 Patent Act).

237. *See, e.g.*, New York Scaffolding Co. v. Whitney, 224 F. 452, 459 (8th Cir. 1915) ("One who makes and sells articles which are only adapted to be used in a patented combination will be presumed to intend the natural consequences of his acts. . . .") (cited in 5 DONALD S. CHISUM, CHISUM ON PATENTS § 17.02[1] (2005)).

infringement of such patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use . . . ."[238] The doctrine of contributory infringement in patent law originated from the law of torts, not intellectual property.[239]

Lower court decisions frequently applied the tort theory of aiding and abetting to hold sellers liable for marketing unpatented components with no purpose but to be part of an infringing combination. The statutory law of contributory infringement was prefigured in the 1871 case of *Wallace v. Holmes*,[240] where for the first time in Anglo-American legal history, a court held a seller liable for supplying an unpatented component of a product with no use except in an infringing combination.[241] The court traces the path of secondary liability in patent law to also include sellers whose products had innocent as well as infringing uses but where "the defendant actively encouraged or induced direct infringement."[242]

The contributory infringement doctrine was incorporated into the Patent Act in 1952 when "Congress enacted Sections 271(b), 271(c), and 271(d) in order to clarify and stabilize the law of contributory infringement."[243] Charles Adams' historical survey of third-party liability in patent law confirms that most contributory infringement cases in patents center on a defendant's knowledge as well as acts inducing infringement. While there is no requirement that the plaintiff prove intent to induce infringement, litigation often centers "on a variety of promotional activities including advertising infringing uses of the defendant's products, . . . and explaining how the defendant's products may be used to infringe a patent."[244]

2. Secondary Copyright Liability

Contributory infringement is established where the defendant "with knowledge of the infringing activity, induces, causes, or

238. 35 U.S.C. § 271(c) (2000).

239. Alfred P. Ewert & Irah H. Donner, *Will the New Information Superhighway Create 'Super' Problems for Software Engineers? Contributory Infringement of Patented or Copyrighted Software-Related Applications?*, 4 ALB. L.J. SCI. & TECH. 155, 164 (1994).

240. Wallace v. Holmes, 29 F. Cas. 74 (C.C.D. Conn. 1871) (No. 17,100).

241. 5 DONALD S. CHISUM, CHISUM ON PATENTS § 17.02[1] (2005).

242. *Id.*

243. *Id.*

244. Charles W. Adams, *A Brief History of Indirect Liability for Patent Infringement*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 369, 389 (2006).

materially contributes to the infringing conduct of another."[245] The elements of contributory infringement are knowledge of the primary wrongdoers' infringing activity,[246] and a showing that the third-party secondary infringer induced, caused, or materially contributed to the infringing activity.[247] In *Fonovisa, Inc. v. Cherry Auction, Inc.*, the operators of a swap meet allowed vendors to sell counterfeit Latin/Hispanic music recordings, which violated the plaintiff's copyrights and trademarks.[248] The plaintiff sued the Cherry Auction swap meet alleging copyright infringement, contributory and vicarious copyright infringement, as well as contributory trademark infringement.[249]

The appeals court observed that there simply was no question about whether the Cherry Auction and its operators knew of infringing activities because the swap meet had been the target of a raid seizing more than 38,000 counterfeit recordings in a 1991 raid.[250] The Ninth Circuit found that Cherry Auction had the "formal, contractual ability to control the direct infringer" which was a necessary element of vicarious liability.[251] The court had little difficulty finding vicarious copyright liability because of Cherry Auction and its operators "pervasive participation in the formation and direction" of the direct infringers, including promoting them (i.e., creating an audience for them).[252] The Ninth Circuit also found contributory copyright infringement to be easily established since the swap meet operators knowingly contributed to the infringement by providing the site for the activity. Finally, the court held that contributory trademark infringement existed because defendants were "willfully blind" to the ongoing infringement.[253]

---

245. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); *See, e.g.*, Playboy Enter., Inc. v. Webbworld, 968 F. Supp. 1171 (N.D. 1997), *aff'd*, 168 F.3d 486 (5th Cir. 1999) (finding the defendant liable for direct as well as secondary copyright liability).

246. To prevail on a contributory or vicarious copyright claim, a plaintiff must show direct infringement by a third party. UMG Records, Inc. v. MP3.Com Inc., 2000 U.S. Dist. LEXIS 13293 (S.D.N.Y. Sept. 6, 2000) (concluding that MP3.com was a willful infringer imposing statutory damages of 25,000 for each copyrighted compact disc in the defendant's online database).

247. *See Gershwin Publ'g*, 443 F.2d at 1162.

248. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261 (9th Cir. 1996).

