6-1-1999

The Economic Espionage Act: Setting The Stage For A New Commercial Code Of Conduct

Kent B. Alexander

Kristen L. Wood

Follow this and additional works at: http://readingroom.law.gsu.edu/gsulr

Part of the Law Commons

Recommended Citation

Available at: http://readingroom.law.gsu.edu/gsulr/vol15/iss4/2

This Article is brought to you for free and open access by the Publications at Reading Room. It has been accepted for inclusion in Georgia State University Law Review by an authorized editor of Reading Room. For more information, please contact jgermann@gsu.edu.
THE ECONOMIC ESPIONAGE ACT: SETTING THE STAGE FOR A NEW COMMERCIAL CODE OF CONDUCT

Kent B. Alexander†
Kristen L. Wood‡

INTRODUCTION

The Economic Espionage Act† (EEA or the Act) recasts federal criminal intellectual property law by creating a new set of tools for owners to protect their trade secrets and a new set of penalties against those who would steal them. The Act is the first federal law to criminalize the theft of non-government trade secrets, but, as the name suggests, the Act also addresses espionage by foreign governments and agents. Although the Act

† Kent Alexander is a Partner at King & Spalding law firm in Atlanta, Georgia. He served as the Presidentially-appointed United States Attorney for the Northern District of Georgia from 1994 to 1997. As an Assistant United States Attorney, from 1985 to 1992, he prosecuted the Legion of Doom case, one of the first computer hacker cases in the country.

‡ Kristen Wood is an Assistant District Attorney in DeKalb County, Georgia. From 1995 to 1999, she was an Associate at King & Spalding and a member of the Special Matters Team, specializing in white collar criminal defense and government investigations. From 1994 to 1995, Ms. Wood was a Judicial Clerk for Judge J.L. Edmondson, of the Eleventh Circuit Court of Appeals.

in its current form ultimately may not trigger an overwhelming number of prosecutions, it will undoubtedly have lasting value in helping to develop a written and de facto commercial code of conduct that heightens the protection of trade secrets.

Enacted in October 1996, the EEA remains in its embryonic stages. There have been few prosecutions to date, and the technologies to which the Act applies are constantly evolving. Although one cannot accurately gauge the full impact and effectiveness of the EEA until the courts further develop the case law under the Act, some educated guesses can be made about the effects and scope of the EEA based on the following: limited prosecutions to date; traditional applications of criminal law; and the Authors’ experiences on both the government and defense sides of federal prosecutions.

After first exploring the background and elements of the Act, this Article examines the nature of government resources devoted to enforcement of the EEA, how the resources are used, and how these factors are likely to affect the type and number of EEA prosecutions. Based on this background, the Article then provides practical suggestions and insights into how to avoid the pitfalls of the EEA, how to use the EEA to protect oneself from economic espionage and trade secret theft, and how to work with the government if you or your client becomes a victim of espionage or theft of trade secrets and decide to seek prosecution. Finally, the Article posits that the most immediate and possibly long term value of the Act will be to provide a deterrence tool for private industry to use in preventing trade secret thefts in the Information Age of the new Millennium.

3. See infra note 104 (listing eleven prosecutions in first two years since EEA’s enactment).

4. See, e.g., Caryl Ben Basat & Julian D. Nihill, International Legal Developments In Review: 1996 Business Transactions and Disputes—Part I, The Economic Espionage Act of 1996, 31 Int’l LAW. 245, 248 (1997) ("[T]he responsibility for developing and refining [the EEA’s] parameters will fall on the federal courts over the next few years."). The case law may be slow to develop, however, as most of the cases will plead. Issues arising under the United States Sentencing Guidelines will likely be the most hotly contested.

5. Throughout this Article, the Authors will suggest practical pointers regarding use and avoidance of the EEA. Much of this information and advice is based on Kent Alexander’s decade of experience as an Assistant United States Attorney and as a United States Attorney. Mr. Alexander has had numerous discussions with officials at all levels of the Department of Justice about the prosecution of hi-tech crimes and, specifically, about the passage and use of the EEA.
THE ECONOMIC ESPIONAGE ACT 909

I. LEGISLATIVE HISTORY OF THE EEA

A. Importance of Trade Secrets and Proprietary Information

The United States leads the world in developing new products and new technologies.\(^6\) Per capita, the United States produces the majority of the world's intellectual property capital, including patented inventions, copyrighted material, and proprietary economic information.\(^7\) If the country is to maintain that edge, however, trade secret information must be protected and kept strictly confidential. In contrast to patents and copyrights, which are public in nature,\(^8\) the value of a trade secret "is almost entirely dependent on its being a closely held secret."\(^9\)

In the last few decades, intangible trade secret assets have become increasingly important to the prosperity of American companies.\(^10\) Prior to the passage of the EEA, the Senate observed that "a piece of information can be as valuable as a factory is to a business. The theft of that information can do more harm than if an arsonist torched that factory."\(^11\) One need look no further than the development of Windows\(^8\) and the Pentium\(^8\) chip to appreciate the astonishing value of trade secrets. But with that value comes the risk of economic espionage and theft.

The American Society for Industrial Security (ASIS) Intellectual Property Loss Survey concludes that potential losses for United States-based companies from theft of trade secrets could exceed $250 billion annually.\(^12\) The EEA, therefore, "reflects congressional determinations that the development and production of trade secrets is integral to the maintenance of a healthy and competitive national economy and that, in turn,

---

8. See id.
9. Id. at 6.
10. See Margaret M. Blair, Ownership and Control: Rethinking Corporate Governance for the Twenty-First Century 234 n.57 (1995) (stating that in 1982, tangible assets of mining and manufacturing companies accounted for 62% of their market value; by 1992 tangible assets accounted for only 38%).
maintenance of a competitive national economy is imperative to national security."  

B. The Legal Need for the EEA

Although a well-established body of civil law has addressed the protection of trade secrets for some time, there has been no federal criminal counterpart. Also, civil laws obviously do not offer the same remedies as criminal sanctions. The Uniform Trade Secrets Act (UTSA)\(^4\) applies to civil disputes and various trade secret concepts, but only provides for damages and injunctive relief to punish violators and only protects against software or computer technology theft. By contrast, the EEA includes criminal sanctions that raise the stakes well above the prospect of civil damages, which are too often viewed merely as a "cost of doing business."  

