# THE ECONOMIC ESPIONAGE ACT OF 1996: ARE WE FINALLY TAKING CORPORATE SPIES SERIOUSLY?

*Thierry Olivier Desmet*[*]

TABLE OF CONTENTS

I. INTRODUCTION ..... 94

II. THE PROBLEMS OF INDUSTRIAL ESPIONAGE ..... 95

III. PRIOR LEGISLATION FOR TRADE SECRETS PROTECTION ..... 101

IV. THE ECONOMIC ESPIONAGE ACT OF 1996 ..... 107
- *A. Legislative History* ..... 107
- *B. EEA Provisions* ..... 109
  - *1. Section 1831* ..... 109
  - *2. Section 1832* ..... 110
  - *3. Section 1834* ..... 112
  - *4. Section 1835* ..... 113
  - *5. Section 1836* ..... 114
  - *6. Section 1837* ..... 114
  - *7. Section 1838* ..... 115
  - *8. Section 1839* ..... 115
- *C. Cases* ..... 118

V. STRATEGIC IMPLICATIONS ..... 123
- *A. Litigation* ..... 123
- *B. Corporate Compliance* ..... 125

VI. CONCLUSION ..... 126

## I. INTRODUCTION

For many companies, information is the most important resource available. Many executives only realize the value of their corporation's secrets when these secrets are stolen and

* J.D., 1998, *magna cum laude*, University of Miami School of Law; B.S., 1993, *with distinction,* University of Nevada, Reno. Attorney in the Miami office of Zuckerman, Spaeder, Goldstein, Taylor, & Kolker, LLP, specializing in complex business litigation and white-collar criminal defense. The author dedicates this article to his family, Alain Desmet, Anita Fol, Olivier Desmet, Victor Elford, and Chantal Braconnier, for their lifelong support and encouragement.

disclosed to a competitor, resulting in huge economic losses.[1] Since the end of the Cold War, American companies have increasingly been targeted by spies funded by competitors or foreign nations, or both, in search of trade secrets.[2] The Economic Espionage Act of 1996 (EEA),[3] enacted to facilitate the criminal prosecution of industrial spies,[4] constitutes a new weapon against corporate spying. It makes the theft of proprietary economic information a felony and protects trade secrets at the federal level.[5] By discouraging improper trade conduct by both foreign governments and private parties, it reflects Congress's recognition of the need to protect U.S. technology from unethical business competitors. The EEA does so by providing severe criminal penalties for those prosecuted under its provisions.[6]

The scope of this Article is to analyze the EEA. Part II describes the nature of international and domestic economic espionage[7] and why it is a threat to corporate success and national security. Part III looks at legislation in existence prior to the EEA and analyzes why that legislation failed to

---

1. *See* Daniel P. Powell, *An Introduction to the Law of Trade Secrets*, 23 COLO. LAW. 2125 (1994).

2. *See* 142 CONG. REC. S12, 207–08 (daily ed. Oct. 2, 1996) (statement of Sen. Specter). "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." *Id.*

3. 18 U.S.C.A. §§ 1831–1839 (West Supp. 1999).

4. *See* H.R. REP. NO. 104-788, at 6–7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4024–25.

5. *See* H.R. REP. NO. 104-788, at 9 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4028; 18 U.S.C. §§ 1831–1832.

6. *See* 18 U.S.C.A. §§ 1831–1832 (West Supp. 1999).

7. Economic espionage is sometimes distinguished from industrial espionage, the former describing a foreign government's sponsoring of intelligence efforts and the latter describing a corporation's use of illegal techniques to collect information. *See* Darren S. Tucker, Comment, *The Federal Government's War on Economic Espionage*, 18 U. PA. J. INT'L ECON. L. 1109, 1112–13 (1997). However, the author does not find this distinction meaningful. "Economic espionage" and "industrial espionage" are used interchangeably throughout this Article. Indeed, the lines are often blurred between foreign and domestic espionage. For example, if a foreign nation conspires with a foreign company to steal trade secrets from a U.S. company, it would seem to involve both economic and industrial espionage. Furthermore, it is often unknown whether a corporation is assisted or sponsored by a foreign nation in its espionage activities. Therefore, what may be branded as industrial espionage may really be an act of economic espionage. Both are essentially the same activity: the collection of secret information by unlawful or clandestine means to gain an economic advantage over competitors. *See generally* UNITED STATES INTELLIGENCE: AN ENCYCLOPEDIA xi (Bruce W. Watson et al. eds., 1990) (distinguishing between strategic intelligence and tactical intelligence); PETER SCHWEIZER, FRIENDLY SPIES (1993) [hereinafter FRIENDLY SPIES].

substantially curb the theft of trade secrets, particularly as it related to small businesses and information stolen by foreign participants. Part IV examines the EEA itself, its legislative history, and the case law that has emerged since its enactment. An analysis of the statute suggests that its provisions are very broad and that if not used selectively, it could potentially hamper the mobility of workers in the labor market, thereby reducing innovation and creativity in the U.S. economy. Part V considers the strategic implications of the Act for practitioners and corporations. This Article concludes, in Part VI, by suggesting a proactive plan allowing companies to protect their trade secrets from foreign spies and from their own employees who may sell that information to the highest bidder. Organizations that have implemented internal security programs are likely to be in the best position to protect their trade secrets from dishonest competitors while insulating themselves from a trade secrets prosecution.

## II. THE PROBLEMS OF INDUSTRIAL ESPIONAGE

Innovation, a significant factor in economic growth, requires a substantial investment of time, money and human resources.[8] If companies lose valuable secrets to industrial espionage, they cannot profit by utilizing their competitive advantage.[9] In turn, if they are unable to recoup their investments in research and development, they lose their motivation to innovate and bring new products or services to consumers. The consequences include higher prices charged to consumers,[10] as well as a decrease in new technologies,

---

8. *See* G.S. Rasmussen & Assoc., Inc. v. Kalitta Flying Serv., Inc., 958 F.2d 896, 900 (9th Cir. 1992).

9. *See* Intermedics, Inc. v. Ventritex, Inc., 822 F. Supp. 634, 642–43 (N.D. Cal. 1993) (discussing, in part, the "continuing tort theory" and whether the various jurisdictions view "the principal interest protected by . . . trade secret law as 'property' *or* as 'confidential relationships' "). For example, if company Z develops a cure for AIDS at a high cost, it must be allowed to profit significantly from that innovation to recoup its investment and encourage other firms to invest in finding cures for illnesses in the hope of achieving similar profits. On the other hand, if company A, a competitor of company Z, finds a comparatively inexpensive way to steal the formula for the AIDS cure from company Z, and subsequently manufactures its own AIDS cure for a fraction of the cost company Z incurred while sharing the humanitarian credit and financial windfall, it is likely that company Z will no longer invest in research and development because its return on investment will be quite low.

10. *See* IRA WINKLER, CORPORATE ESPIONAGE xvi (1997). *But see* 142 CONG. REC. S12, 207–08 (daily ed. Oct. 2, 1996) (statement of Sen. Specter) (positing that the absence of development costs can lead to reduced prices);

creative inventions, and improvements.[11] Furthermore, the very concept of privacy "is threatened when industrial espionage is condoned or is made profitable."[12]

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.[13] Nations have been reshaping their intelligence agencies and investigative resources to be more responsive to the competitive and global needs of businesses.[14] The Cold War has been replaced by the Economic War.[15] 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.[16] Pricing data, customer lists, information on product development, basic research, sales figures, and marketing plans appear to be the most coveted items.[17] In 1997, more than 1,100 documented incidents of economic espionage and at least 550 suspected incidents were reported by U.S. companies.[18] The Federal Bureau of Investigation (FBI), which is now devoting more resources to fight industrial espionage, has reported that its economic espionage caseload doubled from 400 in 1994 to 800 in 1995.[19] It also reports that twenty-three foreign

---

Melody Petersen, *Lawsuits by Rivals Accuse Textile Maker of Corporate Espionage*, N.Y. TIMES, Oct. 13, 1998, at C1 (reporting that competitor lured customers away by using lower prices).

11. *See* Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427, 436 (1995).

12. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 487 (1974) (holding that state protection of trade secrets does not operate to frustrate the achievement of the congressional objectives served by the patent laws).