249. *Id.*

250. *Id.*

251. *Id.* at 263.

252. *Id.*

253. *Id.* at 265.

In the recent Grokster case, The Supreme Court has taken secondary liability one step further, expanding upon an inducement of infringement theory first articulated in the patent law cases.[254] In *Grokster*, the Court expanded the doctrine of contributory infringement to include a theory of inducement imported from patent law, holding that Grokster and Streamcast's statements or actions directed to promoting infringement could trigger liability for contributory infringement.[255]

3. The Poverty of Third-Party Liability in the Law of Trade Secrets

Third-party liability for trade secret misappropriation is rarely imposed, though it may be possible to impose liability on the recipients of unauthorized trade secret transfers if it can be proven that these persons "knew or had reason to know that they are the recipients of unauthorized trade secret information."[256] Third-party liability is a critical component of trade secrets law because third parties are often the only ones with "deep pockets" for the recovery of damages for trade secret violations. Trade secrets law is unlike any other branch of intellectual property because of its dearth of secondary liability rules.[257] There is little by way of commentary on why secondary liability has been so slow to develop for trade secrets.

Software code, for example, may contributorily infringe a patent, but there is no secondary liability imposed when a software provider paves the way or facilitates for trade secret misappropriation.[258] Secondary liability for trade secret misappropriation is well established in the rare case in which there is proof that an employee was induced to transfer trade secrets from his former employer to his

---

254. In this section, I draw upon Jay Dratler's superb presentation at this symposium. For an illuminating discussion of the ways in which the court drew upon patent law to construct a theory of contributory infringement in copyright, see Jay Dratler, Jr., *Common-Sense (Federal) Common Law Adrift in a Statutory Sea, or Why Grokster was a Unanimous Decision*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 413 (2006).

255. Metro-Goldwyn-Meyer Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005).

256. R. Mark Halligan, *Third-Party Liability for Trade Secret Misappropriation*, http://my.execpc.com/~mhallign/3party.html (last visited Apr. 6, 2006).

257. This point was brought home to me in a discussion I had with Professors Robert Bone and Joseph Bauer at a breakfast meeting the day of the Santa Clara Conference on Third-Party Liability in Intellectual Property Law.

258. "Under the present law, new software created by a software architect may contributorily infringe a patent that does not even mention software." Ewert & Donner, *supra* note 239, at 158.

current employer. This form of indirect or secondary liability is frequently predicated upon intentional business torts, which have only a tangential connection to the concept of intellectual property.[259] Injunctions are frequently used to enforce nondisclosure agreements or covenants not to compete because legal remedies for breach of contract are inadequate. Third-party liability centers on contract and tort, not intellectual property. The central issue in these cases is whether a contractual or quasi-tort confidential duty has been breached.[260]

Currently, no court has extended secondary liability to negligence making third parties accountable for negligently enabling liability for third-party misappropriation, even where the vendor was willfully blind to known defects. The next section argues that Congress needs to reform the Economic Espionage Act to recognize a negligent enablement cause of action. Imposing greater liability on the software industry for marketing products known to enable cybercrime will only impact economic espionage cases where access to computers is gained due to a software defect. As in other areas of secondary liability, federal common law standards will evolve to set standards for the storage or transmission of trade secrets on computer systems.[261]

C. Why Trade Secrets Must be Federalized

Trade secrets law is an island of predominately state law in an increasingly federalized body of intellectual property law. Small and medium-sized companies that are victimized by trade secret misappropriation currently have no recourse even if they can identify the primary wrongdoer. Private civil enforcement is the norm in the law of copyrights where the victims of infringement have banded together to form private policing. The U.S. Software and Information Industry Association formed private policing to punish and deter

259. Secondary liability is statutorily conferred by the Patent Act of 1952, which expressly provides for liability for active inducement and contributory infringement. *See* 35 U.S.C. § 271. *See generally*, Charles W. Adams, *A Brief History of Indirect Liability for Patent Infringement*, Symposium Issue, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 369 (2006). The Supreme Court has borrowed from patent law in extending secondary liability to copyright. *See generally* Dratler, Jr., *supra* note 254.

260. Mixing Equip. Co. v. Philadelphia Gear, Inc., 312 F. Supp. 1269 (E.D. Pa. 1970) (preliminarily enjoining the competitor from employing the former employee, or from obtaining the designer's trade secrets from the former employee).