In a letter to Senator Orrin Hatch encouraging passage of the EEA, Attorney General Janet Reno noted that the Act "will close significant gaps in federal law, thereby protecting proprietary economic information and the health and competitiveness of the American economy."\(^5\) The vast and rapid advances in computer technology have highlighted those gaps and have created perhaps the greatest need for the EEA.\(^6\)

Preexisting federal criminal laws\(^7\) did not fully protect trade secrets and proprietary information of companies involved in developing computer technology. For instance, the Interstate Stolen Property Act (ITSP),\(^8\) enacted in the 1930s, applies to

---

17. See Ronald L. Johnston, Contracting and Trade Secrets Online, 14 COMPUTER LAW. 1, 2 (July 1987) (citing ROGER MILGRAM, MILGRAM ON TRADE SECRETS § 2.08(5), at 2-236 (1983)). Ironically, "[i]t is widely recognized that 'probably the single most important "product" eligible for trade secret protection is computer software.' " Id.
19. 18 U.S.C. § 2314 (1994); see also id. § 2315 (criminalizing receipt of Interstate stolen property).
“goods, wares, [or] merchandise” but is not well suited to the intangible world of “intellectual property.”20 In Dowling v. United States,21 the Supreme Court indicated its reluctance to apply the ITSP statute to intellectual property cases, holding that the ITSP could not be used to effectively criminalize copyright infringement. The ITSP, furthermore, applies to thefts of “goods, wares, [or] merchandise . . . of the value of $5,000 or more.”22 Thus, it is possible that under the ITSP, the defendant who downloads computer information onto a diskette could not be charged because the diskette is of nominal value.

Similarly, mail and wire fraud statutes,23 although popular with federal prosecutors because of their nearly universal application and familiarity,24 are sometimes of little or no help in prosecuting theft of trade secrets. Trade secrets, unlike tangible property, can be easily stored and rapidly transferred intrastate over the Internet, on diskette,25 or simply in someone’s mind as he or she walks out the door. In such scenarios, thieves can steal the proprietary information without ever triggering the jurisdictional requirements of using the United States mails (mail fraud) or making interstate telephone calls or data transmissions (wire fraud). While prosecutors have

20. 18 U.S.C. § 2314 (1994); see Toren, supra note 18, at 98 (“As an initial step, Congress should amend 18 U.S.C. § 2314 . . . to specifically include the interstate transportation of stolen intangible property.”).
23. See id. §§ 1341, 1343, 1346. Note that § 1346 statutorily reversed McNally v. United States, 483 U.S. 350 (1987), in which the Supreme Court had held that “the mail fraud statute did not include schemes to defraud citizens of their intangible right to honest government, but rather was limited to protection of ‘property’ rights.” Toren, supra note 18, at 86; see McNally, 483 U.S. at 356. Congress overruled McNally by enacting 18 U.S.C. § 1346, which states that for purposes of the mail fraud statute, “the term ‘scheme or artifice to defraud’ includes a scheme or artifice to deprive another of the intangible right of honest services.” 18 U.S.C. § 1346 (1994). In Carpenter v. United States, 484 U.S. 19 (1987), the Supreme Court held that the disclosure of confidential information for gain can be a violation of mail and/or wire fraud statutes. See Carpenter, 484 U.S. at 28.
24. See, e.g., United States v. Four Pillars Enter. Co. (Avery Dennison case), Crim. No. 1:97mg0109 (N.D. Ohio 1997) (charging EEA violations, but using wire and mail fraud charges as the lead counts in the indictment).
many federal statutes in their arsenal to attack property theft, the "peculiar mismatch between new technological capabilities and the legal infrastructure regulating them has encouraged the expansion of economic espionage." 

Of course, many state laws addressing trade secret theft have long been on the books, and state prosecutions are often a viable avenue for victims. But limited state budgets and other jurisdictional considerations can make the feasibility of conducting an out-of-state investigation impractical. Witnesses often must be subpoenaed from across state lines, and leads must be followed in other states. Also, with ever increasing Internet traffic, state lines continue to blur, and interstate thefts become easier to commit, placing even greater burdens on state attorneys general and district attorneys. Because the federal government has an interstate network and a large budget, federal authorities often are better positioned to handle far-reaching trade secret theft cases.

Prior to the passage of the Economic Espionage Act, federal prosecutors were sometimes left to their own creativity and to strained readings of existing statutes to establish criminal intellectual property theft cases. United States v. Hancock is a case in point. Mr. Hancock represented a California company and offered an AT&T engineer in Atlanta $10,000 to provide blueprints for a manufacturing device to be used to develop plants abroad. Unbeknownst to Mr. Hancock, the engineer reported the attempted bribe to his superiors, and the company called in the Federal Bureau of Investigation (FBI). Under the watchful eye of the FBI, the engineer agreed to negotiate a deal and carry the blueprints to California. The Bureau arrested Mr. Hancock for the attempted theft upon delivery. The prosecutor's dilemma—finding a federal crime to charge.

26. See generally James H.A. Pooley et al., Understanding the Economic Espionage Act of 1996, 5 TEX. INTELL. PROP. L.J. 177 (1997) (providing an excellent overview of federal criminal laws, other than the EEA, designed or used to combat property theft).
27. Basat & Nihill, supra note 4, at 248.
First, the government had difficulty in proving that the blueprints were "property" as defined by the statute, and, second, the blueprints were never actually "stolen" since there had been no conversion of the property. Ultimately, the prosecutor charged the case as an interstate transportation in aid of racketeering, using a California commercial bribery statute as the predicate offense for the attempted racketeering.\(^{31}\) To say the least, this was a circuitous route to prosecute a case that today would fit within the construct of the EEA.\(^{32}\)

C. Passage of the Act

In part because of cases like United States v. Hancock, Congress saw a need to bolster law enforcement's ability to combat the increase in trade secret theft not adequately addressed by existing laws. As FBI Director Louis Freeh stated at the time, "[t]he ever increasing value of proprietary economic information in the global and domestic marketplaces and the corresponding spread of technology have combined to significantly increase both the opportunities and motives for conducting economic espionage."\(^{33}\) President Clinton noted that "[f]ederal law has not accorded appropriate or adequate protection to trade secrets, making it difficult to prosecute thefts involving this type of information. Law enforcement officials have relied instead on antiquated laws that have not kept pace with the technological advances of modern society."\(^{34}\)

Ultimately, Congress drafted the EEA to protect intangible trade secrets, deter economic theft, and combat sophisticated international and interstate criminal activity.\(^{35}\) Originally, however, the drafters of the Act focused on theft of American information by foreign governments, and Congress included broad unilateral penalties to be levied against foreign

---

31. See id. Mr. Hancock offered cash for documents, but the competitor's employee reported the attempted bribe to the FBI and a sting operation resulted. Mr. Hancock pled guilty and was sentenced in 1990. He received a $5000 fine, 60 months of probation, and 500 hours of community service. See id.
perpetrators of thefts of trade secrets. 38 One problem: the drafters soon realized that the Act potentially violated a number of international trade treaties, and Congress had no alternative but to soften its patriotic zeal by modifying the foreign component of the Act and enhancing the commercial trade secret theft provisions. 37 The ironic result has been a shift of much of the practical use of the Act from the realm of foreign agents and governments to the realm of commercial entities. 38 While certain United States Attorneys' offices will no doubt have occasion to prosecute foreign governments and agents, 39 every EEA prosecution to date has focused on the commercial trade secret theft prong of the statute. 40 For that reason, while this Article addresses both prongs of the statute, the primary focus will be on commercial trade secret theft.