13. *See Economic Espionage: Joint Hearing Before the Select Comm. on Intelligence U.S. Senate and the Subcomm. on Terrorism, Tech., and Gov't Info. of the Comm. on the Judiciary U.S. Senate,* 104th Cong., 2d Sess. 10, 11 (1996) [hereinafter *Economic Espionage: Joint Hearing*] (statement of Louis Freeh, Director, FBI); *see also* Vernon Loeb, *Wanted: A Few Good Spies*, WASH. POST, Nov. 27, 1998, at A1 (reporting that the CIA is recruiting candidates with technical skills to strengthen its espionage).

14. *See Economic Espionage: Joint Hearing, supra* note 13, at 3, 4 (statement of Sen. Kohl).

15. *See* Leslie G. Berkowitz, *The Economic Espionage Act of 1996: An Experiment in Unintended Consequences?*, 26 COLO. LAW. 47 (1997).

16. *See* Tom Lowry, *Secrets at Stake, Fears of Chinese Spying Mount*, USA TODAY, Jan. 29, 1998, at 1B.

17. *See* Ronald E. Yates, *Cold War: Part II, Foreign Intelligence Agencies Have New Targets—U.S. Companies*, CHI. TRIB., Aug. 29, 1993, at C1.

18. *See Economic Spying Increases, FBI Reports High Loss of Intellectual Property From U.S. Companies*, CHARLESTON DAILY MAIL, Jan. 12, 1998, at P3A [hereinafter *Economic Spying Increases*].

19. *See* Dean Starkman, *Secrets and Lies: The Dual Career of a Corporate Spy*, WALL ST. J., Oct. 23, 1997, at B1.

nations are systematically stealing intellectual assets from U.S. corporations.[20] The stakes in economic espionage are high.[21] In Silicon Valley alone, more than twenty FBI agents are assigned full-time to investigations of trade secret theft.[22] More than 700 foreign counterintelligence investigations involving economic espionage are pending before the FBI.[23] In 1996, FBI Director Louis Freeh told the Senate Select Committee on Intelligence that "foreign intelligence activities against the United States have grown in diversity and complexity in the past few years."[24] The United States International Trade Commission has estimated that in 1986 alone, U.S. businesses lost $23.8 billion as a result of trade secret theft.[25] In 1997, those losses exceeded $300 billion, according to a survey by the American Society for Industrial Security.[26]

The most targeted regions for spying are the Silicon Valley, Detroit, Michigan, North Carolina, and the Pennsylvania-New Jersey area, where most pharmaceutical and biotechnology companies are headquartered.[27] In particular, high-tech businesses, pharmaceutical companies, manufacturing firms, and service industries are the most frequent targets of corporate spies.[28] France, Germany, Israel, China, Russia, and South Korea were named in a survey conducted by the American Society for Industrial Security as the major offenders and supporters of corporate

---

20. *See* Alan Farnham, *How Safe Are Your Secrets?*, FORTUNE, Sept. 8, 1998, at 114, 114.

21. *See* Alan Farnham, *Spy vs. Spy: Are Your Company Secrets Safe?*, FORTUNE, Feb. 17, 1997, at 136, 136.

22. *See* Norm Alster, *The Valley of the Spies*, FORBES, Oct. 26, 1992, at 200, 204.

23. *See* Jack Nelson, *Spies Took $300-Billion Toll on U.S. Firms in '97*, L.A. TIMES, Jan. 12, 1998, at A1.

24. *See* Lowry, *supra* note 16, at 1B.

25. *See* UNITED STATES INT'L TRADE COMM'N, Pub. No. 2065, FOREIGN PROTECTION OF INTELLECTUAL PROPERTY RIGHTS AND THE EFFECT ON U.S. INDUSTRIES AND TRADE 4–1, 4–2 (1988) [hereinafter USITC PROTECTION].

26. *See* Lowry, *supra* note 16, at 1B. Note that this cost is undoubtedly passed on to consumers in the form of higher prices and job losses.

27. *See id.* Silicon Valley is probably the most targeted area due to the concentration of electronics, aerospace, and biotechnological industries, its ties to Asia, and the mobility and sophistication of its workforce. *See* Timothy D. Foley, *The Role of the CIA in Economic and Technological Intelligence*, 18 FLETCHER F. WORLD AFF. 135, 143 (1994).

28. *See Economic Spying Increases*, *supra* note 18, at P3A.

spies.[29] Interestingly enough, some of these perpetrators have been long-time U.S. allies.[30]

This massive amount of corporate spying is accomplished with increasing ease through advances in communication such as the Internet, satellites, and cellular phones.[31] Computer hackers access proprietary information from corporate computer systems and decode encrypted messages from offices located in other countries.[32] Foreign competitors pick up protected information from governmental postings on the Internet, such as chemical use or product data posted on the Internet site of the Environmental Protection Agency (EPA).[33] Domestic companies also face potential theft of trade secrets by American employees looking to sell information to foreign competitors.[34] Retired Eastman Kodak manager Harold Worden, for example, pleaded guilty in 1997 to selling trade secrets to Kodak officials who were working undercover, posing as Chinese agents.[35] Such "moles" have

---

29. *See id.* France, one of the worst offenders, at one time targeted more than 70 U.S. corporations, including Boeing, IBM, Texas Instruments and Corning Glass. *See* Nelson, *supra* note 23, at A18.

30. Although there is evidence that economic espionage by allies was pervasive during the Cold War, the U.S. government did not consider it a threat to national security because allies were also involved in spying on the Soviet Union, which allegedly furthered our own interests. *See* FRIENDLY SPIES, *supra* note 7, at 5–6.

31. *See id.* at 43.

32. *See* Peter J.G. Toren, *The Prosecution of Trade Secrets Thefts Under Federal Law*, 22 PEPP. L. REV. 59, 61–62 (1994). Rather than copying documents manually, a thief can download information onto a computer disk which is then easily removed from an office. In his comments to the Senate Select Committee on Intelligence, FBI Director Louis Freeh stated:

> Where hackers formerly may have been motivated by the technical challenge of breaking into a computer system, the motivation may be shifting more toward hacking for profit. As more and more money is transferred through computer systems, as more fee-based computer services are introduced, as more sensitive proprietary economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the tendency toward information threats emerging as national security threats will increase.

*Current and Projected Nat'l Sec. Threats to the U.S.: Hearings Before the Select Comm. on Intelligence of the U.S. Senate*, 105th Cong., 2d Sess. 35 (1998).

33. *See* Lowry, *supra* note 16, at 1B.

34. *See id.*

35. *See id.* Insiders not only are able to break into computer systems and steal information by using their legitimate access, but they generally have the knowledge of where to find the most sensitive and valuable information. FBI Director Louis Freeh has stated that a large number of trade secret thefts performed through computer intrusion have at their core an employee, past or present, who has exceeded his or her access, often in revenge for perceived

been known to take documents from offices and hotel rooms.[36] They routinely infiltrate American businesses in disguise, to obtain access to secret information.[37] Graduate students are also used to infiltrate research plants, universities, and businesses.[38]

As the following two examples demonstrate, foreign spies have developed clever techniques to gather valuable information. In one instance, the former chief of the French intelligence service admitted in 1991 that his agency had made it a habit to spy on U.S. business executives traveling to France by bugging first-class seats on Air France and breaking into hotel rooms to search attaché cases.[39] China's conduct is perhaps even more brazen. They are suspected of routinely sending visiting scholars, business delegates, and students to the United States in an orchestrated effort to infiltrate companies and eventually bring back valuable information and trade secrets to China.[40] Predictably, Chinese officials consistently deny charges of economic espionage. Dismissing such allegations as untrue, a spokesperson for the Chinese embassy in Washington has declared that "all of China's relations with other countries have been conducted in compliance with international norms and the laws of those countries."[41] Although China is only one of many nations suspected of spying on the United States, U.S. officials are so worried about the loss of intellectual property to Chinese agents that they have raised this concern in regards to China's efforts to join the World Trade Organization (WTO).[42] Despite this, current U.S.-China relations provide no assurances that industrial espionage by Chinese agents has or is likely to cease.[43] One commentator

---

unfair treatment by the company. *See Economic Espionage: Joint Hearing*, *supra* note 13, at 50.

36. *See Foreign Threat to U.S. Business Travelers* (visited Sep. 12, 1999) <http://www.nacic.gov/foreign.html>.

37. *See* Lowry, *supra* note 16 (reporting two stories of corporate espionage by insiders).

38. *See id.*; JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA 149–160 (1997) (explaining how Chinese and Japanese students flood American schools and corporations).

39. *See* Tom Robbins, *In the Modern World of Espionage, Targets are Economic*, HOUS. CHRON., Sept. 11, 1994, at C10.