261. *See generally* Dratler, Jr., *supra* note 254.

copyright infringement both here and abroad. Even so, an estimated "$7.5 billion worth of American software is illegally copied and distributed annually."[262] Congress provided for a private attorney general role for the victims of unfair competition and trademark dilution when it enacted the 1946 Lanham Act. The Lanham Act gives trademark owners standing to file suit against infringers for unfair and deceptive trade practices in federal courts. The Lanham Act arms private litigants with tort-like consumer remedies, including a remedy for statutory multiple damages to rectify unfair commercial practices.[263]

Trade secrets are the province of state law whereas patent law and copyrights are purely federal branches of intellectual property law. The law of trademarks is hydra-headed with both state and federal rights and remedies. While the general contours of trade secrets law are governed by state law, federal issues are frequently found in trade secrets litigation.[264]

Arming private attorneys general with a negligent enablement tort action will give small and medium firms the possibility of collecting consequential damages as well as punitive damages against intermediaries who enable cyberthefts of trade secrets.

One of the policy alternatives would be to relegate all private enforcement to state causes of action. After all, forty-five states have already enacted some version of The Uniform Trade Secrets Act that codified the basic principles of the common law tort of misappropriation.[265] The model act, for example, defines a trade secret to mean:

---

262. Rustad, *supra* note 19, at 101.

263.

> Any person who . . . uses in commerce . . . any false designation of origin, false or misleading description of fact, or false of misleading representation of fact . . . shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

15 U.S.C. § 1125(a) (2000).

264. *See* sources cited *supra* note 211.

265. Arkansas, California, Connecticut, Indiana, Louisiana, Rhode Island and Washington adopted the original 1979 version of the UTSA. Another thirty-eight states have adopted the 1985 amended UTSA: Alabama. Alaska Arizona, Colorado, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Ohio, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, West Virginia and Wisconsin. *See* Uniform Law Commissioners, A Few Facts about the Uniform Trade Secrets Act,

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[266]

The Uniform Trade Secret Act (UTSA) is a lot less uniform than its title suggests. Table Five lists Massachusetts and New York as economic espionage hot spots and neither state has adopted UTSA. These states are among the handful of states that continue to follow the First Restatement's approach to the tort of misappropriation. Further, there is far less uniformity than one might expect among the states adopting UTSA because of different interpretations in state courts as well as non-uniform amendments. The Georgia Supreme Court, for instance, continues to make a distinction between "head knowledge" and "trade secrets" despite the fact that this distinction is not part of the UTSA.[267] Similarly, the Seventh Circuit applying Illinois law incorporates that doctrine into Illinois' version of the UTSA.[268]

In contrast, the Arkansas Supreme Court no longer distinguishes between head knowledge and written customer information after adopting the UTSA.[269] Non-uniformity among the states will be an even greater problem when private litigants file civil actions against foreign actors or instrumentalities alleging economic espionage. Federal courts are far more experienced when dealing with cross-border issues such as comity, international jurisdiction, and enforcement of judgments. Federal courts are also more qualified in adjudicating cases involving complex intellectual property issues than are state courts.

Trade secret protection remains the only branch of intellectual property without a federal private attorneys general role.[270] Arming

---

http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-utsa.asp (last visited Apr. 6, 2006). *See also* UNIF. TRADE SECRETS ACT (amended 1985), 14 U.L.A. 177 (West Supp. 2004).

266. UNIF. TRADE SECRETS ACT § 1(4) (amended 1985).

267. Randall Scott Hetrick, *Employee "Head Knowledge" and the Alabama Trade Secrets Act*, 47 ALA. L. REV. 513, 522 (1996).

268. *Id.*

269. *Id.* at 523.

270. *See* Beckerman-Rodau, *supra* note 20, at 233 n.34.

private litigants with a federal remedy for economic espionage against the software providers that induce or pave the way for misappropriation brings common sense to the common law by supplementing lax public enforcement with private enforcement by largely corporate victims.

D. The Federal Civil Action for Negligent Enablement

To date, no court has extended the misappropriation tort to make third parties accountable for negligently enabling third-party spies. The federal negligent enablement cause of action will draw in large part upon the common law. As a threshold matter, a litigant will need to prove that they suffered consequential damages from defective software in the form of loss of a trade secret. Corporate and individual victims of trade secret will need to prove three elements: (1) the existence of a trade secret, (2) the acquisition of the secret as a result of a confidential relationship, and (3) unauthorized use of the secret.[271]

To qualify as a trade secret: (1) the information must be neither generally known nor readily ascertainable; (2) the information must derive independent economic value from secrecy; and (3) the plaintiff must make reasonable efforts to maintain secrecy.[272] The additional element will be that a software defect was a substantial factor in enabling the theft of a trade secret. The EEA private cause of action for negligent enablement would base its standard of care on common-law processes because abstract statutory standards would be difficult to draft in an era of rapidly changing technologies.[273] It is likely that industry custom, the Learned Hand risk/utility test, and professional standards of care would evolve to apply in computer security cases.[274] Courts are experienced in determining standards of care in finding

271. Lemmon v. Hendrickson, 559 N.W.2d 278, 279 (Iowa 1997); *See also* Hudson Hotels Corp. v. Choice Hotels Int'l, 995 F.2d 1173, 1176 (2d Cir. 1993).