II. ELEMENTS OF THE EEA

The EEA criminalizes the theft of trade secrets in two different situations. First, the Act prohibits economic espionage by foreign governments or agents ("foreign espionage") 41 Second, the Act criminalizes theft of trade secrets that occur commercially ("commercial theft" or "commercial trade secret

36. See 18 U.S.C. § 1831 (Supp. II 1997) (prohibiting theft by foreign governments); id. §1837 (extraterritoriality provision). While Congress's clear intent in passing the EEA was to protect American companies' proprietary information, the Act conceivably could apply to a situation in which no American company is involved. See Seki & Toren, supra note 37. For example, a United States citizen living abroad could steal a Russian trade secret on behalf of the Chinese government. That act would violate the EEA, even though there is no connection between the theft and the United States other than the thief's nationality. See id. (citing Pooley et al., supra note 26, at 204).
40. See supra note 3 and accompanying text.
THE ECONOMIC ESPIONAGE ACT

1999] The Economic Espionage Act: Setting The Stage For A New Commerce

A. Common Elements of Foreign and Commercial Violations

Although the EEA distinguishes foreign espionage violations and commercial theft violations, the provisions share the following three essential elements: (1) the defendant stole, or without authorization of the owner, obtained, destroyed, or conveyed information; (2) the defendant knew the information was proprietary; and (3) the information was in fact a trade secret. Thus, while some elements differ, the thrust of the conduct proscribed by the two provisions is very similar.43

B. Differing Elements of Foreign and Commercial Violations

1. Foreign Espionage

In the case of foreign espionage, the Act requires that the defendant intend to benefit a foreign government or an agent of a foreign government. This section, however, does not require that the misappropriation economically benefit the foreign government; instead, reputational, strategic or tactical benefit will suffice.44 Also, because of its relation to foreign espionage, § 1831 provides more serious penalties than its commercial counterpart, § 1832.45

An individual defendant convicted of foreign espionage faces a penalty of up to $500,000 or imprisonment of up to fifteen years.46 A corporate defendant may be fined a maximum of $10 million.47 Convictions for commercial theft, on the other hand, carry a maximum prison term of ten years and a penalty of $250,000 per count.48 An organization convicted of a violation of § 1832 may be fined up to $5 million.49

42. See id. § 1832.
43. See id. §§ 1831-1832.
45. See 18 U.S.C. § 1831(a)(5), (b); id. § 1832 (a)(5), (b) (Supp. II 1997).
46. See id. § 1831.
47. See id.
48. See id. §§ 1832, 3571.
49. See id.
2. Commercial Theft

The commercial theft defendant must intend to benefit a third party economically for the misappropriation to violate the EEA.\(^50\) Section 1832 also requires that the defendant intend to harm the owner of the trade secret by conveying the secret.\(^51\) Intent to harm does not require that the defendant act with malice; it simply requires that the defendant must know or be aware to a practical certainty that the act of conveying or stealing or destroying the trade secret would harm the owner.\(^52\)

In addition, § 1832 requires that the trade secret “travel” in interstate or foreign commerce. Thus, the trade secret must be “related to or included in a product” that has traveled in interstate commerce.\(^53\) While most products or components of products travel in interstate commerce, the requirement presents a potential problem for prosecutors. Some trade secrets are in the theoretical or developmental stage and have not yet been incorporated into a product. The Justice Department has urged prosecutors to argue that a product “will ultimately” be sold in interstate commerce.\(^54\) Conversely, if the trade secret is included in a product, then the defendant may be able to argue reverse engineering as a defense to violation of the EEA.\(^55\)

C. Trade Secret and Misappropriation Defined

The definitions of “trade secret” and “misappropriation,” as defined in the Economic Espionage Act, are in some respects broader than definitions found elsewhere in the intellectual property area. An understanding of each is fundamental to determining the appropriate application of the EEA.

---

50. See id. § 1832. The two separate offenses, therefore, are “distinguished by the beneficiary of the misappropriation.” Basat & Nihill, supra note 4, at 246.
54. CRIMINAL RESOURCE MANUAL 1135 (1997) ("[I]n cases in which the trade secret is related to a product still being developed but that product will ultimately be sold in interstate commerce, prosecutors should establish this fact, and argue that it sufficiently meets this element.").
55. See generally discussion, infra Part III.B (discussing the Government’s standards for prosecuting EEA cases).
1. Trade Secret

Although modeled after the definition of "trade secret" in the Uniform Trade Secrets Act (UTSA), the EEA definition is at once broader and narrower than the term used in traditional civil statutes. An EEA trade secret can broadly include "all forms and types of financial, business, scientific, technical, economic, or engineering information." The statute also enumerates specific types of information, such as patterns, blueprints, or formulas, that may be protected. And the trade secrets may be protected "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically." Thus, almost any type or form of information may qualify as a trade secret under the EEA.

Importantly, however, there are two requirements that trade secrets must meet before triggering the EEA: "(A) the owner . . . has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." Of course the *sine qua non* of a trade secret is that it may not be publicly known. And like the UTSA, the EEA places the onus on the owner-victim to take "reasonable" steps to protect the information. Thus, "in order to obtain a conviction, the government will need to prove not only the defendant's culpability, but the trade secret owner's vigilance in protecting its alleged trade secrets."

---

59. Id.
60. Id. § 1839(3)(A)-(B).
61. See id. § 1839(3)(A).
2. Misappropriation

While most federal statutes have generally focused on the physical taking of property as the requisite "misappropriation," the EEA proscribes less traditional methods of misappropriation. Specifically, misappropriation occurs when a person "without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret." As this definition reflects, the intangible nature of trade secrets calls for an expansive view of misappropriation. In the EEA, misappropriation includes thefts in which the original property never actually leaves the custody of the owner, recognizing that mere replication and publication rob the property of its value as a trade secret.

D. Reasonableness and Economic Value

Analysis of the "reasonableness" of measures taken to keep trade secrets confidential is based on an objective standard of reasonableness and does not require a company to implement every possible protection in keeping such information secret. Nonetheless, the idea of self-protection is a relatively novel concept in criminal law, and, in light of this requirement, corporations should take particular care to raise employee awareness of the need to protect specific trade secrets and to limit employee access to such confidential information.