40. *See* Lowry, *supra* note 16, at 1B.

41. *Id.* (internal quotations omitted).

42. *See id.*

43. *See* Porcher L. Taylor III, *Summitry . . . and Economic Espionage*, WASH. TIMES, Nov. 23, 1997, at B1. Some commentators believe that the Clinton administration is not aggressive enough with respect to industrial espionage matters in that it turns a blind eye toward Chinese corporate spying

has suggested tightening the visa process to ensure, for example, that foreigners are not able to fill graduate school slots where they are privy to leading research as part of their studies.[44]

Interestingly, most companies fail to report that they have been the victims of corporate spying.[45] According to Richard Power, an official at the Computer Security Institute, company executives often fear shareholder backlash, negative publicity, and further exposure of trade secrets during prosecution.[46] A disclosure that the company has been the victim of trade secret theft can also result in a reduction of market share, embarrassment, and fear on the part of prospective investors.[47] Thus, the cost of corporate spying may be considerably higher than statistics indicate.

## III. PRIOR LEGISLATION FOR TRADE SECRETS PROTECTION

At common law, employers had a property right in their trade secrets, and the disclosure of such confidential information in violation of an employment relationship was a tort.[48] Section 757 of the *Restatement of Torts*, entitled Misappropriation of Trade Secrets, continues to be cited

---

for the sake of good trade relations. They argue that the State Department should once and for all warn the Chinese Government and Chinese companies that the Justice Department will vigorously prosecute trade secret theft under the EEA. There are also many diplomatic options available for punishing offenders. They include denying access to U.S. labs, withholding access to the U.S. market and government contracts, and expelling diplomats involved in corporate spying. On a related matter, the FBI has been investigating whether John Huang, a former Democratic National Committee fund-raiser, gave classified information, obtained while working for the Clinton administration, to his former employer, the Lippo Group, which has close ties to the Chinese government. According to the Commerce Department, Huang, who was not subjected to a full background investigation by the FBI, a major oversight for someone privy to intelligence briefings, saw 15 classified field reports and 12 finished intelligence reports. The administration's attitude toward background checks has been described as ranging from casual to hostile. *See Economic Espionage: FBI Probing Whether Huang Revealed Secrets*, COLUMBUS DISPATCH, Jan. 30, 1997, at 8A.

44. *See* FIALKA, *supra* note 38, at 152 (revealing that students from the Pacific Rim occupy the majority of doctorate of science and engineering seats). Note that this option is likely to deny valuable talent and human resources to U.S. companies and may in fact do more damage than good to the U.S. economy.

45. *See* Lowry, *supra* note 16, at 1B.

46. *See id.*

47. *See Economic Espionage: Joint Hearing supra* note 13, at 49 (statement of Louis Freeh, Director, FBI).

48. *See* Peabody v. Norfolk, 98 Mass. 452, 458 (1868) (recognizing a cause of action for breach of trust in commercial enterprise).

today as the guide to the law of trade secret misappropriation.[49] According to the *Restatement*, misappropriation occurs once a secret is acquired either by improper means or with notice of its mistaken disclosure.[50]

Although thirty-eight states and the District of Columbia have enacted trade secret statutes, often modeled after the Uniform Trade Secrets Act (UTSA), these state laws have not been effective, primarily because the resources needed to prosecute trade secret cases are usually not available at the state government level.[51] Furthermore, because most states modified the UTSA when they drafted their own state laws, resulting in a complete lack of uniformity, the statutory framework provided by states is inefficient and unpredictable.[52] To complicate things further, states such as New York, Pennsylvania, and Texas have wholly adopted the *Restatement* approach to trade secret theft,[53] ignoring the UTSA and contributing further to the creation of an unstable and unstructured statutory regime.[54] As a result, companies do not know in advance of the trade secret theft which state's law will govern.[55] In other words, company executives have no way of knowing where a stolen trade secret will be

---

49. *See* Pace, *supra* note 11, at 430. Note that the drafters of the *Restatement (Second) of Torts* concluded that trade secret theft and other torts based on unfair trade practices had developed into a more specific area of law deserving individual treatment. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (1995). They decided to drop trade secret theft, as a topic, from the second *Restatement*. *See id.* It was moved to the *Restatement of Unfair Competition*. Instead of using this new *Restatement* when dealing with trade secret theft issues, courts have continued to rely on the first *Restatement*. *See* Pace, *supra* note 11, at 430 n.12.

50. *See* RESTATEMENTS OF TORTS § 757 (1939):

> One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if (a) he discovered the secret by improper means, or (b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or (c) he learned the secret from a third person with notice of the facts that it was a 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 the other, or (d) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake.

*Id.* at 1-2.

51. *See* Pace, *supra* note 11, at 443–45.

52. *See* S. REP. NO. 104–359, at 11 (1996).

53. *See* Pace, *supra* note 11, at 443–45.

54. *See id.* at 443, 445. State courts also disagree on how to define important concepts relevant to trade secret theft, such as "improper means" and "reasonable security steps," resulting in a chaotic and imprecise body of law. *See id.* at 445.

55. *See id.* at 446.

disclosed or where it will be used after disclosure. This leaves executives unable to tailor their confidentiality and compliance programs to a specific region or statutory regime.[56] Finally, in most states, trade secret theft is not even a felony.[57] Commentators agree that a uniform trade secret regime is much more useful to avoid these choice of law issues in litigation.[58] With modern technology resulting in a fountain of information, a uniform federal system of law designed to protect trade secrets appears better suited to combat industrial espionage than fifty conflicting state legal systems.[59] This argument is bolstered by the fact that international trade is a uniquely federal concern.[60]

Federal prosecutors in the past have tried to use the National Stolen Property Act (NSPA),[61] to fight trade secret theft.[62] It prohibits the transportation, transmission, or transfer of "any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud."[63] The NSPA was designed, however, to prevent traditional property crimes and it does not function adequately with respect to intangible property.[64] Consequently, trade secret prosecutions under the NSPA have not been successful.[65] Additionally, the wire and mail fraud statutes, which prohibit the use of the mail, wire, radio, or television to obtain money or property

---

56. *See id.* at 447.

57. *See* S. REP. NO. 104–359, at 11 (1996).

58. *See* Pace, *supra* note 11, at 446–47. *See also* Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L. J. 1633, 1671–74 (1998).

59. *See* Pace, *supra* note 11, at 448.

60. *See id.* at 449. *See also* Spencer W. Waller & Noel J. Byrne, *Changing View of Intellectual Property and Competition Law in the European Community and the United States of America*, 20 BROOK. J. INT'L L. 1, 7–8 (1993) (noting that the United States has made the enforcement of intellectual property rights a top priority, often conditioning trade concessions on the enforcement of intellectual property rights by recipient nations).

61. National Stolen Property Act, 18 U.S.C. §§ 2314, 2315 (1994).

62. *See, e.g.*, United States v. Brown, 925 F.2d 1301, 1305 (10th Cir. 1991) (upholding the dismissal of an indictment for failure to prove that a computer program and source code crossed state lines in tangible form).

63. 18 U.S.C. § 2314.

64. *See Brown*, 925 F.2d at 1307–08 (holding that "[p]urely intellectual property," such as computer code, does not fall under NSPA protection). *But see* United States v. Steerwell Leisure Corp., 598 F. Supp. 171 (W.D.N.Y. 1984). "Judge Friendly's opinion for the Second Circuit in United States v. Bottone, 365 F.2d 389, 393 (1966) stated in no uncertain terms that intangible rights, embodied in tangible objects which are not themselves stolen, can be basis of prosecution under 18 U.S.C. § 2314." *Id.* at 174.

65. *See Brown*, 925 F.2d at 1307 n.14.

fraudulently,[66] have been ineffective in fighting economic espionage.[67] This is because corporate spying does not often involve the use of the mail or wire.[68] Furthermore, proving an intent to defraud is often difficult.[69] Finally, these statutes do not reach acts of memorizing or copying information,[70] the methods used most often to misappropriate trade secrets.[71] Because such federal statutes did not address the particular problems associated with trade secrets and were not applicable to "intangible" intellectual property,[72] UTSA was created in 1979 to codify existing common law standards.[73]

The UTSA constituted the first attempt at comprehensive national legislation of trade secrets theft.[74] The UTSA defines misappropriation similarly to the *Restatement*, but provides examples of what "improper means" include, namely, "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means."[75] The main advantage of the UTSA over the

---

66. *See* 18 U.S.C.A. §§ 1341–1343 (West Supp. 1999).

