Penn State International Law Review

Volume 16
Number 3 *Dickinson Journal of International Law*

Article 4

5-1-1998

Changing Times, Changing Crimes: The Criminal's Newest Weapon and the U.S.'s Response

George J. Moscarino

Michael R. Shumaker

Changing Times, Changing Crimes: The Criminal's Newest Weapon and the U.S.'s Response

George J. Moscarino and Michael R. Shumaker*

I. Introduction

Every evening's newscast is replete with thefts that are committed with a gun, knife or other lethal weapon. Rarely does the lead news story address the criminal's newest, and perhaps most effective theft weapon: the computer. Granted, a criminal's use of a computer does not strike fear in our hearts the same way a sawed-off shotgun might, but the real monetary damage that can be inflicted by these machines far exceeds any take a criminal could obtain by the use of a shotgun. For example, only recently, a group of Russian computer hackers stole $10 million from Citibank by invading its allegedly secure computer network.[1]

Computer theft offers distinct advantages to the cybercriminal. It allows the criminal to pilfer large amounts of money without having to face locked safes, foreign premises, or, most importantly, armed security guards. A heist can be done safely and efficiently through a few strokes on a computer keyboard. Moreover, while a gun offers a thief protection and control over his victims, a computer eliminates this need and supplements the thief's arsenal with anonymity and an unlimited range of victims. As one commentator accurately stated, "If I want to steal money, a

---

* George J. Moscarino is a Cleveland partner and trial attorney for the international law firm of Jones, Day, Reavis & Pogue. He is a senior member and former Chairman of the Corporate Criminal Investigations Section of the Firm's Litigation Group, a Fellow of the American College of Trial Lawyers, and a former Assistant Attorney General and Assistant County Prosecutor, Ohio. Michael R. Shumaker is an associate in the Litigation Section of Jones, Day, Reavis & Pogue's Litigation Group in Washington, D.C.

1. *Russians Arrest 6 in Computer Thefts*, N.Y. TIMES, Sept. 27, 1995, at D5.

computer is a much better tool than a handgun . . . . It would take me a long time to get $10 million with a handgun."[2]

As the Citibank heist[3] illustrates, a cybercriminal's reach is international and his crimes can often be committed without anyone knowing when it was done, how it was done, or who the culprit was. It is for these and other reasons that theft and fraud offenses committed with the aid of computers and other electronic media will soon become leading international crimes. There are no visa or passport requirements, no security checkpoints, and no physical barriers.[4] Perhaps most importantly, such crimes require little manpower and resources.[5]

Although the Citibank heist involved the stealing of U.S. currency, the modern day criminal is now focusing his computer's attention on stealing something that is oftentimes more valuable: the corporate trade secret. The cybercrook has realized that stealing the next version of the Coca Cola recipe or Windows software is worth more than a $10 million heist. Perhaps more importantly, the trade secret—unlike the $10 million in cash—can be duplicated and downloaded without the true owner ever knowing that the trade secret has been stolen. The owner still has a copy; unfortunately, the cybercrook does too.

To combat this ever-increasing problem, President Clinton recently signed into law the Economic Espionage Act of 1996 (EEA).[6] The law serves a dual purpose: 1) it provides a criminal cause of action against trade secret theft; and 2) it prohibits foreign state-sponsored industrial espionage.[7] Most importantly for the purposes of this article, the EEA explicitly criminalizes the theft of trade secrets through the use of computers and the Internet, a method of misappropriation that fell outside the coverage of pre-existing U.S. laws.[8]

---

2. Jon Swartz, *Modern Thieves Prefer Computers to Guns/ Online Crime Is Seldom Reported, Hard to Detect*, S.F. CHRON., Mar. 25, 1997, at A1 (statement of Daniel Geer, director of engineering for Open Market in Cambridge, Massachusetts).

3. *See Russians Arrest 6, supra* note 1.

4. M.E. Bowman, *International Security in the Post-Cold War Era: Can International Law Truly Effect Global Political and Economic Stability? Is International Law Ready for the Information Age?* 19 FORDHAM INT'L L.J. 1935, 1943 (1996).

5. *Id.*

6. 18 U.S.C. §§ 1831-1839 (1996).

7. *Id.* at 1831-1832.

8. *Id.* The EEA was heavily supported by the U.S. Department of Justice and the FBI, who jointly drafted the first version of the EEA for Congress' consid-

This article will discuss the enormity of the trade secret theft problem, the reasons for its recent explosion, and the role of computers and electronic espionage in that explosion. It will then discuss the EEA, including its individual provisions, and its ramifications for the international legal community.

II. The Computer and Its Use in Trade Secret

A. The Problem

Trade secret theft, or economic espionage as it is often called, commonly occurs in one of two ways: 1) a disgruntled employee misappropriates the company's trade secrets for his own financial benefit or to harm his ex-employer; or 2) a competitor of the company or a foreign nation misappropriates the trade secret in order to advance the competitor's or foreign nation's financial interests.[9] The manner in which these thefts occur ranges from the complex (computer hacking, wire interception, spy devices) to the mundane (memorization, theft of documents, photocopying). But in all instances, the owner—who often has invested hours of hard work and millions of dollars in developing the trade secret—is deprived of the commercial advantage he would have obtained by keeping the trade secret unavailable to his competitors and the public.