272. 18 U.S.C. § 1839(3)(A) (2005); *See also* Widmark v. Northrup King Co., 530 N.W.2d 588, 592 (Minn. Ct. App. 1995).

273. Jay Dratler argues that the common-law approach is more likely to evolve to meet changes in technology than drafting cumbersome statutory standards of care. *See* Dratler, Jr., *supra* note 254.

274. The type and degree of Internet security required will depend upon the industry. Financial institutions will calibrate their Internet security to minimize risks such as internal corruption, illegal money laundering, hackers and the attempts of Internet competitors to steal confidential customer information. Universities have a statutory duty to protect the personal information of their students. Companies in general will have a duty to minimize the known risks of identity theft, impostor web sites, viruses, data destruction and the invasion of privacy.

whether a trade secret owner used reasonable means to protect its trade secrets. It is a closely related question whether the software provider supplied reasonably secure software to protect those secrets. As computer security is ratcheted upwards, it is likely that statutory standards of care will be prescribed in specific industries.

The extent of computer security measures taken by the owner of the trade secret need not be absolute, but must be reasonable under the circumstances.[275] Trade secret protection is predicated upon reasonable measures to protect the confidentiality of information, rather than the standard of all available measures irrespective of cost or effort.[276] Foreseeability in federal trade secret misappropriation cases could be established by the "prior similars" test, which is frequently used in premises liability litigation. Under this approach, foreseeability is established by evidence of prior security breaches leading to economic or industrial espionage. Courts would have the most flexibility in choosing either a "totality of the circumstances" or a "balancing" test.[277] A court using either of these approaches could look at all of the relevant circumstances including number, nature, and location of prior data misappropriations. The drawback with this mechanical methodology is that it can lead to subjective outcomes regarding either the number or degree of similarity in cybercrimes.

Courts might examine all of the relevant circumstances including number, nature, and location of prior instances of domestic or foreign spying to determine whether a third party should fortify computer security. A financial institution could, for instance, have a secondary tort action against a software vendor whose products did not implement security precautions meeting industry standards.

In the final analysis, the recognition of new tort duties is a policy-based determination. The judiciary will need to balance such factors as the foreseeability of the harm of computer intrusions or other breaches of security, the degree of certainty between software vulnerabilities and harm, the closeness of the connection between lax Internet security practices and the injury suffered by a computer user; the policy of preventing future intrusions; the burden on the

275. *See, e.g.*, Pioneer Hi-Bred Int'l v. Holden Found. Seeds, 35 F.3d 1226, 1236 (8th Cir. 1994) (describing steps taken by plaintiff to safeguard genetic messages of its genetically engineered corn).

276. E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970) (holding that a plaintiff had no obligation to enclose its unfinished factory to prevent a competitor's use of aerial photographs to unveil secret).

277. *Id.* at 1017 (describing these approaches).

information industry and the consequences to the community of imposing a duty to maintain adequate security; and the availability, costs and prevalence of security solutions as well as insurance.[278]

The vendors of computer software and networks are frequently in the best position to develop products and services with built-in computer security to protect trade secrets. Imposing a duty to implement reasonable security in Internet infrastructure will significantly reduce the radius of the espionage danger.[279] Software licensors are also in the best position to test their product and remediate bugs and holes in the post-marketing period.[280]

Software vendors that market products with known vulnerabilities and online intermediaries who do not implement adequate security foreseeably enable cybercriminals to intercept data and misappropriate trade secrets. An indeterminate number of computer intrusions are caused by known security vulnerabilities that aid or abet unauthorized computer intrusions.[281] The public policy

---

278. These factors are drawn from Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968).

279.

> History has shown that proactive companies that follow a handful of essential security practices will fare better against malicious code exploits. These controls include protections such as file attachment filtering; specific configuration for routers, email clients, email servers, Web browsers, and business applications that are generally easy to implement, require infrequent updates, and go unnoticed by the average user because of their transparency.

Press Release, TruSecure, Malicious Code Problem Continues to Worsen, According to 9th Annual ICSA Labs Virus Prevalence Survey (Mar. 22, 2004), http://www.trusecure.com/company/press/pr_20040322.shtml (on file with the Santa Clara Computer & High Technology Law Journal). In many cases, an online intermediary such as a website is in the least cost avoider in the best position to thwart hackers and other wrongdoers by implementing cost-effective security measures.