67. *See* S. REP. NO. 104–359, at 10 (1996).

68. *See id.* For example, imagine a case where a lab technician steals valuable trade secrets, used, let's say, in the research of medicine to decrease cholesterol levels, and attempts to sell them to a competitor for a large amount of money. If the thief implements his scheme without involving the mails, phones, and interstate travel, the wire and mail fraud statutes would be useless to prosecute him.

69. *See* S. REP. NO. 104–359, at 10 (1996).

70. *See* Victoria A. Cundiff, *The Economic Espionage Act and You*, *in* THIRD ANNUAL INSTITUTE FOR INTELLECTUAL PROPERTY LAW, at 9, 22 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series NO. G-490, 1997).

71. *See* S. REP. NO. 104–359, at 6, 8 (1996).

72. *See* United States v. Brown, 925 F.2d 1301, 1309 (10th Cir. 1991).

73. *See* UNIF. TRADE SECRETS ACT, Prefatory Note (amended 1985), 14 U.L.A. 433–34 (1990).

74. *See* Linda B. Samuels & Brian K. Johnson, *The Uniform Trade Secrets Act: The States' Response*, 24 CREIGHTON L. REV. 49, 49–51 (1990).

75. UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 438 (1990). The UTSA defines misappropriation as:

> (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 reasons to know that his knowledge of the trade secret was (I) derived from or through a person who had 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 [or her] position, knew or had reason

common law is that it allows an aggrieved party to sue and recover from a third party that has accepted stolen information, which often turns out to be a foreign company with deeper pockets than the culprit.[76] The Act also provides for civil remedies for the theft of trade secrets, including both injunctive relief and recovery of monetary damages.[77] Although damages include lost profits, the cost of investment in research and development, loss of reputation in the business community, and loss of the value of the trade secret,[78] many of the businesses engaging in these offenses view the potential damages as a necessary risk, the cost of doing business, and a way to gain an economic advantage over competitors. In other words, for many companies and individuals involved in stealing competitors' secrets, the penalties are not a deterrent.[79]

A civil statute may be particularly useless to small businesses that may not be able to afford the exorbitant expenses of a civil suit against a much larger competitor engaging in trade secret theft. Such small businesses cannot afford to be involved in litigation that often takes years.[80] The civil statute is also fairly ineffective in curbing industrial espionage schemes implemented by foreign culprits. A corporation based in North Carolina, for example, is not likely to recover from one of its former engineers, a Korean citizen who has relocated to Korea after disclosing company

---

to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

*Id.*

76. *See* Jeff Augustini, Note, *From Goldfinger to Butterfinger: The Legal and Policy Issues Surrounding Proposals to Use the CIA for Economic Espionage*, 26 LAW & POL'Y INT'L BUS. 459, 475 (1994).

77. *See* UNIF. TRADE SECRETS ACT § 2-3, 14 U.L.A. 449–445 (1990).

78. *See* Next Level Communications LP v. DSC Communications Corp., 179 F.3d 244, 247 (5th Cir. 1999) (awarding damages for future lost profits on a trade secrets misappropriation claim); University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 538 (5th Cir. 1974) (noting that damages should take into consideration development costs in trade secret cases); IDS Life Ins. Co. v. SunAmerica, Inc., 958 F. Supp. 1258, 1262 (N.D. Ill. 1997) (outlining that injury to plaintiff's business reputation may result from misuse of a trade secret); *In re* Ivan F. Boesky Sec. Litig., 825 F. Supp. 623, 632 (S.D.N.Y. 1993) (stating that the value of the information misappropriated is limited to the value which was destroyed or diminished at the expense of the public shareholders by the premature disclosure of the information).

79 *See Economic Espionage: Joint Hearing, supra* note 13, 14 (statement of FBI Director Louis Freeh).

80. *See generally* Thomas M. Kerr, *"Trade Secrets," i.e., Confidential Business Information or Business Intelligence*, 145 PITT. LEGAL J. 27, 28 (Dec. 1997) (discussing lengthy discovery processes, and low priority docket scheduling for non-criminal cases).

secrets to a Korean company. Finally, such a civil statute does not ensure that the confidentiality of the information at issue will be preserved in the course of a trial.[81] Without such guarantees, civil litigation can do more harm than good.[82]

Consequently, legislative reform was needed to provide stronger deterrent and to address the modern concerns of instant communication, a decrease in employee loyalty, a shift from an economy based on manufacturing to one based on intellectual property, and a shift of espionage resources by foreign countries to economic targets. As the Supreme Court noted years ago, "[existing] trade secret law provides far weaker protection in many respects than the patent law."[83] Therefore, it became increasingly clear that a federal criminal statute would better protect companies, which could not afford to wait years to resolve disputes through civil litigation. Also, criminal cases have scheduling precedence on dockets.[84] A federal criminal statute would allow small businesses to "ride the coattails" of federal prosecutors who perform investigations, gather evidence, and build a record for them.[85]

## IV. THE ECONOMIC ESPIONAGE ACT OF 1996

### *A. Legislative History*

Hearings on "business intelligence" were held in 1996 to address the topic of economic espionage both as a crime and as a national security issue.[86] Trade association and business representatives spoke to highlight their concerns for a comprehensive federal effort to curb industrial espionage.[87] The inventor of magnetic resonance imaging technology testified that both German and Japanese firms systematically spied on his company.[88] The former president of a defunct software business described how his firm had been driven out of the market after Chinese agents pilfered confidential

81. *See id.*
82. *See id.*
83. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 489–90 (1974).
84. *See* Kerr, *supra* note 80, at 28.
85. *See id.*
86. *See id.*
87. *See id.* at 30; *see also Economic Espionage: Joint Hearing*, *supra* note 13, at 23 (statements from officers of Lockheed Martin Corporation, Fonar Corporation, Hughes Electronics Corporation, and Ellery Systems, Inc.).
88. *See* Cundiff, *supra* note 70, at 18.

software information.[89] As a result of the perceived need for stronger measures against industrial espionage, the EEA was designed to criminalize the misappropriation of trade secrets and encourage and preserve investments in innovation.[90] It was passed by Congress with strong majorities, 399-3 in the House of Representatives and unanimous consent in the Senate.[91] It was signed into law by President Clinton on October 11, 1996.[92]

An analysis of the legislative history indicates that the EEA is not intended to apply to innocent innovators or to individuals who seek to capitalize on personal knowledge, skill or abilities.[93] Moreover, the statute is not meant to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed.[94] Rather, the goal of the EEA is to preserve fair competition by making sure that corporate spies do not illegally take the fruits of their competitors' hard labor and innovation.[95] It is meant to criminalize the acts of "employees who leave their employment and use their knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer."[96]

Although it is still too early to predict how aggressively the EEA will be applied by the Justice Department, it is clear from the legislative intent that potential employers should not be hesitant or discouraged from recruiting from competitors.[97] Luring a knowledgeable employee is perfectly legal. The EEA is not meant to chill competition or restrict mobility of employment.[98] It is, however, meant to stop companies from hiring employees in order to gain access to a competitor's trade secrets.[99] Because there is a fine line between generic information and "trade secrets," it will be

---

89. *See id.*

90. *See* Peter Schweizer, *New Spy Law Could Cramp Economy*, USA TODAY, Nov. 20, 1997, at 15A.

91. *See* Kerr, *supra* note 80, at 28.

92. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (1996).

93. *See* H.R. Rep. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4025–26.

94. *See id.*

95. *See id.* at 3, 1996 U.S.C.C.A.N. at 4022.

96. *Id.* at 7, 1996 U.S.C.C.A.N. at 4025–26.

97. *See id.*

98. *See id.*

99. *See id.*

interesting to see whether the Justice Department targets employees who leave businesses to join competitors and share "general acquired knowledge" or whether it will focus strictly on employees or spies who are caught misappropriating "specific knowledge."

There do not seem to be legal constraints in place to ensure the integrity of the distinction between general and specific knowledge under the EEA. In other words, the difference between luring a valuable employee for her skills, which is legal under the EEA, and luring an employee for her knowledge of trade secrets, which is illegal, is neither obvious nor precise. On that ground, the statute is rather vague. In light of the legislative history, one would hope that prosecutors will focus on obvious cases of unlawful activity, such as the ones they have selected thus far.[100]

While the EEA was pending, Attorney General Janet Reno assured Congress that for the first five years after its adoption, the Justice Department would not pursue borderline cases, and that prosecution would require the personal stamp of approval of either the attorney general, deputy attorney general, or assistant attorney general for the criminal division.[101] If the Justice Department fails to honor this promise, the vibrancy of the U.S. economy, the strength of which is in part based on the mobility of the workforce, would be deeply affected.