The statistics on trade secret theft are startling. One survey estimated that U.S. businesses currently lose $24 billion a year to trade secret theft,[10] and that this could potentially rise to $63 billion a year.[11] A 1994 study estimated the cost as high as $100 billion annually.[12] A 1996 survey of Fortune 1000 firms by WarRoom Research found that 58 percent reported computer break-ins during the previous twelve months, and 18 percent suffered losses exceeding $1 million.[13] As early as 1988, 48

---

eration. Counterintelligence Executive Notes 13-96 (visited 31 October 1996) <http://www.nacic.gov>; *see* H.R. Rep. No. 104-788, at 6 (1996) (inapplicability of federal criminal laws) [hereinafter "House Rep."].

9. *See* House Rep., *supra* note 8, at 6.

10. Counterintelligence Executive Notes 13-96, *supra* note 8 (the 1996 survey was conducted by the American Society for Industrial Security).

11. House Rep., *supra* note 8, at 6.

12. 142 Cong. Rec. S377, at S377 (Jan. 25, 1996) (statement of Sen. Cohen).

13. *See* News Release by WarRoom Research L.L.C. (visited Nov. 21, 1996) <http://www.isecure.com>, at 2 [hereinafter "WarRoom Research"].

percent of 150 research and development companies surveyed by the National Institute of Justice reported that they had been victims of trade secret theft.[14] Finally, the president of Lockheed Martin Corporation informed the United States Congress that a recent survey of international aerospace companies revealed that 100 percent of them believed that a competitor, either domestic or international, had used intelligence techniques against them in an effort to obtain trade secrets.[15]

Whether these figures are accurate or merely the prognostications of doomsayers,[16] one thing is clear: trade secret theft is on the rise. In 1995, the American Society for Industrial Security (ASIS) found that of the 325 companies surveyed, almost half experienced trade secret theft of some sort during the previous two years—an increase of 323 percent from a survey conducted four years earlier.[17] Just prior to the EEA's enactment, Louis Freeh, then Director of the FBI, informed Congress that from 1995 to 1996, the number of economic espionage cases the FBI was investigating doubled from 400 to 800.[18] Similarly, the Computer Emergency Response Team at Carnegie-Mellon University received 132 reports of unauthorized computer access in 1989; in 1995 it received 2412.[19]

B. Why the Explosion in Trade Secret Theft?

1. The Relative Ease of the Theft.—No one reason can be given for the increase in theft. There are many contributing factors and the most notable are discussed below. However, the single

---

14. *Id.*; *see also* William J. Cook, *Industrial Espionage and the Internet*, CHI. LAW., Feb. 1997, at 57.

15. 142 Cong. Rec. S12201-03, at S12212 (Oct. 2, 1996) (statement of Sen. Kohl).

16. One commentator believes the EEA is an overreaction to contrived statistics, and is really designed to employ a largely obsolete intelligence force. Robert Dreyfuss, *Tinker Taylor, Silicon Spy*, CAL. LAW., May 1996, at 37; Robert Dreyfuss, *Spy vs. No-spy: The New Espionage Scare*, NEW REPUBLIC, Dec. 23, 1996, at 9.

17. 142 Cong. Rec. S12201-03, at S12212 (Oct. 2, 1996) (statement of Sen. Kohl).

18. S. Rep. No. 104-359, *available in* 1996 WL 497065, at 20 (1996) [hereinafter "Senate Rep."].

19. Susan E. Davis, *Gangster Tech*, CAL. LAW., June 1996, at 42, 44.

greatest reason for the dramatic increase is undoubtedly the world's ever-expanding use of the computer.

Increasing public use and access to computers has allowed people who harbor criminal intentions to copy sensitive information or to enter confidential areas to which they previously had no access. For example, a disgruntled employee who wants to take the company's most attractive new plan or product to his next employer no longer needs to spend hours clandestinely duplicating documents. He can now download the plans, schematics or documents to a three and a half inch computer disk—a perfect size for his front shirt pocket—in a matter of seconds.[20]

The increase in computer networking and Internet connections also has played a significant part in the growth of trade secret theft. Every time a new computer is linked to a network, or a company network is linked to the Internet, the points of entry through which a hacker may gain access to a company's confidential system are increased. Each new addition increases the chance that someone will not follow the proper security instructions or allow access to an unauthorized user.[21]

To illustrate, suppose you have two houses: one with two doors, and one with ten. It is considerably harder to remember to lock all ten doors at the end of the day than it is to lock up just two. Much the same can be said for the number of connections a computer network has to the outside computer community.

This development has allowed some of the formerly annoying, but relatively harmless computer hackers to become accomplished international criminals. Unethical competitors and some foreign

---

20. A 3.5 inch computer disk can store approximately 720 pages of double-spaced type. Peter J. Toren, *Internet: A Safe Haven for Anonymous Information Thieves?*, 11 ST. JOHN'S J. LEGAL COMMENT. 647, 648 n.5 (1996). As one commentator summarized the problem:

> An employee can download trade secret information from a company's computer to a diskette, transfer the information to the hard drive of a home computer and then upload it to the Internet, where it can be transmitted worldwide within minutes . . . Within days, a U.S. company can lose complete control over its trade secrets forever.

R. Mark Halligan, *Intellectual Property*, NAT'L L.J., Dec. 9, 1996, at B6; *see also* Senate Rep., *supra* note 18, at 18.