280. There would be no need for a defense of contributory negligence because a trade secret owner's own negligence would preclude a lawsuit against a third party for negligent enablement of trade secret misappropriation or economic espionage. Security breaches in many cases are not due to third party hackers but to inadequate security precautions being taken by software users. Many of these precautions are neither expensive nor difficult to undertake. No action for negligent enablement should be available for trade secret owners that fail to implement reasonable security. Negligent enablement claims against software licensors would not be cognizable where trade secret theft is by insiders since they are not misappropriating data because of a defect in software. Typically, such insiders have access to the electronic systems so they gain and steal data via their legitimate access, not due to exploiting security flaws in software.

281. The term, "defective software" encompasses software that fails to produce an accurate result when used according to instructions, or that fails to conform to contract specifications in some other manner. Failure is interpreted broadly, to encompass not only "incorrect" results, but also such matters as the absence of promised features, or the tendency to crash in use. David Polin, *Proof of Manufacturer's Liability for Defective Software*, 68 AM. JUR. 3D *Proof of Facts*

reason for imposing secondary liability on software publishers is to raise the level of Internet or computer security and reduce the level of economic or industrial espionage.[282]

The empirical findings in Part Two of this article demonstrate that software and the computer industry are primary targets for trade secret theft. Defectively designed software and computer networks enable trade secret theft, however federal law enforcement has yet to detect—let alone punish—such wrongdoing.[283] The 2001 CSI/FBI Computer Crime and Security Survey found the Internet connection to be the point of attack in 70% of computer intrusions.[284] One in four "Internet application service providers (ASPs) were found to have substandard protection against security breaches and viruses."[285] "CGI scripts are a major source of security holes. Although the CGI (Common Gateway Interface) protocol is not inherently insecure, CGI scripts must be written with just as much care as the server itself."[286] The availability of properly configured technologies to prevent cybercrime is a key factor in assessing the adequacy of existing safeguards.[287] The imposition of secondary liability for trade secret misappropriation is a necessary incentive to raise the level of computer security in the industry.

---

333 § 1 (2002). Courts have been unreceptive to aiding and abetting claims based on secondary liability. Lawsuits against Visa and MasterCard for aiding and abetting the users of Napster and Grokster were dismissed. *See, e.g.*, Perfect 10, Inc. v. Visa Int'l. Serv. Ass'n, No. C 04-00371 JW, 2004 U.S. Dist. LEXIS 27477 (N.D. Cal. Dec. 3, 2004) and Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077 (C.D. Cal. 2004); *see also* Cohen, *supra* note 211.

282. The Ninth Circuit ruled the software vendors were protected from secondary liability claims even if they knew that the service was primarily used to download copyrighted materials. Metro-Goldwyn-Meyer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004) (ruling that peer-to-peer file sharing software was capable of substantial non-infringing uses and therefore distribution of the software was protected by fair use).

283. Defectively designed software is a widespread problem. Apart from security problems, software may have design defects that cause problems with formatting, processing speeds, the amount of data that could be handled, and problem of system integration with other software components or users. Michael L. Rustad, *Making UCITA More Consumer-Friendly*, 18 J. MARSHALL J. COMPUTER & INFO. L. 547, 573 (1999) (citing survey of computer cases regarding bad software conducted by Michael Rustad and Cynthia Anthony).

284. Richard Power, *2001 CSI/FBI Computer Crime & Security Survey*, COMPUTER SECURITY ISSUES & TRENDS (Computer Security Inst., San Francisco, CA), Spring 2001, at 8.

285. *Many ASPs Have Substandard Protection against Security Breaches—IDC*, AFX, Mar. 8, 2002 (citing worldwide "survey of 50 ASPS finding that 25% lacked fundamentals such as user authentication, virus protection, network security and firewall services").

286. World Wide Web Consortium, World Wide Web Security FAQ, http://www.w3.org/Security/faq/wwwsf1.html#GEN-Q5 (last visited Apr. 6, 2006.

287. The negligent enablement tort does not address the problem of trade secret theft by insiders who exploit trust and access rather than vulnerabilities in software.