The second qualification necessary to trigger the EEA—that the information derives "independent economic value"—can be difficult to prove. In pre-EEA cases, however, courts have been relatively flexible in allowing different methodologies to

---

64. See, e.g., MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 521 (9th Cir. 1993); see also Pioneer Hi-Bred Int'l v. Holden Found. Seeds, 35 F.3d 1226, 1235 (8th Cir. 1994); Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823, 848-49 (10th Cir. 1993); ROGER M. MILGRIM, 1 MILGRIM ON TRADE SECRETS § 1.04, at 1-26 (1998).
65. See discussion, infra Part III.B (citing monetary value of the trade secret and the resulting economic injury to the owner as a factor to be considered in determining whether to initiate a prosecution).
66. See Hosteny, supra note 57, at 9 (stating that the definition of a trade secret is narrow).
determine the value of trade secrets. For instance, judges approved valuations based on the open market and the "thieves" market, as well as other reasonable means of determining market value.

E. Conspiracy, Attempt, Forfeiture, and Other Unusual Provisions

The EEA contains a few unusual provisions that merit particular attention, including attempt, conspiracy, and forfeiture provisions. Some of these provisions heighten the criminal exposure for corporations that come into possession of a competitor's trade secrets. Conversely, the same provisions provide welcome opportunities for victim corporations to recover the damages they suffer from trade secret thefts.

1. Attempt and Conspiracy

Under §§ 1831 and 1832, attempts and conspiracies to commit any of the enumerated offenses are punishable by the same penalties that attach to the underlying offenses. The attempt provision is significant because Title 18 of the federal criminal code does not contain a general attempt provision. The inclusion of a conspiracy provision as part of the EEA also is significant. Although there is a general conspiracy provision in the criminal code that applies to all Title 18 offenses, that standard conspiracy statute limits the penalty to five years incarceration. By contrast, the EEA conspiracy provision imposes the same sanctions for conspiracy as for substantive offenses. This penalty feature is more commonly found in the drug arena than in fraud cases. The inchoate offense

69. See United States v. Drebin, 557 F.2d 1316, 1331 (9th Cir. 1977); see also United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990) (holding that the government ultimately failed to prove the economic value of 9-1-1 software). The parameters of the economic value requirement of the EEA will become clearer as future cases are litigated.
71. See id. § 373.
72. See id. §1831 (15 years for foreign espionage violations); id. § 1832 (10 years for commercial theft violations).
provisions also allow for the prosecution of incomplete offenses, including those involving sting operations.

Additionally, the unusual inclusion of attempt and conspiracy provisions in a Title 18 substantive offense creates vicarious corporate liability risks for actions by employees and officers, which exceed the risks already posed by aiding and abetting liability. For example, undue pressure—real or perceived—on employees to develop new products or increase market share could arguably drive the employee to steal information from a competitor corporation and result in the corporation and its officers being named as defendants under this provision. Hiring new employees with trade secrets away from competitors—without proper in-house safeguards in place—may prove equally problematic by creating an appearance of a conspiracy between the employee and the new employer to steal the trade secrets.

2. Forfeiture

The EEA also provides that courts imposing a sentence shall order the forfeiture of any proceeds or property derived from violations of the EEA and may order the forfeiture of any property used to commit or to facilitate the commission of the crime. Thus, if a corporation’s car, computer network, or even its headquarters is used to facilitate a crime, the facilitating property arguably is subject to forfeiture. Congress did, however, include a direct reference to “proportionality” in the statute, with an eye toward eliminating some of the earlier disproportionate forfeitures levied as a result of overzealous prosecutions in the drug arena.76

75. See id. § 1834(a)(1)-(2) (Supp. II 1997).
3. Confidentiality

Addressing a common dilemma for companies wishing to pursue trade secret litigation, § 1835 of the EEA provides that courts shall enter orders as necessary and appropriate in EEA prosecutions to preserve the confidentiality of the trade secrets at issue. It remains to be seen what kinds of protections courts will be able to establish that will protect the due process rights of defendants on one hand and the confidentiality of trade secrets on the other. So far, at least one court has ruled that defendants' discovery requests in a criminal prosecution do not overcome Congressional intent to protect the confidentiality of trade secrets.  

4. Reports to Congress

The EEA requires the Attorney General of the United States to submit a report to Congress, no later than two years and four years after the October 1996 enactment of the statute, detailing the amounts of money received and distributed from EEA fines. While this provision is designed to keep Congress abreast of the funds that ultimately will be deposited into the Crime Victims Fund, it would seemingly have the effect of spurring increased prosecutions both two and four years out from the passage of the Act (i.e., 1998 and 2000). Currently, however, as already stated, there is a dearth of EEA prosecutions. If the numbers do not increase between now and the second reporting period deadline, some members of Congress may question the Justice Department's representation at the time of the EEA's passage that the need for the law, in the words of Attorney General Janet Reno, "cannot be understated as it will close significant gaps in federal law."
5. Extraterritorial Jurisdiction

Another unusual aspect of the Economic Espionage Act is the extraterritorial jurisdiction provision. Most federal criminal laws do not apply to conduct outside of this country, but the EEA rebuts the general presumption against extraterritoriality and applies to conduct outside of the United States if: "(1) the offender is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a state or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States." The inclusion of extraterritorial jurisdiction recognizes the increasingly global nature of our economy and is significant for corporations with offices in countries with far fewer protections regarding trade secrets and other intellectual property. The provision does not, however, apply to foreign citizens who are not also citizens or permanent residents of the United States.

III. The Government's Push for EEA Prosecutions

The Department of Justice is actively pushing for EEA prosecutions, and the white collar defense bar is anxiously awaiting the same. Based on the limited number of prosecutions thus far and the Government's own standards for bringing the cases, it appears that the Government will look to prosecute the most egregious cases in which criminal intent is clearly borne out by the evidence, usually as a result of sting operations.

82. Id.
84. See Blind-Flor, supra note 15, at A1 ("Some lawyers have wasted no time gearing up for the anticipated run of cases.").
85. See Hosteny, supra note 57, at 12 ("No matter what, the EEA is going to be selectively applied, at least for some time to come.").
1999] THE ECONOMIC ESPIONAGE ACT 923

A. Government Resources

The Department of Justice Criminal Division charges its Computer Crime & Intellectual Property Section (CCIPS) with the hands-on, front-line duty of evaluating all proposed EEA commercial trade secret theft prosecutions.86 As the name suggests, CCIPS attorneys have the technical expertise to combat high-tech criminals and to help protect American proprietary information, and they act as the principal points of contact for computer-related prosecutions.87 In May 1997, the Section issued a monograph to federal prosecutors “to provide enforcement guidelines under the EEA,” which very clearly and logically lays out the process for bringing such cases.88

In the area of high-tech crimes generally, and with Economic Espionage Act cases in particular, the government is mounting a considerable effort to increase the number of federal prosecutions. To help handle EEA cases and other high-tech prosecutions, each of the ninety-three United States Attorneys’ offices has designated at least one Assistant United States Attorney to serve as a Computer/Telecommunications Coordinator (CTC). The CTCs receive specialized training to develop their legal expertise and remain current in the field of computer and telecommunications technology. With this expertise, the CTCs generally act as resident consultants within their respective United States Attorneys’ offices, and are often the CCIPS’s principal points of contact for technology cases in those offices.89