21. Davis, *supra* note 19, at 44; Richard Behar, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 56, 58 (". . . every technology manager knows: The more the computers of the business world become interconnected—via the Internet and private networks—the more exposed they are to break-ins.").

nations now employ these hackers to take advantage of the chinks in certain companies' computer armor.[22] Consequently, it is no longer necessary to trespass on corporate turf to steal a competitor's confidential information.[23]

This fact is further exacerbated by the ease with which these hackers can break into the systems. Although companies routinely respond to these threats with ever-increasing computer security measures, the hackers have developed an impressive array of techniques that singularly or in tandem allow for a stunningly high degree of success. The names given these techniques sound like something out of a James Bond movie. They include: spoofing,[24] sniffing,[25] social engineering,[26] demon dialing,[27] dumpster diving,[28]

---

22. *See* Behar, *supra* note 21, at 58.

23. Behar, *supra* note 21, at 58.

24. "IP Spoofing" is a technique in which the hacker convinces one computer on a network that his computer is friendly and authorized to enter the system. This is done by manipulating the internet protocol ("IP") address—the digital information that the host computer reads to determine access—on the requesting computer. *See generally* Lou Dolinar, *Spoofing Lets Hackers Hijack Computers, Officials Warn*, NEWS TRIB. (Tacoma, Wash.), Jan. 24, 1995, at B5; Jeffrey Young, *Spies Like Us*, FORBES, June 3, 1996, at 70, *available in* 1996 WL 15115548, at 15 ("spoofing").

25. "Sniffing" involves the use of certain computer network monitoring tools to eavesdrop on the electronic messages traversing a computer network. By doing so, the hacker can learn a variety of information (depending on the system's security) such as the IP addresses the network is accepting. As one commentator put it, the electronic messages are like postcards and the sniffer merely reads them for the hacker searching for clues to entry. Vicki Tardif, *Sniffers and Spoofers*, Internet World (visited December 1995) <http://www.internetworld.com>; Behar, *supra* note 21, at 66.

26. "Social engineering" is "hacker-speak for tricking workers into offering information that will help during break-ins." Behar, *supra* note 21, at 66. It is still the most common method used to gain access to a secure computer system. Davis, *supra* note 19, at 44.

27. "Demon" or "war dialing" involves sequential dialing of telephone numbers within a set range to determine which phone lines are hooked up to active computer modems. By going directly to the individual computers, hackers avoid the security system set up by the company to filter Internet traffic (often termed a "firewall"). Once identified, the hacker focuses on those computers for possible infiltration. Behar, *supra* note 21, at 59; Winn Schwartau, *Hackers, Sniffers, Worms and Demons*, INFORMATION WEEK, May 16, 1994, at 39, *available in* 1994 WL 3323412, at 12.

28. "Dumpster diving" occurs when a hacker sifts through a company's dumpster at night to find valuable information that may assist in future hacking efforts. Swartz, *supra* note 2.

and pinging.[29]

One of the most exotic tools used by the hacker is the so-called Van Eck device, which is named after the Dutch scientist who invented it.[30] This device allows anyone to pick up emissions from a computer screen from as far as two kilometers away.[31] This device was reportedly used to capture CIA double-agent Aldrich Ames.[32]

The fact that the computer equipment needed to implement these techniques costs relatively very little adds further fuel to the fire. As one commentator opined, computer crime has exploded because the "tools have gotten so good and so cheap."[33] To make matters worse, these hacker techniques, and the software needed to implement them, are often available for free on the Internet.[34]

2. The Extremely Profitable Nature of the Theft.—The relative ease with which a trade secret can be stolen using a computer is perhaps exceeded only by the size of the windfall that can be obtained. Once inside a secure computer system, what or how much a person takes is often entirely up to them. "Now taking $100 million dollars is no harder than taking ten dollars. It just depends on where the decimal point is."[35]

Trade secrets, however, are often more valuable than U.S. currency. In one case, computer hackers breached the internal network of Interactive Television Technologies, the creators of a device that lets consumers access the Internet using their television set. Once in, the hackers then stole trade secrets worth $250 million.[36] Interactive Television Technologies is now out of business.[37]

Similarly, computer hackers broke into a U.S. automobile manufacturer's secure computer network during the summer of

---

29. "Pinging" uses a software program to send an electronic signal to every computer address for a given company to determine whether the computer is up and alive. Obviously, the alive computers are then targeted for infiltration. Behar, *supra* note 21, at 59.

30. *Id.* at 70.

31. *Id.* A high quality Van Eck device can be purchased for US $4,000. *Id.*

32. *Id.* at 66.

33. Davis, *supra* note 19, at 44.

34. Behar, *supra* note 21, at 66; Davis, *supra* note 19, at 44.

35. Davis, *supra* note 19, at 60.

36. Swartz, *supra* note 2, at A1.

37. *Id.*

1991, and stole confidential designs for future cars.[38] These designs ultimately ended up in their competitors' hands, and the company estimated it lost $500 million from the intrusions.[39]

3. Anonymous Nature of Computer Theft.—Not only is computer trade secret theft easy and profitable most of the offenses go undetected. The FBI estimates that as many as 95% of computer intrusions go undetected.[40] The sophisticated computer hacker simply knows how to construct his activity so that no one detects his infiltration of the system.[41] As one commentator stated, computer theft is often anonymous: "Just loop your message through a couple of different servers, including one that makes your return address 'anonymous,' and bingo, you're in business."[42]

The anonymous nature of computer theft is one of its greatest attractions. Experts have found that the anonymity softens or even erases the intruder's guilty feelings.[43] A business executive may be reluctant to break into his competitor's offices and copy their trade secrets, but may not be so reluctant to do it in the safety of his den. As a result, computers have created a completely new class of criminal. Many white-collar executives have discovered, "[i]f you want to get away with a crime today, do it using a computer."[44]

4. Difficulties in Prosecution.—Prior to the EEA's passage, prosecution of trade secret theft was rare. This was primarily due to the unwillingness of prosecutors to take on complex criminal cases where an intimate knowledge of computers was a prerequisite, and corporations' unwillingness to report the theft of their trade secrets.