E. Bringing in the Private Attorney General

One way to stem the tide of trade secret theft would be for Congress to permit the victims to sue software vendors and other intermediaries for the negligent enablement of cybercrime. One approach would be to hold software manufacturers liable for negligent design of their products or processes that enable foreign and domestic spies to exploit known vulnerabilities, bugs, or holes in software products and services.[288] One of the great weaknesses of the EEA is that it under-deters corporate spies. At present, there is a low probability of detection and an even lower probability of punishment. The criminal side of the law is more difficult to prove because of the elevated standard of beyond a reasonable doubt:

> The EEA is a criminal statute; thus the burden of proof is on the government and each element of every offense must be established beyond a reasonable doubt. This may prove to be a difficult burden to shoulder, especially in satisfying the proof of the requisite intent (i.e., the intent to injure the owner of the trade secret, or the knowing theft of a trade secret). The existence of the criminal remedy may also complicate civil litigation involving trade secret misappropriation. Witnesses in the civil action may refuse to answer questions by asserting their Fifth Amendment right against self-incrimination.[289]

A private statutory cause of action would give the corporate victims of attempted and completed trade secret misappropriation standing in federal court to seek equitable and monetary damages. A federal court will be able to order injunctive relief if it finds that:

---

288. This article addresses the single question of whether software vendors or other intermediaries should be liable for negligence in the production or servicing of their software and security-related services enabling trade secret theft.

> Three theories of liability exist when software is implicated as a possible accident cause: (1) strict liability, (2) breach of warranty, and (3) negligence. Strict liability looks at a product itself and determines whether liability should be assessed against a manufacturer by one who is not in privity with the manufacturer. Warranty concerns the representations by the manufacturer as to a product's capabilities. Negligence looks at the acts of the manufacturer and determines if it exercised ordinary care in the design and production of the product.

R.L. Mays, *Patent No. 6,035,321— Opening the Door to Software Product Liability Exposure*, 6 STAN. J.L. BUS. & FIN. 197, 199 (2001).

289. Sorojini J. Biswas, The Economic Espionage Act of 1996, http://www.myersbigel.com/ts_articles/trade_secret4.htm (last visited Apr. 6, 2006).

> (1) [A] moving party will suffer irreparable injury if the relief is denied; (2) a moving party will probably prevail on the merits; (3) the balance of potential harm favors a moving party; and (4) the public interest favors granting relief. To obtain preliminary injunctive relief in the alternative, a movant must demonstrate either a likelihood of success on the merits and the possibility of irreparable injury, or that serious questions going to the merits raised or the balance of hardships tips sharply in its favor.[290]

Congress has already armed private citizens with federal causes of action in nearly every conceivable regulatory regime from federal environmental and consumer protection to the Sherman Anti-Trust Act and the Federal Trade Commission Act. "In the field of toxic torts, the government relies on private litigants to enforce certain environmental statutes."[291]

A private civil action is already widely available under state trade secret law since most states have adopted the Uniform Trade Secrets Act. However, it will be more efficient to avoid parallel civil proceedings in state courts. If the EEA was amended to include a private cause of action, small or medium-sized companies might then have the incentive to incur the expense of funding private investigators to prove the theft or attempted or completed theft of trade secrets.[292] The federal cause of action should incorporate the robust remedies of the Uniform Trade Secrets Act. Victimized companies would be able to underwrite the cost of tracking foreign governments or agents conducting espionage with the proceeds from uncapped tort awards. Private enforcement of the EEA would help fulfill the public law enforcement gap in this area. By encouraging plaintiffs to serve as private attorneys general, punitive damages fulfill their most critical latent function as they vindicate the larger societal interest by bridging the enforcement gap and increasing both

290. This is the standard for ordering injunctive relief under the Computer Fraud and Abuse Act. *See*, Pac. Aero. & Elecs. Inc. v. Taylor, 295 F. Supp. 2d 1188, 1198 (E.D. Wash. 2003).

291. Rustad, *supra* note 19, at 103. *See also* Robert F. Blomquist, *Rethinking the Citizen as Prosecutor Model of Environmental Enforcement under the Clean Water Act: Some Overlooked Problems of Outcome-Independent Value*, 22 GA. L. REV. 337, 367 (1988) (noting that Congress enlisted citizens to supplement the work of the Environmental Protection Agency).

292. *See* Wangen v. Ford Motor Co., 294 N.W.2d 437, 454 (Wis. 1980) (discussing role of private attorney general in punitive damages in products liability litigation setting).

punishment and deterrence.[293] A private cause of action for misappropriation may result in hundreds of millions of dollars in punitive damages.[294]

The mobilization of private attorneys general to supplement public enforcement is a proactive approach to identifying, locating, and apprehending foreign and domestic industrial spies.[295] The private attorney general can also serve as a "powerful engine of public policy" because of its responsiveness to social problems.[296] Private attorneys general use private enforcement to advance the public interest in an efficient manner that is responsive to market forces.[297] Federal law enforcement resources are not adequate to shoulder the complete load of punishing and deterring corporate espionage.[298]

F. Breach in Third Party Trade Secret Enablement Cases

Courts must first recognize that a software vendor, Internet service provider, or other data handler owes a duty to protect the trade secrets of the plaintiff. Some in the software industry already recognize that software vendors and developers need to be accountable, if not liable, for gross negligence in enabling security threats. In the November issue of *PC World* magazine, Whitfield Diffie, chief security officer of Sun Microsystems, is quoted as saying, "Developers need to stop expecting users to police

---

293. David G. Owen, *Punitive Damages in Products Liability Litigation*, 74 MICH. L. REV. 1257, 1287-88 (1976) (noting how the possibility of punitive damages creates greater incentives for private lawsuits for a public purpose).