### *B. EEA Provisions*

#### *1. Section 1831*

Stealing, duplicating, or even the of receiving trade secrets by a foreign agent without authorization are all prohibited acts under the EEA.[102] Attempt or conspiracy to engage in this unlawful activity is also illegal.[103] The statute

---

100. So far, it is undeniable that the Department of Justice has acted very reasonably in its selection of cases pursued. *See infra* text accompanying notes 152–196.

101. *See* Joseph F. Savage, Jr., *I Spy: The New Economic Espionage Act Can Be Risky Business*, 12 CRIM. JUST. 13, 16 (1997).

102. *See id.* Section 1831 requires that the offender intends or knows that his conduct is likely to benefit a foreign nation, entity or person. *See* 18 U.S.C.A. § 1831 (West Supp. 1999). One could conclude that a perpetrator who steals "for fun" or "as a challenge," without an intent to benefit anyone, would not be guilty under the Act.

103. *See* 18 U.S.C.A. §1831(a)(4); *see also* United States v. Hsu, 982 F. Supp. 1022, 1029 (E.D. Pa. 1997), *rev'd on other grounds*, 155 F.3d 189 (3rd Cir. 1998) (holding that a defendant may be convicted of attempted theft of trade secret when his objective conduct corroborates the requisite criminal

recognizes that trade secrets can have great value which can be destroyed without a physical transfer. For example, an employee disclosing trade secrets that she remembers from her time at the previous employer can constitute economic espionage under this provision.[104] Conspiracy to engage in this unlawful activity is also illegal.[105] Section 1831 does not set a minimum value for the loss of trade secrets. Also, because "benefit" is not among the terms defined in section 1839, it is unclear whether section 1831 includes a reputational or tactical benefit as compared to just an economic benefit, which the statute explicitly requires.[106]

Anyone convicted under the EEA of a theft intended to benefit any "foreign instrumentality, or foreign agent" may be imprisoned for up to fifteen years or fined up to $500,000, or both.[107] Companies may be fined up to $10 million.[108] The severity of these penalties reflects a desire to launch a strong assault on economic espionage and sends a message that theft of confidential economic information, routinely accepted during the Cold War, will no longer be tolerated by the United States.

*2. Section 1832*

The same acts prohibited by section 1831 are made illegal under section 1832 in relation to "a trade secret that is related to or included in a product that is produced for or placed in interstate or foreign commerce . . . ."[109] It is unclear whether this provision makes a distinction between trade secrets relating to services as opposed to tangible products.[110] Indeed, the word "product" is not defined in section 1839. The penalties for violation of section 1832 vary according to the nature and status of the defendant and the purpose for which the defendant acted.[111] Penalties for theft of a trade secret not involving a foreign nation are less harsh

---

intent, that is, he demonstrates specific intent to commit the substantive crime and he takes a substantial step towards the commission of that crime).

104. *See* 18 U.S.C.A. § 1831(a)(2).
105. *See id.* § 1831(a)(5).
106. *See id.* § 1831(a).
107. *Id.* § 1831(a)(1).
108. *See id.* § 1831(b).
109. *Id.* § 1832(a).
110. *See* Cundiff, *supra* note 70, at 31.
111. *See* 18 U.S.C.A. § 1832 (West Supp. 1999).

than for a theft involving a foreign nation.[112] The difference in punishment can be explained by the legislative intent to focus particular attention on espionage sponsored and sanctioned by other countries.[113]

Section 1832 indicates that a violation does not occur if the disclosure was unwittingly made.[114] Furthermore, mere possession of the material constituting a trade secret should not be enough to constitute a misappropriation.[115] Taking advantage of a skill learned on the job or of knowledge gained during employment, if not acquired by illegal means, also does not fall under the scope of the EEA.[116]

Three elements of intent are required for a successful prosecution under section 1832.[117] These elements constitute a considerable burden for the government to satisfy beyond a reasonable doubt. First, the defendant must "knowingly" commit one of the listed acts of misappropriation.[118] Second, the defendant must act "with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof,"[119] which may preclude prosecution of defendants who act out of revenge or who take

---

112. *Compare* 18 U.S.C.A. § 1831, *with* 18 U.S.C.A. § 1832 (limiting punishment of individuals to $500,000, 10 years imprisonment, or both, and of organizations to $5,000,000).

113. H.R. REP. NO. 104-788, at 4–5 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022–24.

114. *See* 18 U.S.C.A. § 1832.

115. *See id.*

116. *See* H.R. REP. NO. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4025–26.

117. *See* 18 U.S.C.A. § 1832 (West Supp. 1999). Under the EEA, a person is guilty if she acts with the requisite intent and:

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

*Id.* § 1832(a)(1)–(5).

118. *Id.* § 1832(a).

119. *Id.*

information without the specific goal of benefiting anyone financially.[120] Third, the defendant must act "intending or knowing that the offense will injure any owner of that trade secret . . . ."[121] This effectively eliminates prosecution of individuals who are not aware that their actions are wrong.

*3. Section 1834*

Recognizing that monetary fines alone may be inadequate to stop businesses from stealing trade secrets in cases in which the information is worth more than the fine incurred, the statute empowers courts to compel the forfeiture of property constituting proceeds or flowing from proceeds of the violation, as well as property used to facilitate the infraction.[122] The U.S. government may seize these assets under procedures followed pursuant to the Comprehensive Drug Abuse Control Act of 1970.[123] To illustrate, if a foreign agent uses computers, phones, office space, and other equipment to facilitate the theft of a company's trade secrets, a court may order these items confiscated. The broad forfeitures sought in drug and money laundering cases point to the potential for abuse and due process violations such provisions may create.[124] Although it is hoped that Janet Reno's call for moderation in prosecution will avoid such forfeiture abuses in the context of the EEA, history teaches us to remain skeptical.[125]

---

120. *See id.*

121. *Id.*

122. *See* 18 U.S.C.A. §1834 (a)(1)–(2) (West Supp. 1999).

123. *See* 18 U.S.C.A. § 1834(b) (West Supp. 1997); 21 U.S.C.A. § 853 (West 1999). Property is defined in § 853(a) as: "(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; (2) any of the person's property used, or intended to be used, in any manner or part, to commit, or to facilitate the commission of, such violation." Further, § 853(n) allows victims to petition the court to return all forfeited property in which they claim an interest. This would allow owners of stolen trade secrets to recover their property rather than allowing the government to auction it off to the highest bidder.

124. For evidence of prosecutors' tendencies to overuse the tool of forfeiture, see United States v. $506,231, 125 F.3d 442, 452 (7th Cir. 1997) (allowing the forfeiture of currency without any evidence of criminal activity); United States v. $31,990,982 F.2d 851, 854 (2d Cir. 1993) (affirming order returning money seized without any evidence of illegal activity because evidence was insufficient to demonstrate probable cause that currency was traceable to sale of narcotics).

125. *See* Susan Adams, *Forfeiting Rights*, FORBES, May 20, 1996, at 96, 96.

*4. Section 1835*

One of the most important features of the EEA is the provision regarding confidentiality of information during trial.[126] The courts may order such actions as are "necessary to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, and the Federal Rules of Evidence, and all other applicable laws."[127] Section 1835 encourages plaintiffs to cooperate with the government in the design of an appropriate protection.[128] The choice of an interlocutory appeal is a valuable tool to challenge an order authorizing disclosure during trial.[129] It will be interesting to see how courts reconcile this right of confidentiality with a defendant's right to a fair trial which would seem to require disclosure for the preparation of an adequate defense.[130]

*5. Section 1836*

Although the Attorney General of the United States, in a civil action, also may seek and obtain injunctive relief against violators of the EEA, the statute does not provide a private cause of action to litigants who will presumably be required to use existing civil injunctive relief available in state courts.[131] Of course, a conviction in federal court should enable private litigants to win in a subsequent civil suit without the extreme expenses ordinarily involved in an intellectual property action.