Prosecutors were especially unwilling to take on these cases since the criminal statutes available to them were not well-suited

---

38. Schwartau, *supra* note 27, at 4.
39. *Id.*
40. Behar, *supra* note 21, at 59.
41. "Spoofing" and "sniffing" are almost impossible to detect. *See* Schwartau, *supra* note 27, at 4 ("sniffing"); Young, *supra* note 24, at 15 ("spoofing").
42. Davis, *supra* note 19, at 45.
43. Young, *supra* note 24, at 2-3.
44. *Id.* at 20.

for such crimes.[45] Federal prosecutors primarily relied on the National Stolen Property Act (NSPA),[46] and the mail and wire fraud statutes.[47]

The NSPA was designed to prevent criminals from evading state prosecution by fleeing across state lines. Prosecution under the Act requires proof that "goods, wares or merchandise" were transported in foreign or interstate commerce.[48] Unfortunately, some U.S. courts have held that the theft of "purely intellectual property" does not constitute the theft of "goods, wares or merchandise" as required by the statute.[49]

The chief problem with the U.S. federal mail and wire fraud statutes—which prohibit any scheme involving the use of the mail or wires to obtain property by false pretenses—is the need to prove a "scheme to defraud." Since a trade secret thief often only copies information, he does not necessarily "defraud" the company permanently of the information. Moreover, much trade secret theft occurs without the use of the mail or wires.[50]

Probably the greatest reason why trade secret theft is not prosecuted more often is the failure of victim companies to report such thefts to government authorities.[51] Companies are reluctant to report such crimes because of concern over a loss of public trust and public image.[52]

For many companies, security and control over their operations and assets are vital to their success, and thus reporting breaches in that security is potentially damaging to future business. As one commentator stated, "Who wants to do business with a company whose unstable network security is being splashed across the front page?"[53] For example, Citibank's reward for reporting the $10 million stolen from its allegedly secure computer network was seeing its top twenty customers "wooed by rival banks, all claiming

45. House Rep., *supra* note 8, at 6.
46. 18 U.S.C. §§ 2314-2315 (1970 & Supp. 1997).
47. *Id.* §§ 1341, 1343.
48. United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991).
49. *See id.*; Dowling v. U.S., 473 U.S. 207, 227 (1985); *see generally* Halligan, *supra* note 20, at B6.
50. Senate Rep., *supra* note 18, at 27.
51. Swartz, *supra* note 2, at A1.
52. *Id.*
53. *Id.*

their computer systems were more secure."[54] Companies also are reluctant to report such thefts because they can spawn unwanted SEC attention and shareholder derivative suits.

5. Foreign Economic Espionage.—Another reason for the increase in trade secret theft is the changing nature of foreign espionage. The world's nations have realized that economic superiority now ranks in importance with military superiority. As the legislative history to the EEA states: "Typically, espionage has focused on military secrets. But as the cold war has drawn to a close, this classic form of espionage has evolved. Economic superiority is increasingly as important as military superiority. And the espionage industry is being retooled with this in mind."[55]

The statistical numbers reflect this shift. Louis Freeh, former director of the FBI, informed Congress that the FBI was investigating reports and allegations of economic espionage conducted by twenty-three different countries against U.S. companies.[56] The list included countries that were typically hostile to U.S. interests, but also included long-time allies of the United States.[57] The FBI also reported that at least seven nations are training their intelligence agents how to hack into U.S. computers for trade secrets.[58] In probably the most often cited example of foreign economic espionage, a former director of the French secret service publicly admitted that he directed French intelligence agents to search the Paris hotel rooms of visiting foreign businessmen for confidential trade secrets.[59]

---

54. Behar, *supra* note 21, at 64.

55. House Rep., *supra* note 8, at 5; *see also* Senate Rep., *supra* note 18, at 20; Behar, *supra* note 21, at 64.

56. House Rep., *supra* note 8, at 5; Senate Rep., *supra* note 18, at 20; Behar, *supra* note 21, at 64.

57. The list included: China, Canada, France, India and Japan. Behar, *supra* note 21, at 64.

58. *Id.*

59. Jim Landers, *Foreign Spies Target Corporate Secrets*, DALLAS MORNING NEWS, Oct. 7, 1996, at 1D; *see* Statement of Senator Cohen, *supra* note 12, at 377.