294. *See, e.g.*, Mangren Research and Dev. Corp. v. Nat'l Chemical Co., 87 F.3d 937 (7th Cir. 1996) (affirming a jury verdict awarding Mangren $252,684.69 in compensatory damages and $505,369.38 in exemplary damages as well attorney's fees and costs in a trade secret misappropriation lawsuit where malicious and willful misappropriation was proven).

295. Professors Brenner and Crescenzi point to the danger of relying upon "traditional solutions in a non-traditional era; reacting to completed acts of economic espionage by sanctioning the perpetrator(s) is an effective strategy only if they can be identified, located and apprehended." Brenner & Crescenzi, *supra* note 100, at 3.

296. Jeremy A. Rabkin, *The Secret Life of the Private Attorney General*, 61 LAW & CONTEMP. PROBS. 179, 179 (1998).

297. *See* WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 160-61 (1987).

298. "As of 1996, at least twenty-four states had criminal statutes directed at the theft of trade secrets.... Yet the states often lacked sufficient resources to pursue espionage prosecutions." United States v. Hsu, 155 F.3d 189, 195 (3d Cir. 1998) (quoting James H. A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 186 (1977)).

themselves, and take responsibility for the users' safety."[299] The co-creator of the Mozilla Firefox Internet browser makes a similar point:

> The security community needs to provide information and incentive to change behavior. This means education for users, developers, and organizations doing business on the Internet; attribution and penalties for criminal activities; and accountability for unsafe software, unprotected systems, and insecure handling of sensitive information.[300]

Once a duty has been established, the particular standard of care must be calibrated or set. In general, an Internet gatekeeper would breach its standard of care if it created an unreasonable risk that trade secrets would be intercepted. The statutory tort action would only apply if a third party has failed to take reasonable precautions for protecting trade secrets.[301]

No reliable data exists on basic facts such as the number of attacks by hackers or financial losses due to the misappropriation of trade secrets. Similarly, not much data is available on the probability of harm, severity of harm, or the cost of instituting precautions to protect the integrity of online commercial transactions. Efficiency, however, is the starting point for establishing what "ought to be done" to eliminate known vulnerabilities that place the corporate crown jewels at risk.

The World Wide Web, for instance, has morphed into an ideal venue for the misappropriation of trade secrets because of defective software, insufficient Internet security and other computer-based vulnerabilities allowing data theft without a significant probability of detection. Cybercriminals misappropriate trade secrets by intercepting data by bypassing firewalls, altering e-mail headers, or obtaining elevated privileges on computer networks by subterfuge.

The corporate victims of economic espionage and industrial spying need a private cause of action giving them standing in federal court to redress domestic and foreign trade secret theft. A second reform would be to recognize an EEA cause of action for the negligent enablement of trade secret theft. This secondary liability

---

299. Bruce Sterling, *Is The Net Doomed?*, PC WORLD, Nov. 2005, at 32, *available at* http://www.pcworld.com/reviews/article/0,aid,122499,00.asp.

300. *Id.*

301. An online intermediary such as software vendor should be liable for negligence if it fails to conform to industry standards of Internet security and its failure is the factual cause of the plaintiff's injury.

will incentivize the software industry to build better security into their products and services. The recent *Grokster* case raises the parallel question of whether computer software vendors, who create a product that promotes illegal file swapping, should be liable for secondary copyright infringement. Secondary tort liability should be imposed on software publishers that facilitate economic espionage by marketing products with known vulnerabilities. At present, the victims of state-sponsored or corporate espionage have the tragic choice of deciding whether to report trade secret theft to the FBI or to file common law tort claims for misappropriation in state or federal court.[302]

CONCLUSION

The rapid pace of technological change has exposed a fundamental weakness in the American civil justice system in our federal trade secret law. United States' industry has become the equivalent of a giant cookie jar by permitting foreign agents to steal American know-how with a low probability of detection or prosecution. In a decade of EEA prosecutions, no foreign government has been charged with state-sponsored espionage. All but a few EEA prosecutions were on behalf of Fortune 500 corporations or well-known institutions that can afford to conduct thorough investigations. EEA should therefore be reformed to formally recognize private causes of action.[303] At present, the EEA does not give private individuals or entities standing to file suit for damages when they are victimized by industrial or economic espionage.