The CTCs are also charged with working on technology and legal issues with other United States Attorneys’ offices, investigative agents, and experts.90 The result is a national network of specialists or specialists-in-training who will

---

86. Another Justice Department Section, the Internal Security Section, oversees the foreign espionage cases. See Protecting Trade Secrets Requires Multiple Approaches, CORP. LEGAL TIMES, Oct. 1998, at 48.
88. Calmann & Goldstein, supra note 56, at 19; see also U.S. DEP’T OF JUSTICE, FEDERAL PROSECUTION OF VIOLATIONS OF INTELLECTUAL PROPERTY RIGHTS (May 1997) [hereinafter DOJ FEDERAL PROSECUTION].
89. See DOJ FEDERAL PROSECUTION, supra note 88.
90. See id.
expedite technical assistance in computer-crime investigations. This network operates in multi-agency, multi-distict, and international cases.91

In addition to the CCIPS and the CTC program, Attorney General Janet Reno announced the creation of the National Infrastructure Protection Center (NIPC) in February 1998. The NIPC, an outgrowth of the FBI's Computer Investigations and Infrastructure Threat Assessment Center, came into being after the President's Commission on Critical Infrastructure Protection issued a report highlighting the vulnerability of the nation's cyber-infrastructure.92 The NIPC is designed to serve as the lead mechanism for responding to an infrastructure attack and includes representatives from the Department of Justice, the intelligence community, and other government agencies, as well as representatives from the private sector.93 The Department of Justice has asked Congress for $64 million in additional funding to support the NIPC's efforts in protecting the nation's critical infrastructure.94

The NIPC's mission is "to detect, prevent and respond to cyber and physical attacks on our nation's critical infrastructures."95 Critical infrastructures are those "physical and cyber-based systems essential to the minimum operations of the economy and government."96 Included within critical infrastructures are the industrial and economic sectors of government operations, gas and oil storage and delivery, banking and finance, transportation, electrical energy, and telecommunications. Thus, a great deal of American industry is involved in critical infrastructures and comes within the purview of the NIPC. Each business or governmental entity within these industrial sectors has critical proprietary and trade secret information, including computer and other electronic information, which is protected under the EEA.

While the NIPC's primary goal is not specifically to support the prosecution of EEA violations, the EEA serves as a valuable

91. See id.
93. See id.
94. See id.
95. Id.
Alexander and Wood: The Economic Espionage Act: Setting The Stage For A New Commercial

1999] THE ECONOMIC ESPIONAGE ACT 925

tool for the NIPC in combating high-tech invasions of the United States' critical infrastructures. Concurrent with the formation of the NIPC, Presidential Decision Directive Number 63 assigned "lead agencies" to each infrastructure sector. These lead agencies include the Departments of Treasury, Transportation, Energy, Commerce, Justice, Health and Human Services, the FBI, the Federal Emergency Management Agency (FEMA), and the Environmental Protection Agency.

The vast number of agencies and entities involved, from the CCIPS and CTC network to the NIPC, demonstrates the United States government's strong commitment to preventing and pursuing high-tech crimes and attacks on our nation's cyber-economy and infrastructure. It is important to bear in mind, however, that while the federal law enforcement community is making noteworthy strides in increasing its level of high-tech expertise, the vast majority of cutting-edge expertise still resides in the private sector and among the country's youth. One commentator noted that "for the first time since World War II, government and military technology now trails, rather than leads civilian technology."

B. Standards for Prosecutions

It is important for both attorneys and clients to know the Government's standards for prosecuting EEA cases. With an understanding of the many written and unwritten factors that comprise these standards, one can better avoid becoming a possible defendant in EEA cases and victims can more effectively enlist the Government's support in prosecuting EEA cases.

While the federal government is devoting substantial resources toward pursuing commercial trade secret theft cases, prosecutors must follow established standards to avoid criminalizing legitimate business conduct. To the Authors'
knowledge, there have been no reported EEA cases alleging government over-reaching. The legislative history makes it clear that the statute is "not intended to apply to innocent innovators or to individuals who seek to capitalize on personal knowledge, skill, or abilities they may have developed."\textsuperscript{100} By its language, Congress intended "to minimize the risk that the statute will be used to prosecute persons who use generic business knowledge to compete with former employers."\textsuperscript{101}

Adhering to Congressional intent, the Justice Department set forth several factors for prosecutors to consider in determining whether to initiate EEA prosecutions. These policies, contained in the United States Attorney's Manual, include the following factors:

(a) The scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality;
(b) The degree of economic injury to the trade secret owner;
(c) The type of trade secret misappropriated;
(d) The effectiveness of available civil remedies,\textsuperscript{102} and
(e) The potential deterrence value of the prosecution.\textsuperscript{103}

Beyond the stated factors considered by the Department of Justice, the Authors' experiences with federal prosecutions suggest that other factors will aid in determining when Assistant United States Attorneys will seek EEA prosecutions. Additional factors may include the following—in no particular order:

- The priorities of a given United States Attorney and his or her office;

\textsuperscript{101} Id. The Act also "is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed." Id.
\textsuperscript{102} Note, however, that prosecutors should be careful not to place too much emphasis on the availability of civil remedies. See Hosteny, supra note 57, at 10; UNITED STATES ATTORNEY'S MANUAL § 9-59.100 (1997) ("The availability of a civil remedy should not be the only factor considered in evaluating the merits of a referral because the victim of a trade secret theft almost always has recourse to a civil action. The universal application of this factor would thus defeat the Congressional intent in passing the EEA.").
\textsuperscript{103} UNITED STATES ATTORNEY'S MANUAL, § 9-59.100 (1997).
The priorities of a given FBI Special Agent in Charge and his or her field office—the FBI must investigate the case before it is prosecuted;
The willingness of the victim to come forward and cooperate;
The coherence and persuasiveness of the referral from the victim;
The relative absence of ulterior competitive motives in making the referral;
The adequacy of the measures taken by the trade secret owner to protect the trade secret;
The availability of more traditional and easier to prove causes of action, such as wire fraud or mail fraud;
The “encouragement” from Washington to prosecute EEA cases—expressed in a variety of ways, including internal memoranda, State of the Union addresses, case credit guidelines, and Congressionally funded positions;
The egregious and clearly criminal nature of the alleged violation;
The criminal history or reputation of the putative defendant;
The strength of the evidence, which will often involve sting operations with tapes, surveillance, corroborating documents, and “cooperating individuals”;
The availability of prosecutors and agents at a given time;
The individual adventurousness of a given Assistant United States Attorney or FBI Agent—EEA cases will present not only unique opportunities, but also new proof challenges, such as the requirement of proving that the trade secret owner has taken reasonable steps to preserve the confidentiality of the trade secret in question; and
The amount of time that an agent has spent consulting with the prosecutor during the course of the investigation to make sure that all of the proof elements have been met from the start.