III. The U.S.'s Response: Enactment of the Economic Espionage Act

A. The EEA's Focus on Trade Secret Theft By Computer

Although the EEA was passed to criminalize all trade secret theft and foreign economic espionage, a clear focus of the Act was theft via the computer.[60] As President Clinton's Statement in support of the Act reports, the EEA was designed to "protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secret theft and deter and punish those who intrude into, damage or steal from computer networks."[61] The legislative history to the Act further underscores the importance of computers in trade secret thefts:

> As this Nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow. Ironically, the very conditions that make this proprietary information so much more valuable make it easily stolen. Computer technology enables rapid and surreptitious duplications of the information. Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner.[62]

B. The Individual Provisions of the Economic Espionage Act

1. Trade Secret Theft - General Prohibition.—With computer trade secret theft in mind, section 1832 of the EEA prohibits anyone who, "with intent to convert a trade secret," "knowingly" steals or otherwise misappropriates a trade secret for "the economic benefit of anyone other than the owner," if the trade secret is

---

60. The Senate Report on the EEA states that the Act covers "a variety of behavior-from the foreign government that uses its classic espionage apparatus to spy on a company, . . . to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics." Senate Rep. *supra* note 18, at *8. It concludes that "[a]ll of these forms of industrial espionage are troubling, and they are punished as the theft of proprietary economic information in this measure." *Id.*

61. Statement by President William J. Clinton Upon Signing H.R. 3723, 142 Cong. Rec. 4034, at 4034-35 (1996).

62. House Rep., *supra* note 8, at 5.

"related to or included in a product that is produced for or placed in interstate or foreign commerce."[63] The Act expressly applies to any individual who without authorization "copies, duplicates, . . . photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, or conveys such information."[64] Of course, the inclusion of "downloads" and "uploads" in the statutory language unambiguously reveals the EEA's explicit focus on unwanted computer intrusions. The Act also prohibits the more classical manner of theft: one who "steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice or deception obtains such information."[65]

Like most U.S. theft statutes, the EEA also criminalizes anyone who knowingly "receives, buys or possesses" the stolen trade secret knowing it has been obtained without authorization;[66] or who conspires with anyone to commit any of the offenses described above.[67] The maximum penalty for a violation of this section is a $250,000 fine[68] and imprisonment of 10 years for individuals,[69] and a $5,000,000 fine for offending organizations.[70]

It is also noteworthy that the general prohibition against trade secret theft requires the "intent to convert a trade secret."[71] Thus, a computer hacker who infiltrates a secure computer system and destroys or tampers with a particular trade secret cannot be prosecuted under the EEA.[72] A separate U.S. federal statute criminalizes this behavior.[73]

2. Foreign Economic Espionage - General Prohibition.— Section 1831 essentially takes the conduct prohibited by section 1832 and adds a foreign component to it. Specifically, if a trade

---

63. 18 U.S.C. § 1832 (1996) (the authors have restructured the language of the provision to allow for a more simplistic and logical reading).
64. *Id.*
65. *Id.* § 1832(a)(1).
66. *Id.* § 1832(a)(3).
67. *Id.* § 1832(a)(5).
68. 18 U.S.C. § 3571(b)(3) (Supp. 1997).
69. 18 U.S.C. § 1832(a) (1996).
70. *Id.* § 1832(b).
71. *Id.* § 1832(a).
72. *See* James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L. J. 177, 192 (1997).
73. The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(4) (Supp. 1997).

secret is stolen or misappropriated in any of the manners described above and the offense is done with intent to, or knowing it will, "benefit any foreign government, foreign instrumentality, or foreign agent,"[74] the offender may be fined $500,000 and imprisoned for up to 15 years.[75] The increased penalties that accompany a violation of the provision indicate the importance that Congress attaches to criminalizing foreign economic espionage.

A "foreign instrumentality" is defined to include any "association . . . or . . . legal, commercial or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government."[76] Because there are still no reported decisions under the EEA, there is little guidance on what amount of control by a foreign government is necessary for a foreign company to be considered a foreign instrumentality. It is safe to say, however, that no set percentage of ownership will protect a foreign company from coverage under the EEA if its operations or procedures are in some manner controlled or directed by a foreign government.[77]

3. Protection in the Trade Secret Definition.—A great deal of the EEA's coverage depends on the definition of a "trade secret."

> The definition includes "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if— (1) the owner thereof has taken reasonable measures to keep such information secret; and (2) the information derives independent economic value, actual or potential,

---

74. 18 U.S.C. § 1831(a).
75. *Id.*
76. *Id.* § 1839(1).
77. The legislative history states:

> We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.

142 Cong. Rec. S10882, at S10885 (Sept. 18, 1996) (statement of Sen. Kohl).

> from not being generally known to, and not being readily ascertainable through proper means by, the public."[78]

Congress in the EEA instructed the courts to read this definition broadly.[79]

a. "Reasonable Measures."—The requirement that "reasonable measures" be implemented before certain information qualifies as a "trade secret" under the EEA places a considerable onus upon the owner of the trade secret. Since there have not yet been any reported decisions under the EEA, what qualifies as "reasonable measures" is somewhat elusive. However, the legislative history does give some guidance. The drafters did not wish "to impose any requirements on companies or owners."[80] Rather, "[e]ach owner must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be."[81] The drafters further opine that "what constitutes reasonable measures in one particular field of knowledge or industry may vary significantly from what is reasonable in another field or industry."[82]

At minimum, the drafters suggest that only those who need access to the trade secret should be granted access and that the owner indicate in some way that he considers the information confidential and proprietary.[83] No "heroic or extreme measures" are necessary.[84]

b. "Independent Economic Value."—The second prong of the "trade secret" definition is also noteworthy because it only mandates that the information have "independent" economic value by its status of not being generally known to the public at large. In contrast, the definition of a "trade secret" under the Uniform