302.

> "Misappropriation" means acquiring a trade secret by "improper means" or from someone who has acquired it through "improper means." Things like theft, bribery, and misrepresentation are "improper means." Misappropriation also includes disclosure and use of a trade secret acquired through "improper means." If there is a misappropriation, the injured person may have injunctive relief and damages. Injunctive relief may extend into the future, and may condition future use on a proper royalty. Damages include actual loss and unjust enrichment.

Uniform Law Commissioners, Uniform Trade Secrets Act Summary, http://www.nccusl.org/nccusl/uniformact_summaries/uniformacts-s-tutsa.asp (last visited Apr. 6, 2006).

303. Unlike the EEA, a claimant may establish a civil cause of action under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by demonstrating that a person has (i) "knowingly and with intent to defraud," (ii) accessed a "protected computer," (iii) "without authorization," and as a result (iv) has furthered the intended fraudulent conduct and obtained "anything of value." 18 U.S.C. § 1030(a)(4) (2005).

Secondary or indirect liability should extend to software companies and other entities that enable trade secret theft. Expanded federal trade secret protection will encourage greater investment in research not covered by other criminal statutes. Federalizing the tort of enabling industrial or economic espionage will require Congress to amend the EEA to provide for a private cause of action. The key question about third-party liability for trade secrets is whether corporations, software vendors, and other critical Internet infrastructure owners and operators owe a duty of care to implement adequate security safeguards to prevent trade secret misappropriation. A software vendor, Website, or Internet gatekeeper should be held liable when it "facilitates" the realization of an independently created risk by doing something that they knew or should have known would "pave the way" for a third party to harm the victim."[304]

Corporate and industrial espionage poses a great threat to U.S. competitiveness in a global economy. Law enforcement has been slow to punish and deter Internet-related espionage where a company's trade secrets and other crown jewels can disappear with a click of the mouse.[305] "Computer crimes cost U.S. businesses billions of dollars every year. Many of these foreseeable economic losses would have been prevented had companies taken even basic security measures."[306]

With cybercrimes skyrocketing and an ever-increasing amount of sensitive information being exchanged on the Internet, fortified federal tort remedies are a necessity. EEA must be amended to

304. Twerski & Sebok, *supra* note 191, at 1383. I use the term "Internet gatekeeper," to refer to software developers, licensors, Internet Service Providers (ISPs), e-commerce websites, Internet search engines, and other online intermediaries who protect critical Internet infrastructure. This article proposes extending common law principles into cyberspace by imposing a qualified duty of care on all Internet gatekeepers.

305. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs. Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (ruling that trade secret status as to church documents was lost when information was anonymously posted to the Internet). *Cf.* DVD Copy Control Ass'n, Inc. v. McLaughlin, No. CV 786804, 2000 WL 48512 at *3 (Cal. Super. Ct. Jan. 16, 2000) (ruling that trade secret status was not lost when misappropriators posted it to the Internet because "to hold otherwise would do nothing less than encourage misappropriators of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever.").

306. *Former Justice Department CyberLawyer Peter Toren Authors Guide to Protection Against High-Tech Theft and Intellectual Property Violations*, BUSINESS WIRE, Sept. 12, 2003 (quoting Peter Toren).

permit private actions for economic or industrial espionage.[307] This means that the corporate victim of espionage will have a uniform federal remedy against domestic and foreign spies. Startup companies without the resources to launch private investigations of trade secret theft will be armed as private attorneys general to augment criminal enforcement.

Since 9/11, federal law enforcement officials have not made economic or industrial espionage a priority. The government lacks sufficient resources to tackle this type of crime without the help of private attorneys general. Corporate espionage affects all Americans because it has a corrosive impact on our tax base, destroys jobs, and undermines our position in the global economy.

A robust regime of private enforcement is needed to supplement the EEA. "Private enforcement in the form of 'E-cops' is already becoming well established on the Internet, as many American high technology companies are skeptical about the role of government in detecting and punishing hackers."[308] The EEA needs to be reformed to permit private causes of action to augment lax public enforcement. The private attorney general is urgently needed to punish and deter economic espionage and to protect American competitiveness.

307. *See* Boyd v. University of Illinois, No. 96 Civ. 9327(TPG), 1999 WL 782492 (S.D.N.Y. 1999) (holding that private citizens had no standing to file actions under Title I of the Economic Espionage Act of 1996 because it is a purely criminal statute).

308. Rustad, *supra* note 19, at 100.