Each case differs, and each United States Attorney and FBI office will make prosecutive decisions based on different factors. Regardless of what decisions are made, however, prosecutors considering the feasibility of pursuing an EEA case will usually consider more factors than those listed in the United States Attorney’s Manual.
C. Cases Presented So Far

In the first two years following the enactment of the EEA, there were only eleven prosecutions in the country. This limited universe of cases, however, offers at least a glimpse of what future prosecutions may look like.

Virtually all of the cases thus far have involved FBI undercover operations, which have included tape recorded conversations. Because of the high level of proof needed to successfully prosecute an EEA case, either taped conversations or other strong direct evidence will likely be necessary. Also, it appears that contractors, consultants, and former employees will be the most likely perpetrators. Four of the cases involved contractors or consultants, and four involved former


For updates on EEA cases, see <http://www.fbi.gov/majcases/copy> and <http://www.usdoj.gov>. In September 1999, Matthew Lange was indicted for allegedly attempting to sell engineering drawings belonging to his former employer, Replacement Aircraft Parts Co., Inc. See Gretchen Schulte, Eastern Wisconsin Indicts Man on Charges of Economic Espionage, MILWAUKEE J. & SENTINEL, Sept. 9, 1999.

employees. Only two of the cases involved pure outsiders, and one involved a current employee whom a competitor was hiring. The alleged trade secret thefts have come to light in a variety of ways, including competitors notifying the putative victims, employees notifying management of attempted bribes, and at least one case of law enforcement receiving a report of a physical burglary. Alleged violations have also come to light in unexpected and somewhat quirky ways. In one of the prosecutions, a current employee misdirected an e-mail intended for a competitor, in another the defendant posted an offer to sell the trade secrets on the Internet, and, in yet another, the defendant invited a competitor via a newspaper classified ad to purchase the trade secrets of the intended victim.

Most of the trade secrets so far have involved formulas or other technical information. The most severe term of incarceration handed down thus far has been a prison sentence of six years and five months, without parole. The most significant restitution order imposed has been $1,271,151.

---

113. See United States v. Hartley, Crim. No. 4:98cr00041 (E.D. Tex. 1998) (noting that the defendants first offered to sell the trade secrets to the victim, Intel, for $1,000, but reneged and tried to sell them to a competitor for $75,000).
IV. LIMITS ON THE EEA'S APPLICATION

While government attorneys are pushing enthusiastically for more and more EEA prosecutions, and while the white-collar defense bar anxiously awaits the same, in-house and outside counsel should bear in mind that a flood of prosecutions is unlikely. The EEA is indeed a significant development in the criminal realm of intellectual property law and the ramifications of successful prosecutions are considerable, but a number of existing government and private sector factors have so far caused prosecutors to apply the Act selectively, if not sparingly.

A. Government-Driven Factors

A practical application of the written and unwritten prosecutive standards in place at the Justice Department suggests that we will not be inundated with EEA prosecutions in the coming years. First and foremost, the statute effectively requires that an Assistant United States Attorney affirmatively prove that the victim took appropriate steps to maintain the confidentiality of the trade secret at issue; otherwise there is no trade secret status. This is a foreign concept to most prosecutors who are accustomed to proving the criminality of a defendant's conduct, but not the reasonableness of the victims' conduct. It is somewhat akin to requiring the Government to prove that a burglary victim has an effective alarm system before successfully prosecuting the burglar. The requirement is by no means insurmountable but does create additional difficulty in proving cases beyond a reasonable doubt.\(^ {117}\)

In a similar vein, many trade secrets also deal with information that is extremely technical in nature and, thus, can make EEA prosecutions laborious for a line prosecutor to prepare and difficult for a jury to understand. This is especially so because many prosecutors, like most lawyers, have little experience in dealing with technical intellectual property issues. Nevertheless, the technical side of the cases can hold some allure for prosecutors. EEA prosecutions are likely to be

\(^ {117} \text{See Ballon, supra note 62, at 759 ("The law therefore places the conduct of the victim on trial, making convictions potentially more difficult to obtain.").}\)
considered "sexier" than run-of-the-mill drug cases or bank robberies and will often attract media attention.\(^{118}\)

In some areas around the country, economic espionage may fall far down on the priority list when United States Attorneys’ offices are battling against the proliferation of gang and drug crimes.\(^{119}\) The availability of agents and prosecutors thus becomes an additional consideration.\(^{120}\) Thus, if the victim has a practical civil remedy, the prosecutor may decide to conserve scarce law enforcement resources for those crimes without such remedies and leave the vindication of a victim’s rights to the civil litigation arena, particularly if no criminal statute squarely and smoothly applies.\(^{121}\)

Additionally, many United States Attorneys’ offices have their own minimum dollar threshold for prosecution of white collar cases. As a result, if the value of a misappropriated trade secret does not meet that minimum requirement, a United States Attorney may decline to prosecute.

Finally, the chilling effect of the requirement of advance approval from Washington before a United States Attorney can prosecute an EEA case should not be underestimated. For the first five years of the Act, the Attorney General, Deputy Attorney General, or Assistant Attorney General for the Criminal Division personally must approve any Economic Espionage Act prosecution.\(^{122}\) While the Justice Department section that is the point of contact in commercial theft cases—the Computer Crimes and Intellectual Property Section—is among the best qualified and most user-friendly branches in the Department, prosecutors in "the field" have a natural aversion to going to Washington to seek approval for anything if they can avoid doing so by using another statute. For the same reason, prosecutors pursue many tax cases as non-

---

\(^{118}\) See Dean Starkman et al., Reuters Denies Unit Is Probed On a Break-In, WALL ST. J., Feb. 5, 1998, at A4.

\(^{119}\) See Hosteny, supra note 57, at 9.

\(^{120}\) See id. In addition, unforeseen events, such as the Atlanta Olympic Park Bombing in July 1998, can consume large amounts of an investigative agency’s resources, leaving other investigations to languish. See id. Likewise, expected but unavoidable events may have the same effect. For example, Secret Service investigations drop noticeably in Presidential election years due to the agency’s heightened security requirements. See id.

\(^{121}\) See id.

\(^{122}\) See Reno Letter, supra note 16.
tax fraud cases because of the layers of Departmental approval they must seek before bringing an action under the tax laws. Because traditional criminal statutes such as mail and wire fraud\textsuperscript{123} are easy to use, do not require advanced approval by Washington, and do not require the Government to prove the reasonableness of the victim's conduct (\textit{i.e.}, whether appropriate steps were taken to protect trade secrets), prosecutors may sometimes leave the EEA on the indictment cutting room floor. In the Authors' experience, federal prosecutors generally take the easier and more secure route in drafting indictments, by charging traditional criminal statutes that squarely apply rather than those that are more complex and burdensome and later can be challenged on appeal.\textsuperscript{124} Alternatively, prosecutors often charge traditional crimes in tandem with more complex statutes, but obtain convictions only on the traditional offenses.