---

78. 18 U.S.C. § 1839(3).
79. Chaim A. Levin, *Trade-Secret Thieves Face Fines, Prosecution*, NAT'L L.J., Jan. 27, 1997, at C12, C13; House Rep., *supra* note 8, at 12.
80. 142 Cong. Rec. S12201-03, at S12212, S12213 (Oct. 2, 1996) (managers' statement) [hereinafter "Managers' Statement"].
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*

Trade Secrets Act[85]—the definition on which the EEA's definition is based—requires proof of "independent economic value," and that the stolen information has economic value to the individual who misappropriated it.[86] The EEA definition is an easier standard to satisfy since it eliminates the need to establish the accused's subjective state of mind with respect to the information's value.

c. General Knowledge Is Not Covered.—The trade secret definition holds considerable significance for those individuals who fear they may be prosecuted under the EEA for merely applying the general knowledge they acquired in a previous position to their latest job. There was considerable debate on this matter during the drafting of the EEA and it was the drafters' intention that any ill-advised prosecution of such individuals be foreclosed.[87] As the legislative history states, employees "who change employers or start their own companies should be able to apply their talents without fear of prosecution."[88]

By requiring the owner of a trade secret to take proactive, "reasonable measures" to protect information that it deems a "trade secret," nomad employees gain a valuable affirmative defense to any attempted prosecution under the EEA. The EEA affirmatively places the burden on the procecutor to prove, beyond a reasonable doubt, that it took the appropriate "reasonable measures" and that the employee is not merely applying their

---

85. Unif. Trade Secrets Act § 1(4) (1990). The Uniform Trade Secrets Act, which creates a separate, civil cause of action for trade secret theft, has been adopted, in whole or in part, by 42 states. UNIF. TRADE SECRETS ACT (Supp. 1996).

86. *Id.* § 1(4)(i) (requiring those who misappropriate the information to be able to "obtain economic value from its disclosure or use" in order for it to qualify as a trade secret).

87. Managers' Statement, *supra* note 80, at S12213.

88. *Id.* In the Manager's statement supporting the EEA, a Pennsylvania Supreme Court decision is quoted to emphasize this concern:

> It is not a phenomenal thing in American business life to see an employee, after a long period of service, leave his employment and start a business of his own or in association with others. And it is inevitable in such a situation, where the former employee has dealt with customers on a personal basis that some of those customers will want to continue to deal with him in that new association. This is . . . natural, logical and a part of human fellowship . . . .

Id. The Manager then concludes that "[t]his legislation does not criminalize or in any way hamper these natural incidents of employment." *Id.*

general knowledge obtained during their previous employment with the claimed owner of the trade secret.

The fact that the EEA requires some identifiable piece of information to be stolen also provides employees who frequently change employers some protection from prosecution. As the legislative history states, "[i]t is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ" and that the individual is inappropriately using such knowledge.[89] Unlike the "reasonable measures" provision, however, the protection granted the employee will depend upon the employee proving that the product being challenged was the result of accumulated experience and knowledge, rather than the theft of a trade secret. This is because the owner will likely be able to show some link between the employee's past work and the trade secret allegedly stolen, thereby shifting the burden to the defendant employee.

d. The "Product" Requirement.—Although the definition of a trade secret under the EEA is intentionally broad, it is actually narrow in one important respect. In order for a trade secret to be protected under the EEA, it must be "related to or included in a product that is produced for or placed in interstate or foreign commerce."[90] In limiting the EEA's application to products sold in commerce, the drafters of the statute appear to have excluded the possibility of prosecuting an individual for misappropriation of trade secrets that are related to services, or information discovered, but not used by a company, both of which qualify as trade secrets under the Uniform Trade Secrets Act.[91]

e. "Reverse Engineering" and "Parallel Development" Are Not Prohibited.—Two valid defenses to an alleged violation of the EEA are that the information was obtained through "reverse engineering" or "parallel development." Neither are prohibited by the EEA.[92] "Reverse engineering" involves the taking apart and subsequent reconstruction of the product to determine how it was

89. *Id.*
90. 18 U.S.C. § 1832(a).
91. Pooley, *supra* note 72, at 200.
92. U.S. Dep't. of Justice, Federal Prosecution of Violations of Intellectual Property Rights, May 1997, at 80-81.

made or what components were used.[93] "Parallel development" involves the discovery or creation of an alleged trade secret through one's own research and hard work. The owner of a trade secret does not have an absolute monopoly on the information or data that comprises the trade secret.[94]

3. Confidentiality.—One of the chief deterrents to companies bringing civil suits against individuals who have stolen a trade secret has historically been the increased exposure such a lawsuit brings to the trade secret. More specifically, by bringing the lawsuit, the company highlights the trade secret for the broader public, including its competitor who may be a named defendant, and thus often does more damage than good.

To combat this problem, the EEA includes a provision instructing the court to "enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets" consistent with the applicable federal rules of procedure.[95] The legislative history further instructs that when considering the matter, the court should "always assume that the material at issue is in fact a trade secret."[96] This provision does not necessarily give the court any power that it did not already have, but it certainly makes the court more cognizant of the issue.