*6. Section 1837*

The EEA aims to reach extraterritorial acts by punishing offenders, regardless of nationality, whose illegal conduct occurred outside the United States, if an act in furtherance of such conduct was committed inside the United States.[132] It also punishes U.S. citizens or lawful permanent residents or entities organized under U.S. laws even when the secret theft occurs outside the United States.[133] Corporate spying

126. *See* U.S.C.A. § 1835 (West Supp. 1999).
127. *Id.*
128. *See id.*
129. *See id.*
130. *See, e.g.*, Stamicarbon N.V. v. American Cyanmid Co., 506 F.2d 532, 540 (2d Cir. 1974) (holding that restricting access to the trial during disclosure of trade secrets is permissible if it can be achieved with "minimal disruption").
131. *See* 18 U.S.C.A. § 1836(a).
132. *See id.* § 1837(2).
133. *See id.* § 1837(1).

between nations appears to fall under the jurisdiction of the EEA if any part of the offense involved a resident of the U.S. or took place in the United States.[134] Foreign spies must realize that they may not be able to escape prosecution under the EEA by simply returning to their country after misappropriating trade secrets.[135] On the other hand, the EEA does not appear to apply to acts committed strictly on foreign soil by foreign nationals, even if directed at U.S. subsidiaries doing business in that country.[136] As a result, U.S. businesses involved in trade abroad should be particularly careful in monitoring their trade secrets outside the United States since the statute may not have any deterrent value or offer any legal recourse when misfeasance is strictly foreign.[137] It is also unclear whether foreign entities whose trade secrets are misappropriated on U.S. soil could invoke the EEA.[138]

*7. Section 1838*

According to this section, businesses may have to defend against suits brought under the EEA, and under other federal statutes, as well as against state-based suits. Similarly, victimized businesses wishing to sue for theft of trade secrets should continue to consider civil remedies, state criminal statutes, and other federal criminal laws such as the mail and wire fraud statutes, along with the EEA. In other words, the EEA adds a new remedy without removing existing ones.

---

134. *See id.* § 1837.

135. *See id.*

136. *See id.*

137. Note that there exists a uniform mechanism for the international protection of trade secrets under the General Agreement on Tariffs and Trade (GATT) which established the WTO and promulgated a series of trade-related agreements including the Trade-Related Aspects of Intellectual Property Rights (TRIPS). *See* Karen Sepura, Note, *Economic Espionage: The Front Line of a New World Economic W*ar, 26 SYRACUSE J. INT'L L. & COM. 127, 143–44 (1998). Under GATT, member countries must provide effective remedies for trade secret theft that is contrary to honest commercial practices, including injunctive relief and damages. *See id.* This constitutes protection for victims of trade secrets on foreign soil who are not directly protected by the EEA. *See id.*

138. *See* Cundiff, *supra* note 70, at 51 (observing that the Act could, in theory, be used on behalf of foreign corporations doing business in the United States).

*8. Section 1839*

The Supreme Court has twice held that information is property.[139] The EEA builds on this concept by using traditional property concepts in its statutory definitions. For example, "owner" is defined as "the person or entity in whom or in which rightful legal or equitable title to . . . the trade secret is reposed."[140]

Section 1831 provides for prosecution of those who act "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent . . . ."[141] When read in conjunction with the definitions in section 1839, this means that corporations or individuals cannot be potential defendants under section 1831 unless they intend or know the offense will benefit an entity that is "substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government; . . . [or] any officer, employee, proxy, servant, delegate, or representative of a foreign government . . . ."[142] As previously discussed, the primary intent of the EEA is to curb corporate espionage sponsored by foreign nations, not foreign corporations per se, although foreign businesses may be prosecuted under section 1832.

The definition of a trade secret in the EEA includes "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . . ."[143] This definition is broader than that provided in many state trade secret criminal statutes, which tend to be focused on the theft of medical or scientific information.[144] It is also broader than the UTSA, which covers "information, including a formula, pattern, compilation, program, device, method,

---

139. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984); Carpenter v. United States, 484 U.S. 19 (1987).

140. 18 U.S.C.A. § 1839(4) (West Supp. 1999).

141. 18 U.S.C.A. § 1831(a) (West Supp. 1999).

142. 18 U.S.C.A. § 1839(1)–(2) (West Supp. 1999).

143. 18 U.S.C.A. § 1839(3) (West Supp. 1999).

144. *See, e.g.*, IDAHO CODE ANN. § 48-801 (Michie 1997); IND. CODE ANN. § 24-2-3(2) (Michie 1996); IOWA CODE ANN. § 550.2(4) (West 1997); MASS. GEN. LAWS ANN. ch. 266, § 30 (West 1990); TEX. PENAL CODE ANN. § 31.05(a)(4) (Vernon 1994).

technique, or process . . . ."[145] This broad definition may result, however, in dangerous implications for the free mobility of labor. Employers may shy away from hiring highly qualified individuals for fear of liability under the EEA. Similarly, employees may hesitate to change jobs, unclear about whether the knowledge they could bring to a new company may fall under the definition of trade secret.

Yet defining property so broadly encompasses all novel information that has independent economic value to its owner.[146] Moreover, a unique combination of known components may qualify as a trade secret.[147] The information must not be generally known or exist in the public domain and the owner must make reasonable efforts to keep the information secret.[148] Extraordinary efforts are not required, however.[149] "Reasonable steps" is likely to be interpreted by looking at the presence, or absence, of a corporate compliance program designed to protect trade secrets. Such a compliance program should have as its goals (1) stressing proprietary claims to confidential information, (2) restricting access to trade secrets, (3) warning employees and visitors of the existence of trade secrets, and (4) publicizing the consequences of misappropriation.[150] If the trade secret owner fails to take reasonable steps to protect the information, there is no felony under the statute for taking the secret.[151] It must objectively be kept secret. In other words, a guilty mind is not enough. This requirement assures that the potential culprit is placed on notice that the information is considered secret, and it assures that the owner considers the information valuable.

---

145. UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 437–38. (1985).

146. *See* 18 U.S.C.A. § 1839(3)(B) (West Supp. 1999).

147. *See* Integrated Cash Management Servs., Inc. v. Digital Transactions, Inc., 732 F. Supp. 370, 374–77 (S.D.N.Y. 1989) (granting injunction to prohibit corporate spy from using certain generic programs).

148. *See* Patrick P. Phillips, *The Concept of Reasonableness in the Protection of Trade Secrets*, 42 BUS. LAW. 1045–46 (1987).

149. *See id.* at 1046; *see also* Aries Info. Sys., Inc. v. Pacific Management Sys. Corp., 366 N.W.2d 366, 368 (Minn. Ct. App. 1985) (stating that the owner of a trade secret is not required to guard against unanticipated, undetectable or unpreventable methods of discovery).

150. For more information on the design of corporate compliance programs to protect a company from trade secret theft, *see infra* text accompanying notes 214–232.

151. *See* 18 U.S.C.A. § 1839(3) (West Supp. 1999).

### C. Cases

While the legislative history of the statute clearly indicates that the EEA was created mainly to fight international spies who have shifted their resources towards economic intelligence since the end of the Cold War,[152] the first prosecution under the statute demonstrated that federal prosecutors will also be using the EEA for domestic cases involving strictly American interests.[153] Patrick Worthing, a maintenance supervisor in Pittsburgh-based PPG Industries' fiberglass research center contacted the chief executive officer of Corning Glass, a competitor,[154] and offered to sell PPG's trade secrets, including computer disks, research and blueprints.[155] The Corning Glass executive promptly contacted PPG, which called the FBI.[156] An undercover operation was planned in which an agent, posing as a Corning employee, met with Worthing to exchange money for the trade secrets.[157] The PPG employee was arrested on December 7, 1996 and charged with violating the EEA. He pleaded guilty and was sentenced to fifteen months in prison.[158] His brother, Daniel Worthing, who assisted in the scheme, pleaded guilty to similar charges and was sentenced to five years' probation.[159] PPG estimated that the stolen secrets were worth up to $20 million.[160]

In the second case brought by federal prosecutors, an engineer employed by a consulting firm helping the Gillette Company design its next generation of razors pleaded guilty to stealing secrets relating to new technology.[161] He attempted to sell product, equipment, and assembly drawings,[162] because he had been passed over for a promotion and was angry with his supervisor.[163] In the

---

152. *See* H.R. REP. No. 104-788, at 5–7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023–26.

153. *See* Stan Crock & Jonathan Moore, *Corporate Spies Feel a Sting*, BUS. WK., Jul. 14, 1997, at 76, 77–78.

154. *See id.*; Schweizer, *supra* note 90, at 15A.

155. *See id.*

156. *See* Crock & Moore, *supra* note 153, at 77–78.

157. *See id.* at 76.