\textit{B. Private Sector-driven Factors}

Companies are generally reluctant to bring cases to the government for a host of reasons, including fear of negative publicity, mistrust of the government, and fear of losing control of the process. A review of these factors will shed some light on the relative dearth of cases referred for prosecution to date. Still, in many instances, however, companies would be well-advised to work with the government to vindicate their rights through the cost-effective and results-oriented approach of EEA prosecutions.

First and foremost, going to the government can raise legitimate concerns about maintaining the confidentiality of a trade secret. While the theft or conveyance of the trade secret may have caused \textit{some} damage, making the trade secret public through court proceedings can exacerbate the situation. The EEA provides courts with a mechanism to prevent the added damage caused by public disclosure of a trade secret, but any trade secret case—criminal or civil—raises concerns among parties seeking to protect the secret in the litigation process.

Importantly, the Act does include a provision directing courts to "enter such orders and take such other action as may be

\textsuperscript{124} See, \textit{e.g.}, id. § 1030 (Computer Fraud and Abuse Act); \textit{id.} §§ 1961-1988 (RICO).
necessary and appropriate to preserve the confidentiality of trade secrets." 125 Nevertheless, the necessity for following pretrial discovery rules while still preserving the secrecy of proprietary information causes unavoidable tension in trade secrets litigation. 126 This tension heightens in criminal cases when a defendant has a constitutional right to discover materials helpful to the defense. 127 For instance in United States v. Hsu, 128 a federal district court initially refused to grant the Government’s motion for a protective order, granting instead the defendant’s much more permissive protective order out of a concern for the defendant’s constitutional rights. 129 In a breakthrough ruling for EEA effectiveness, however, the Third Circuit overruled the District Court, holding that because the defendants were charged only with attempt and conspiracy under § 1832, and not with the completed offense, they did not need to have access to the confidential material and, thus, had no constitutional right to it. 130 Because legal impossibility was not a defense, it did not matter whether the information that the defendants allegedly conspired and attempted to steal was in fact a trade secret, and the defendants did not need unfettered access to the information in order to mount their defense. 131 Nonetheless, the question remains whether courts will permit the discovery of a trade secret in a case involving an alleged substantive violation of the Act. 132

Additionally, a victim of trade secret theft, like a victim of any other crime, does not direct the litigation; the Government does.

125. Id. § 1835 (Supp. II 1997).
127. See id. In Hsu, the Government sought a protective order restricting disclosure of trade secrets. See id. The court instead granted defendants’ request that confidential materials be produced “only to individuals requiring access to the documents for defense purposes.” Id.
129. See id. at 1025; see also Kathy Pearsall, No News May Be Good News for Victims of IT Crime, COMPUTING CANADA, Apr. 6, 1998, at 11 (stating that provisions such as § 1835 “limit[] the defendant’s right to confront his accuser and gather and examine evidence against him”).
130. See United States v. Hsu, 155 F.3d 189, 203 (3d Cir. 1998).
131. See id.
While the victim or the victim’s counsel is well-advised to forge a close working relationship with the prosecution, the Government still has ultimate control of the investigation and directs the course of the case during trial. The victim’s input into the prosecution of the case will always be advisory. By contrast, in a civil case the plaintiff directs the discovery sought and the strategy pursued. Of course, one advantage to the victim in a criminal case is that the Government foots most of the legal bill.

When reporting a crime, a victim of trade secret theft must also consider the Government’s broad powers of investigation. If, during the course of its investigation, the prosecution discovers a potential criminal act by the victim or witness, the prosecution can of course turn its sights on the victim’s conduct. The lines between witnesses, subjects, and targets in criminal investigations are sometimes thin and easily crossed. Thus, victims who report trade secret thefts must do so with the full confidence that they have clean hands in the theft and any related matters.

Finally, and perhaps most importantly, victims of trade secret thefts often fear unwanted publicity. Bad publicity can tarnish a company’s reputation and, particularly with publicly traded companies, adversely affect a company’s equity value. On the other hand, assistance in aggressive enforcement of the EEA, in some instances, could enhance a company’s value and reduce the possibility of future thefts by stressing to shareholders and would-be thieves that the company will take every measure possible to protect its trade secrets.

V. PROTECTING YOURSELF AND YOUR CLIENT—EEA AS A NON-LITIGATION DETERRENT

While the breadth and novelty of the EEA offer an unprecedented opportunity for the business community to enlist the federal government’s resources in the fight against trade secret theft, the greater value of the statute may

134. See Hosteny, supra note 57, at 8. The kinds of cases one might successfully refer to the FBI or to the United States Attorney include cases that “fit within their guidelines: foreign involvement, the payment of bribes, the existence of physical
ultimately lie in its use as a deterrent, \textsuperscript{135} \textit{sans} prosecutions. By carefully weaving the EEA into negotiations, compliance programs, and hiring practices, private citizens and corporations can use the statute as an effective tool to prevent theft of trade secrets and—at the same time—avoid becoming unwittingly snared as co-conspirators or aiders and abettors in trade secret theft prosecutions. This approach, combined with the message sent by the high profile EEA prosecutions that do go forward, can help establish the same sort of commercial code of conduct that Securities and Exchange Commission regulations\textsuperscript{136} and related prosecutions have established in the insider trading arena and that the Justice Department and antitrust laws have established in the price fixing arena. While no commercial code of conduct is foolproof, the existence and use of a code of conduct, whether in the area of trade secret theft, insider trading, or price fixing, will no doubt substantially reduce the amount of illegal activity.

Corporations may find that the Act is well-suited for pursuing disgruntled employees who steal or attempt to steal the company's trade secrets. While such a defendant will likely have few resources with which to reimburse the company, prosecution will send a strong message to current and prospective employees that the company will not tolerate trade secret theft. The Act also permits the Attorney General in a civil action to obtain injunctive relief against violations.\textsuperscript{137}

A commercial code of conduct in the trade secret area is also critically important in light of the high degree of employee mobility and the increased reliance on easily transferrable software, customer lists, source codes, and the like in today's internet economy. The issue of trade secret theft in a cyber society will no doubt loom larger and larger. Unfortunately, trade secret theft prosecutions cannot keep pace with trade

\footnotesize{misappropriated evidence, the facts of the case are a 'slam dunk,' the likely ineffectiveness of civil remedies (for instance, when the perpetrator is a foreign government or a foreign corporation with no U.S. offices), where the FBI can run a sting, or where your resources are limited." \textit{Id.} at 12.}

\textsuperscript{135} \textit{But see} Toren, \textit{supra} note 18, at 62 ("American corporations will increasingly turn to the criminal law system to try to protect their trade secrets. Therefore, federal criminal law and federal prosecutors must prepare for this high-tech challenge.").


secret thefts. The FBI and United States Attorneys' offices maintain responsibility for investigating and prosecuting hundreds of federal crimes, ranging from Child Support Recovery Act cases to international terrorism cases. As a result, a self-help approach to using the EEA to protect against trade secret theft based on the standard of conduct the Act creates will often be the statute's highest and best use.