4. Victim Compensation.—Although the EEA is a federal criminal statute, one of Congress' concerns in passage was ensuring that victims of trade secret theft receive adequate compensation for their losses. There are two ways (outside a civil proceeding) that a victim can obtain compensation for losses incurred through the theft of a trade secret: 1) forfeiture; and 2) restitution.

a. Forfeiture.—Section 1834 of the EEA expressly provides for forfeiture of both the proceeds and assets used to facilitate a violation of the EEA. Specifically, it states that any person who violates the EEA shall forfeit 1) "any property

---

93. Pooley, *supra* note 72, at 195.

94. U.S. Dep't of Justice, Federal Prosecution of Violations of Intellectual Property Rights, May 1997, at 80.

95. 18 U.S.C. § 1835.

96. Managers' Statement, *supra* note 80, at S12213; *see also* 142 Cong. Rec. S10882, at S10886 (Sept. 18, 1996).

constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation;" and 2) "any of the person's property used, or intended to be used . . . to commit or facilitate the commission of such violation."[97] This includes any profit the individual or company obtained from use of the trade secret and any computer hardware and other instrumentation that a person might use to intrude into a secure system. Whether to award forfeiture is subject to the court's discretion, "taking into consideration the nature, scope, and proportionality of the use of the property in the offense."[98] All fines are for the benefit of the government.[99]

After identifying the property that can be forfeited, the EEA expressly incorporates the Comprehensive Forfeiture Act of 1984, the existing federal law on distribution of forfeited property.[100] Under this law, any party who believes they have an interest in the forfeited property may petition the court "for a hearing to adjudicate the validity of his alleged interest."[101] The party's petition must set forth the bases for their claim to the forfeited property and be signed under penalty of perjury.[102] At the hearing, the petitioning party may testify, present evidence and witnesses, and cross examine all witnesses who appear,[103] and must prove their "right, title or interest" in the property by a preponderance of the evidence.[104] Victims are afforded priority in forfeiture proceedings due to the U.S. Department of Justice's policy of providing restitution to crime victims.[105] Fines are exclusively paid to the federal government.[106]

b. Restitution.—In addition to the EEA's forfeiture provisions, victims may also seek restitution under the Victim and

97. 18 U.S.C. § 1834(a).
98. *Id.*
99. *The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings Before the Subcomm. on Economic and Commercial Law*, 102nd Cong., 245 (1992).
100. 18 U.S.C. § 1834(b).
101. 21 U.S.C. § 853(n)(2) (Supp. 1997).
102. *Id.* § 853(n)(3).
103. *Id.* § 853(n)(5).
104. *Id.* § 853(n)(6).
105. Managers' Statement, *supra* note 80, at S12213.
106. *Id.*

Witness Protection Act that was passed by Congress in 1982.[107] This law generally compels the federal judge who is sentencing a criminal defendant to consider the effect and impact of the defendant's crime on the victim.[108] Restitution is proper for all federal criminal offenses. Thus, if an individual or entity is the victim of trade secret theft, and the federal authorities convict the defendant, the victims may be entitled to restitution.[109]

Restitution may not be ordered, however, if the court "determines that the complication and prolongation of the sentencing process resulting from the fashioning of an order of restitution outweighs the need to provide restitution to any victims . . . ."[110] Consequently, an order of restitution is by no means a sure thing for the victims.[111]

If properly implemented, the forfeiture and restitution provisions can make victims of trade secret theft whole, thereby eliminating the need for an injured party to bring a civil action.[112] This would save the injured party significant court and attorneys' fees, and minimize the potential for further exposure of the stolen trade secret. Nonetheless, a prudent victim should consider filing a civil action to protect their claim and forestall any attempt by the defendant or other interested party to argue that the trade secret was either abandoned or has somehow become general knowledge. In other words, it is a good idea for victimized companies to get

---

107. Pub. L. No. 97-291, 96 Stat. 1248 (originally codified at 18 U.S.C. §§ 1512-1515, 3146(a), 3579, 3580 (1982)).

108. *See* Lawrence P. Fletcher, Note, *Restitution in the Criminal Process: Procedures for Fixing the Offender's Liability*, 93 YALE L.J. 505, 509 n.18 (1984).

109. 18 U.S.C. §§ 3663, 3664 (1994). "The restitution provisions are intended to aid crime victims by requiring convicted defendants to compensate their victims to the greatest extent possible, thus achieving the 'ultimate justice.'" Lorraine Slavin and David J. Sorin, *Congress Opens a Pandora's Box—The Restitution Provisions of the Victim and Witness Protection Act of 1982*, 52 FORDHAM L. REV. 507, 508 (1984) (citing 128 Cong. Rep. H8207 & H8209 (daily ed. Sept. 30, 1982) (remarks of Rep. Fish and Rep. McCollum)).

110. 18 U.S.C. § 3663(d) (1985 & Supp. 1997).

111. *See generally* George J. Moscarino & Michael R. Shumaker, *Beating the Shell Game: Bank Secrecy Laws and Their Impact on Civil Recovery in International Fraud Action*, 1 J. MONEY LAUNDERING CONTROL 42, 45 (1997) (discussing problems raised by qualification).

112. Some companies may be hesitant to make forfeiture or restitution claims because they invite unwanted scrutiny of company operations and their trade secrets.

their foot in the courthouse door so that they can preserve their rights and options.

6. Civil Proceedings to Enjoin Violations.—In an effort to provide protection for victims as soon as trade secret theft is discovered, the EEA authorizes the U.S. Attorney General to bring a civil action to "obtain appropriate injunctive relief against any violation" of the EEA.[113] No criminal indictment need be on file at the time.[114] This provision allows the government to enjoin a victim from using the trade secret to his advantage while an investigation or prosecution takes place.