158. *See id.*

159. *See id.*

160. *See id.*

161. *See Engineer Pleads Guilty to Selling Gillette Secrets; Faxes, E-Mails of New Razor's Design Sent to Competitors*, BOSTON GLOBE, Jan. 28, 1998, at C5.

162. *See* Michael Davis, *Engineer Faces Fraud, Theft Charges*, TENNESSEAN, Sep. 27, 1997, at E1.

163. *See* David Talbot & Cosmo Macero, Jr., *Feds: Engineer Tried to Sell Gillette Secrets*, BOSTON HERALD, Sep. 26, 1997, at 30.

case of label-maker Avery Dennison Corporation, a former employee pleaded guilty to selling secrets related to Avery's adhesive technology to a company based in Taiwan.[164] The president of a Taiwanese company that manufactures pressure-sensitive products in Taiwan, Malaysia, Singapore, and China[165] was arrested along with his daughter by the FBI. They were charged with mail and wire fraud, money laundering, and receipt of stolen property after they bought trade secrets from an Avery employee who was working with the FBI.[166] Beginning in 1989, the pair was stealing trade secrets that reportedly cost Avery $50 to $60 million in research and development costs.[167]

Retired Eastman Kodak manager, Harold Worden, also pleaded guilty in 1997 to selling trade secrets to Kodak officials who were working undercover, posing as Chinese agents.[168] He agreed to pass on Kodak's formulas, drawings, and blueprints to undercover agents.[169] Because he agreed to cooperate in a continuing investigation, he was able to negotiate a plea bargain which resulted in a one-year prison sentence, including three months of home confinement with a monitoring bracelet, and a fine of $30,000.[170] In sentencing him, U.S. District Judge Telesca denounced him for disclosing trade secrets to "not just any foreign national, but China," a long-time adversary of the U.S. with a poor human rights record.[171]

In a case tried in 1998, two men were arrested by the FBI and charged with attempting to steal the secret formula for Taxol, an anticancer drug developed by the Bristol-Myers

---

164. *See* Frances A. McMorris, *Corporate-Spy Case Rebounds on Bristol*, WALL ST. J., Feb. 2, 1998, at B5.

165. *See* Jerry Seper, *Taiwanese Pair Arrested in Theft of Trade Secrets*, WASH. TIMES, Sep. 7, 1997, at A3. At the time of publication of this Article, the two Taiwanese executives were acquitted of mail fraud but convicted of two charges of economic espionage. *See Taiwanese Executives Are Convicted Under Economic Espionage Act*, IP LAW WKLY., May 13, 1999, at 15; United States v. Yang, No. 1:97 CR 288, 1999 U.S. Dist. LEXIS 6764 (N.D. Ohio April 29, 1999).

166. *See* Seper, *supra* note 165, at A3.

167. *See Taiwan Execs Stole Avery Secrets, U.S. Charges,* L.A. TIMES, Sep. 7, 1997, at D2.

168. *See Business Watch-Legal*, SUN-SENTINEL (FT. LAUDERDALE), Nov. 14, 1997, at D3.

169. *See Spies Step Up Attacks on U.S. Firms*, IRISH TIMES, Jan. 16, 1998, at 60.

170. *See Ex-Kodak Employee Sentenced*, GREENSBORO NEWS & REC., Nov. 15, 1997, at B2A.

171. *Id.* (internal quotations omitted).

Squibb Company.[172] In an interesting turn of events, a federal judge ordered prosecutors to turn over to the defendants and their attorneys the very documents they had allegedly tried to steal because they needed the information to prepare their defense.[173] The court held that certain material be designated as confidential, preventing disclosure to the public, but allowing inspection by defense attorneys and expert witnesses.[174] The court required each person given access to the data to sign a confidentiality agreement.[175] In granting the defendants' proposed protective order, the court held that the right to a fair trial trumps any right to protect trade secret.[176] The Third Circuit reversed the district court's discovery order and remanded the case for a determination on the materiality of the documents.[177] On remand, the district court held that the documents were not material to the defendants' case and did not require the Government to turn them over to the defense.[178] Commentators have noted that if the district court's order had been upheld, many companies would ultimately choose to forego cooperation with the FBI.[179] Although in the end the discovery order was overturned, there still seems to be a question as to whether a similar order could be issued in the future for documents that are deemed material.

Bristol-Myers had cooperated with prosecutors by providing real documents to make the sting operation look authentic.[180] An undercover FBI agent posing as a technology information broker was contacted by a Taiwanese executive based in Taiwan.[181] The executive set up a meeting

---

172. *See* United States v. Hsu, 982 F. Supp. 1022, 1022–23 (E.D. Pa. 1997).

173. *See id.* at 1029–30.

174. *See id.*

175. *See id.*

176. *See id.* at 1025. The Court stated that the government could not be relieved of the burden of proving one of the essential elements of its case: the existence of a trade secret. The government must convince the trier of fact of all the essential elements of guilt beyond a reasonable doubt. Furthermore, the Court found that if it were to restrict the defendants' access to the Taxol technology documents by giving them redacted documents during discovery, it would interfere with their Sixth Amendment right to cross-examination at trial. *See id.* at 1024–25.

177. *See* United States v. Hsu, 155 F.3d 189, 204–05 (3rd Cir. 1998).

178. *See* United States v. Hsu, 185 F.R.D. 192, 198–99 (E.D. Pa. 1999).

179. *See* McMorris, *supra* note 164, at B5. The possibility of such a ruling sends clear warning signals to businesses of the dangers of reporting trade secret theft to the U.S. Attorney's Office for criminal prosecution. *See id.*

180. *See id.*

181. *See id.*

between the agent and Kai-Lo Hsu, an employee of her company.[182] During the meeting, Hsu asked the agent to locate a Bristol-Myers employee willing to sell information on the anticancer drug.[183] Bristol-Myers agreed to provide an employee to pose as a corrupt engineer. Defendants Hsu and Chester S. Ho, a biochemist and professor at a Taiwan university, examined scientific documents that contained some of the trade secrets and discussed the technology with the undercover agent and "corrupt" employee.[184] Reportedly, about $400,000 in cash, stocks of a Taiwanese company, and royalties from the sale of the drug were offered for the information.[185]

Recently, allegations also surfaced that Reuters Holding PLC, the news service whose main source of revenue comes from electronic information, stole trade secrets from its competitor Bloomberg LP.[186] Reuters employees have become increasingly worried about competition and have been under pressure to develop analytical programs to compete with both Bloomberg and Dow Jones & Company to provide information to trading desks of the world's financial houses.[187] FBI agents have been investigating[188] whether Reuters accessed Bloomberg's computer program through a third company that had contracted for Bloomberg products.[189] At least one inside informant assisted in recording a number of executives.[190] A grand jury is looking into whether to indict several of Reuters' employees.[191] As of February 3, 1998, federal prosecutors reportedly had obtained more than 100 written communications between Reuters Analytics, the subsidiary at the heart of the controversy, and the consulting company that might have

---

182. *See id.*

183. *See id.* The request was made after the FBI agent stated that Bristol-Myers would probably not be willing to share the information. *See id.*

184. *See id.*

185. *See id.* (noting that potential losses could amount to billions of dollars over the ten-year period Bristol-Myers holds the patent for the plant cell culture technology).

186. *See* G. Bruce Knecht & Robert Frank, *Reuters Fallout Grows From Bloomberg Probe*, WALL ST. J., Feb. 2, 1998, at B10.

187. *See id.*

188. *See id.*

189. *See id.*

190. *See id.*

191. *See id.* As of July 1999, the United States Attorney's Office had dropped their investigation. A spokesperson for Bloomberg was not willing to comment on the possibility of a civil suit against Reuters. *See* Sarah Stirland, *Federal Investigation Into Reuters Analytics Unit Dropped*, SEC. INDUS. NEWS, July 19, 1999, *available in* 1999 WL 24067137.

been engaged in stealing proprietary codes from Bloomberg.[192] Reuters, which has placed three of its executives on paid leave as a result of the investigation,[193] denies any knowledge of unlawful activity.[194] It also promises "remedial action" if, through its own internal investigation overseen by one of its top London executives, any of Bloomberg's proprietary information is discovered.[195] Clearly, if the news reports are correct, the company and the individuals involved could be prosecuted under the EEA. Indeed, if true, the conduct appears to constitute precisely the type of offense Congress intended to punish by enacting the EEA—a foreign company using espionage to gain a competitive advantage over a smaller American competitor.