Defensively, the effective use of the EEA in compliance and employment practices, and the resulting employee awareness, will greatly reduce a company's exposure as a potential co-conspirator or an aider and abettor under the principles of vicarious liability. Prosecutors normally treat companies with strong compliance programs very favorably when making discretionary decisions.\(^{138}\) While a company can still technically be held vicariously liable for the criminal acts of its employees, even if it has expressly counseled against criminal activity and taken reasonable steps to try to ensure that its employees are complying with the law,\(^{139}\) practically speaking that outcome is unlikely.

Many commentators have suggested steps that private citizens and corporations should take to comply with the EEA.\(^{140}\) Although stand-alone EEA compliance programs are by no means always necessary, the provisions of the EEA should at least be woven into existing compliance programs and employment practices, and can generally be used to enhance

---

139. See Samuel R. Miller et al., *New Developments in Corporate Criminal Liability: The Benefits and Risks of Compliance Programs*, C800 ALI-ABA 287 (1992) ("[U]nder prevailing law, a corporation can be held criminally liable for an isolated act of a low-level employee, even if the unlawful activities were specifically forbidden and corporate executives exercised significant efforts to prevent such activities."); see also United States v. Hilton Hotels Corp., 487 F.2d 1000 (9th Cir. 1972). *But see* Holland Furnace Co. v. United States, 158 F.2d 2, 8 (6th Cir. 1946) (holding that when employee acted illegally, disregarding numerous company bulletins and written instructions, company was not liable because to hold it liable "would carry corporate responsibility beyond . . . the boundary to which we think corporate criminal responsibility should be carried"); United States v. Beusch, 596 F.2d 871 (9th Cir. 1979).
rather than replace existing practices. What follows is a listing of some suggested practices that allow corporations to use the EEA to their advantage without necessarily involving the government. If a corporation chooses to involve the government, however, these practices can make EEA referrals by victims more attractive to prosecutors and can help would-be defendants avoid liability for the alleged illegal acts of rogue or misguided employees and colleagues.

- **Compliance programs.** Incorporate EEA provisions and warnings into existing employee handbooks and compliance plans. When trade secrets are the bread and butter of a company’s business, consider stand-alone compliance programs.

- **Trade secret audits.** Consider internal or external audits of all physical practices and policies for trade secret protection. In-house or outside counsel can provide the necessary attorney-client protections. You should be aware of various means of stealing trade secrets, including “social engineering” (*i.e.*, using social skills to talk one’s way into gaining access to a system).

- **Confidentiality and patent assignment agreements.** Require employees to sign confidentiality and patent assignment agreements as part of their employment contracts. The employee should acknowledge in the confidentiality agreement that he or she is familiar with the terms of the EEA and should be given a copy of the agreement.

- **Entrance interviews.** Counsel new hires on the terms of the EEA and the company’s commitment to abiding by the terms of the EEA, particularly when the employee is coming from a competitor. Again, have the new employee sign the confidentiality statement.

- **Exit interviews.** Keep departing employees on the trade secret straight and narrow by alerting them verbally or in writing about their continuing duty under the EEA to preserve the confidentiality of trade secrets and other proprietary information. The ten- and fifteen-year prison sentences provide powerful disincentives even for the most disgruntled former employees who might consider stealing or leaking trade secret information.
Franchises and licenses. Refer to the EEA in franchise and license agreements and clearly outline the scope of the trade secret information subject to protection. As discussed earlier, the burden is on the victim to take reasonable steps to protect the secrecy of the trade secret.

Negotiations and other business dealings. Those concerned about trade secret poaching by competitors should freely inform the competitors of the existence of the EEA and its provisions during negotiations and other business dealings. Of course, parties must take care not to use the threat of criminal prosecution during civil actions.141

Physical restrictions. Establish or upgrade physical protections of sensitive trade secrets. Physical restrictions include restricted access to premises (key cards, receptionists, building security), file cabinet locks, Chinese walls, password protection, the labeling of confidential materials, the destruction of confidential materials when they are no longer needed, and the distribution of information only on a “need to know” basis.

Document retention policies. Make sure that clear document retention policies are in place to ensure that documents and software falling outside of the policy are destroyed. Because “dumpster diving” is a popular means of trade secret theft, source materials should be shredded or otherwise destroyed beyond recognition.

Awareness of “at risk” employees. In the human resources area, employers should be particularly aware of the actions of employees who pose the greatest risks to trade secrets. “At risk” employees include employees who are being terminated, leaving to work for competitors, experiencing financial problems, experiencing substance abuse problems, or generally showing signs of being unusually disgruntled.

Compliance officers and reporting. Add EEA compliance to the list of duties for your compliance officer or whomever handles compliance issues. Consider creating a system that encourages employees to report internally other employees suspected of stealing or disseminating trade secrets.

• **Training.** Incorporate brief presentations on the EEA as part of training that the company may otherwise hold on other topics. More extensive training or warnings would be appropriate for the people who deal extensively with company trade secrets.

• **Referrals to law enforcement.** Know how and when to refer cases that you want pursued by law enforcement. The FBI handles the investigations, and the United States Attorneys prosecute the cases. Thorough and timely referral packages and presentations increase your chances of gaining action. Because the Fourth Amendment restrictions on searches and seizures apply only to government-related investigations, corporate internal investigations often can turn up invaluable pre-referral information through searches of company premises and downloading of information from company computer systems. Also, the most fruitful employee interviews often occur before the government becomes involved.

### CONCLUSION

In passing the Economic Espionage Act, Congress tightened a seam in the existing patchwork of federal criminal laws that help safeguard intellectual property. While there certainly will be many important cases prosecuted under the new Act, and while great care must be taken in the defense and prosecution of these cases, the Government likely will be very selective in undertaking prosecutions and usually will handle only the most egregious cases that send an appropriate message to private industry and would-be trade secret thieves.

Ultimately, the Economic Espionage Act’s greatest importance will probably be the role it plays in heightening the awareness of the seriousness of trade secret theft. The potential punitive stakes now include civil and criminal remedies, and a new code of commercial conduct in the area of intellectual property is emerging as a result. As long as corporations and other owners of trade secrets adhere to that code and appropriately weave the provisions of the Act into their compliance programs, business dealings, and employment practices, greater trade secret protection in the private sector
undoubtedly will result, often with no direct involvement by the government whatsoever.