C. Application of the EEA to International Conduct

The territorial reach of the EEA is intentionally broad and includes a provision that explicitly addresses "conduct outside the U.S."[115] This provision rebuts "the general presumption against the extraterritoriality of U.S. criminal laws" and makes "it clear that the Act is meant to apply to the specified conduct occurring beyond U.S. borders."[116] It is designed to provide the Justice Department "with broad authority to prosecute international theft and will prevent willful evasion of liability for trade secret misappropriation by using the Internet or other means to transfer the trade secret information outside the country."[117]

The EEA contains a number of jurisdictional hooks to accomplish this goal. The EEA applies to "conduct occurring outside the United States" if 1) the offender is a citizen or permanent resident alien of the United States; 2) the offender is an organization organized under the laws of the United States or any state or political subdivision of the United States; or 3) "an act in furtherance of the offense was committed in the United States."[118]

The first two standards are easy to apply, but the third will likely engender diverging opinions of the proper jurisdictional scope of the EEA. To illustrate, suppose a computer hacker in

---

113. 18 U.S.C. § 1836.
114. Halligan, *supra* note 20, at B6.
115. 18 U.S.C. § 1837.
116. House Rep., *supra* note 8, at 14.
117. Halligan, *supra* note 20, at B6.
118. 18 U.S.C. § 1837.

France uses IBM's computer network in New York to break into a company's system in Canada. Was an "act in furtherance of the offence" committed in the United States such that jurisdiction exists?

This jurisdictional puzzle is particularly perplexing given the manner in which the Internet works. The Internet is not one computer "superhighway" as some mistakenly believe; there is no centralized storage location for information, no central control point, and no singular communications channel.[119] Rather, the Internet is hundreds of thousands of computer networks linked together. For example, if someone sends an e-mail message from London to Madrid, that message may pass from London to Madrid via a Paris computer network on one occasion, and from London to Madrid via a New York computer network on another. Suppose someone in France uses the Internet to steal the trade secret of a Canadian company and the Internet—unbeknownst to the thief—uses a computer network in the United States to complete the computer-instructed request. Was an act committed in the United States such that jurisdiction exists?

These scenarios raise interesting questions, illustrate the potential breadth of the EEA, and portend significant jurisdictional battles under the EEA. Nonetheless, two instructive points can be safely made. First, the greater the value of the trade secret stolen or harm to the U.S.'s interests, the more likely a court will allow a prosecutor to stretch the court's jurisdictional arm in order to prosecute a foreign thief. Even the most zealous prosecutor will not attempt a risky prosecution if the injury or harm is relatively ordinary. Second, it is unlikely that a prosecutor will attempt to assert jurisdiction over conduct that is only marginally connected to the United States at this point in the EEA's young life. The Attorney General has promised Congress that it will clear all prosecutions under the EEA at the highest levels of the Justice Department[120] and will report back to Congress on the results in

---

119. *See* William A. Hodkowski, Comment, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 COMPUTER & HIGH TECH. L. J. 217, 222 (1997).

120. Statement of Senator Kohl, NEW REPUBLIC, Feb. 24, 1997, at 4. An earlier version of the EEA required the Attorney General to authorize all prosecutions under the EEA. This provision was subsequently deleted when Attorney General Janet Reno promised Congress that the Department of Justice would promulgate regulations to the same effect. Jonathan Band & William

two years.[121] Thus, it is a safe bet that the U.S. Attorney General's office will select only those cases that they are sure to win or at a minimum sure to gain favorable precedent.[122]

III. Conclusion

Without question, the commission of sophisticated electronic crimes has been greatly facilitated by global technology and computerized information systems. The detection and ultimate prosecution of such crimes have similarly changed. Criminal and civil trials worldwide increasingly feature the use of electronic media to produce both live and graphic evidence to assist courts and juries to understand the often complex evidence of fraud. Computer e-mail messages, the interception of cellular telephone communications, and pager records are also valuable, accessible evidence of incriminating conversations and communications that were unavailable only a few years ago.

The passage of the Economic Espionage Act marks a significant milestone in the prosecution of global economic crime. U.S. and foreign citizens, as well as foreign governments, who attempt to steal their way into unearned profits now face substantial monetary penalties and jail time. The use of the EEA will also greatly increase the likelihood that victims will obtain just compensation for their injuries and will further allow courts to insure the confidentiality of U.S. companies' most valuable economic assets, their private and valuable trade secrets. Finally, the international cyber-criminal who specializes in surreptitious computer theft can no longer feel secure that his conduct will go undetected or that he can escape liability because he is not a U.S. citizen or not physically located in the United States.

Leschensky, *New US Law Hits at Foreign Theft of Trade Secrets*, Intellectual Property Worldwide (visited Feb. 1997) <http://www.ipww.com.>.

121. 142 Cong. Rec. S10882, at S108886 (Sept. 18, 1996) (statement of Sen. Kohl); Victoria Slind-Flor, *New Spy Act to Boost White-Collar Defense Biz*, NAT'L L.J., July 28, 1997, at A1, A18.

122. As one commentator stated, "[t]he government will take only the lay-down cases where there is no question that they're going to win." Slind-Flor, *supra* note 121, at A1, A18.