All these cases are similar in that they constitute instances of clear-cut theft of trade secrets, often induced by bribes paid to undercover agents working in sting operations, in which the defendants' guilt is flagrant and easily exposed in court.[196] It will be interesting to see whether, with time, the Department of Justice's selection of cases to prosecute remains so careful.

## V. STRATEGIC IMPLICATIONS

### *A. Litigation*

Under the EEA, a party is not charged unless there has been theft of a trade secret,[197] a meaningful disclosure,[198] or a conspiracy to steal or disclose.[199] The recipient must receive information that gives him a material advantage.[200] Recipients must know the trade secrets have been stolen in order to be guilty under the EEA.[201] Criminal defense attorneys can use the fact that guilt under the EEA

---

192. *See FBI Investigating Ex-Bloomberg Worker*, ATLANTA J. & CONST., Feb. 3, 1998, at E7.

193. *See id.* (reporting that a Reuters spokesman would not confirm the third executive being placed on leave); Knecht and Frank, *supra* note 186, at B10.

194. *See* Dean Starkman et al., *Reuters Denies Unit is Probed On a Break-In*, WALL ST. J., Feb. 5, 1998, at A4.

195. *See id.*

196. *See* Mark D. Seltzer & Angela A. Burns, *The Criminal Consequence of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Your Company's Trade Secrets From Theft and Render Civil Remedies Obsolete?*, 12 No. 8 WHITE-COLLAR CRIME REP. 1 (1998).

197. *See* 18 U.S.C.A. §§ 1831(a)(1), 1832(a)(1) (West Supp. 1999).

198. *See id.* §§ 1831(a)(2), 1832(a)(2).

199. *See id.* §§ 1831(a)(5), 1832(a)(4).

200. *See id.* §§ 1831(a), 1832(a).

201. *See id.* §§ 1831(a)(3),1832(a)(3).

necessitates that the recipient be able to use the trade secret. In other words, the one buying the stolen trade secret may not be guilty of trade secret theft if she is unable to derive financial value from it or unable to derive a commercial "headstart" from its use.[202] Showing that the secret has little value and that the theft has not caused damage to the company or the industry may discourage prosecution. Showing a lack of overt acts such as physical removal of information from offices will also decrease the chance of prosecution. Most commentators agree that as long as criminal intent is not readily apparent, prosecution is unlikely. Thus, the typical honest employee need not fear changing jobs even though he may be incidentally taking trade secrets with him.[203] But specific intent on the part of employers may be inferred from a pattern of hiring employees who are highly specialized and privy to competitors' trade secrets.

Under section 1832, the theft, by itself, is not enough. The government has the burden to demonstrate that (1) the agent had the intent to convert the secret to someone's economic benefit, and (2) the agent had knowledge that the offense would injure the owner of the trade secret.[204] It is unclear whether "reckless disregard" or "willful blindness" is enough to prove guilt. Although most prosecutors will likely look at civil trade secret cases for guidance and precedent, the standard of showing criminal intent beyond a reasonable doubt must be satisfied.[205]

Therefore, unless these steps were taken, there is no crime because the information is not a trade secret under the statute's definition.[206] In *United States v. Hsu,*[207] defense lawyers argued that the Taxol technology their clients allegedly attempted to steal did not fall under the definition of a trade secret under the EEA because Bristol-Myers failed to take sufficient steps to protect it from disclosure.[208] They also argued that much of the information was publicly available.[209] Potential defendants could follow similar defense

---

202. *See* Intermedics, Inc. v. Ventritex, Inc., 822 F. Supp. 634, 642 (N.D. Cal. 1993).

203. *See* Schweizer, *supra* note 90, at 15A.

204. 18 U.S.C.A. § 1832(a) (West Supp. 1999).

205. *See* Savage, *supra* note 101, at 17.

206. 18 U.S.C.A. § 1839(3)(A).

207. 982 F. Supp. 1022, 1025 (E.D. Pa. 1997), *rev'd*, 155 F.3d 189, 204 (3rd Cir. 1998).

208. *See* McMorris, *supra* note 164, at B5.

209. *See id.*

theories and argue that the data at issue was unprotected. Showing that it has no economic value is also a valid defense.[210] In fact, if it can be shown in the pre-indictment phase of a case that the information is not worth much, the Department of Justice is not likely to pursue prosecution.[211] Finally, if a protective order is issued, similar to that in *Hsu,* the defense can argue that they and their experts should be able to inspect the confidential material at issue so as to build a defense. As the trial court stated in *Hsu*, the right to a fair trial trumps the rights of a company to protect its trade secrets.[212] Though the strength of such an argument appears to be questionable, reasoning such as this could convince prosecutors to drop cases to prevent trade secrets from being revealed.[213]

### *B. Corporate Compliance*

Many corporations that own trade secrets have spent substantial resources acquiring and developing them, through research and long-term development. Yet many such companies have inadequate protection.[214] Often, it is too late when corporate executives and in-house attorneys become aware of the theft of important documents or information. Some companies doing business abroad do not address the problem of spying because they consider misappropriation of secrets as part of the price of doing business. However, most corporations should take preventive steps by hiring security specialists and attorneys specialized in corporate compliance and intellectual property.

Companies that have a lot invested in their trade advantages should implement long-term programs to protect their trade secrets from misappropriation.[215] These measures are likely to maintain or improve the company's image in the event of a lawsuit, by showing that safeguards were in place, thus elevating the value of the company's maintained trade

---

210. *See* Seltzer & Burns, *supra* note 196.

211. *See* Savage, *supra* note 101, at 17.

212. *See* United States v. Hsu, 982 F. Supp. 1022, 1025 (E.D. Pa. 1997), *rev'd*, 155 F.3d 189, 204 (3rd Cir. 1998) (the order was reversed on grounds that discovery regarding this information was not necessary to sustain the specific defense presented).

213. *See* McMorris, *supra* note 164, at B5.

214. *See* Yates, *supra* note 17, at C1.

215. *See* Greenberg v. Croydon Plastics Co., 378 F. Supp. 806, 812 (E.D. Pa. 1974); Derek P. Martin, Comment, *An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation,* 1993 BYU L. REV. 949, 967 (1993).

secrets.[216] Additionally, under the U.S. Sentencing Commission's guidelines, companies that have a meaningful and efficient compliance program in place are entitled to mitigation in sentencing.[217] Finally, such measures will communicate to researchers and employees that the company greatly values the time and effort they expend in designing innovative products or services and that management is taking responsible steps to protect their innovation as well as the goodwill of the company.

## VI. CONCLUSION

Globalization, increasing competition, and the growing importance of intellectual property have heightened temptations to steal corporate secrets, both by domestic employees and foreign spies.[218] Such misappropriation of trade secrets is costing American corporations billions of dollars annually.[219] The security of these trade secrets is essential to maintaining the vitality of the economy. Prior to the enactment of the EEA, matters of corporate theft were usually handled by private parties through civil litigation. This is no longer the case. The EEA now makes it a federal felony to steal trade secrets.[220] It allows the federal government to prosecute employees and companies, seize assets, and fine organizations up to $10 million.[221]

In an age in which information provides a critical competitive advantage to companies, the EEA might just be the instrument necessary to fight this growing form of espionage. As long as prosecutors apply the EEA selectively, which appears to be the case so far, and courts construe its provisions narrowly, it could effectively address the failures of existing state and federal laws. If the statute is applied broadly, however, and if its legislative intent is not honored, it has the potential to create a chilling effect on the mobility of labor and to produce disastrous results for our economy. Similarly, if courts fail to allow trade secrets to remain sealed and confidential during trial, companies may be hesitant to come forward, report economic espionage, and cooperate with the FBI and federal prosecutors.

---

216. *See* Cundiff, *supra* note 70, at 33–34.

217. *See* Kerr, *supra* note 80, at 29.

218. *See Economic Espionage: Joint Hearing*, *supra* note 13, at 43 (statement of FBI director Louis Freeh).

219. *See* USITC PROTECTION, *supra* note 25, at 4–2.

220. *See* 18 U.S.C.A. §1831 (West Supp. 1999).

221. *See id.*

It is crucial that organizations think ahead and implement corporate compliance programs, both to protect their industrial secrets from theft and to make sure that their own employees are not involved in industrial espionage on behalf of the company. Employers need to explain to their employees that leaking information will result in loss of markets, which will in turn result in loss of jobs. In-house attorneys should be diligent in taking precautions to control the dissemination of confidential information. The benefits of safeguarding precious trade secrets, of avoiding potential prosecutions, and of limiting adverse publicity should greatly outweigh the costs associated with the implementation of compliance programs.