The Economic Espionage Act: Bear Trap or Mousetrap?

By Chris Carr*, Jack Morton** and Jerry Furniss***

Table of Contents

I. Introduction ............................................................................................................. 161

II. Why the Increase in Economic Espionage and Trade Secret Theft? .......... 163
   A. The End of the Cold War ........................................................................ 164
   B. Increased Access to and Use of Computers and the Internet ............... 164
   C. It’s Profitable and Guilt Free..................................................................... 166
   D. Lack of Company Resources to Investigate and/or Pursue
      Unlawful Misappropriations ................................................................. 166
   E. A Hesitancy to Report Such Theft.......................................................... 167
   F. The Inadequacy of Existing Federal and State Laws............................ 168
      1. The Interstate Transportation of Stolen Property Act.................... 168
      2. Federal Mail Fraud and Wire Fraud Statutes ................................ 169
      3. State Laws .................................................................................. 170

III. A Summary of the Economic Espionage Act .................................................... 171
   A. Trade Secret – What Is It? ...................................................................... 171
      1. Secrecy ........................................................................................ 171
      2. Value ......................................................................................... 172
      3. “General Knowledge, Skills and Expertise” – Not Covered ............. 172
      4. Reverse Engineering and Parallel Development – Not
         Prohibited ................................................................................ 174
   B. Foreign Activity – Section 1831 ................................................................ 175
   C. Domestic Activity – Section 1832 ............................................................. 176
   D. Other Sanctions and Remedies ................................................................. 176

* Assistant Professor of Business Law and Public Policy, California Polytechnic State University—San Luis Obispo. Of Counsel, Jencks Law Group, Arroyo Grande, California.

** Professor of Business Law, University of Montana.

*** Professor of Business Law, University of Montana. The authors thank Special Agent Christopher Graham of the Federal Bureau of Investigation’s Criminal Investigative Division—Financial Crimes Section (Washington, D.C.) for his invaluable assistance in the preparation of this article. The authors also thank Michelle Garcia for her excellent research assistance.
E. Protective Orders................................................................. 177
F. The Territorial Reach of the EEA............................................. 179
G. Preemption............................................................................. 180

IV. Government Enforcement Efforts Under the EEA.......................... 180
A. The Worthing Case .................................................................. 180
B. The Hsu Case .......................................................................... 181
C. The Four Pillars Case .............................................................. 182
D. The Gillette Case................................................................. 184
E. The Deloitte & Touche Case .................................................... 185
F. The Atlanta Journal & Constitution Case .................................. 185
G. The Roche Diagnostics Case..................................................... 187
H. The Vactec Case ................................................................... 187
I. The Indexx Labs Case............................................................ 188
J. The Intel Case .......................................................................... 190
K. The Joy Mining Case.................................................................. 190
L. The RAPCO Case................................................................. 191
M. The Preco Case ...................................................................... 192
N. The Varian Associates Case.................................................. 192
O. The IBM Case ........................................................................ 193
P. The 3Com Case ....................................................................... 194
Q. The Caterpillar Case........................................................... 195
R. The Fina Oil Case.................................................................... 196

V. An Analysis of the Cases – What Does It All Mean? .......................... 196

VI. An EEA Trade Secret Compliance Program – Recommendations for Business ................................................................. 200
A. Reasonable Compliance Standards and Procedures .................... 201
B. Assignment of Compliance Responsibility to High-Level Personnel ........................................................................ 203
C. Use of Due Care in Delegating Discretionary Authority .................. 203
D. Effective Communication to Employees and Agents ..................... 205
E. Reasonable Steps to Achieve Compliance .................................... 207
F. Consistent Enforcement............................................................. 208
G. Appropriate Response to Known Violations ................................. 208
I. Introduction

Dorothy Young, now 88, was an assistant to one of the great secret-keepers of all time – Harry Houdini. She had to sign an oath that read in part: “I hereby swear by God the Almighty not to reveal in any manner to anyone nor even to give the smallest hint of the secrets you have confided in me.” Thanks partly to such precautions, many of Houdini’s greatest tricks remain secret to this day, even among magicians. Mrs. Young gets to the heart of her old boss’ secret-keeping genius when she recalls his “compassion, kindliness and thoughtfulness” and how he “made me feel as if I was a part of the family.” That’s your best guarantee of protection: employees who identify your interests as their own. Since 1926, when she last saw Houdini, Mrs. Young states that she has had “many people try to get me to divulge his secrets.” But, she hasn’t. Now that’s a trick.¹

It is not often that law professors get to write about the world of spies, espionage and trade secret theft. Yet, the Economic Espionage Act of 1996 (EEA),² signed into law by President Clinton on October 11, 1996, provides such an opportunity. The EEA appeared on the public policy agenda and was passed by Congress against the following backdrop:

In 1994, the New York Daily News reported that “American business executives were stunned in 1991 when the former chief of the French intelligence service revealed that his agency had routinely spied on U.S. executives travelling abroad [and] that his agency had regularly bugged first-class seats on Air France so as to pick up conversations by traveling execs, [and] then [entered] their hotel rooms to rummage through attaché cases.”³ A survey released by the American Society for Industrial Security (ASIS) noted a 323% increase in economic espionage between 1992 and 1996.⁴ Of 1,300 companies surveyed by the ASIS, more than 1,100 had

¹ Adapted from Alan Farnham’s, How Safe Are Your Secrets?, FORTUNE, Sept. 8, 1997, at 120.
² 18 U.S.C. §§ 1831-1839 (Supp. IV 1998). In signing the EEA, President Clinton stated: “This Act is an outstanding example of my Administration, the Congress, and the business community working together to provide law enforcement with the tools to combat the problems of economic espionage and trade secret theft.” See PUBLIC PAPERS OF THE PRESIDENT, WILLIAM J. CLINTON, Vol. II, at 1814 (Oct. 11, 1996).
³ Robbins, In the New World of Espionage, the Targets are Economic, N. Y. DAILY NEWS, Sept. 5, 1994, available in Dow-Jones News (Publications Library).
confirmed incidents of economic espionage, while 550 suspected incidents of espionage but were unable to prove them.\(^5\) In early 1996, the FBI was investigating approximately 800 cases of economic espionage, double the figure from 1994.\(^6\) Different sources estimated the monetary loss to U.S. industry resulting from economic espionage activities to be between $1.8 billion to $100 billion per year.\(^7\) The number of jobs lost as a result of such activities was estimated to be between one million to six million.\(^8\)

Moreover, the FBI reported that 23 foreign governments were actively targeting the intellectual property assets of U.S. corporations.\(^9\) One FBI study also found that of 173 countries, 100 were spending resources to acquire U.S. technology.\(^10\) Further, of those 100 countries, 57 were engaging in covert operations against U.S. corporations.\(^11\) A CIA report listed the following countries as “extensively engaged” in economic espionage against the United States: France, Israel, Russia, China and Cuba.\(^12\) The most frequently targeted industries included aerospace, biotechnology, computer software and hardware, transportation and engine technology, defense technology, telecommunications, energy research, advanced materials and codings,
“stealth” technologies, lasers, manufacturing processes and semi-conductors.\textsuperscript{13} Victims were not just the naïve and unsophisticated—they included such corporate giants as GM, Intel, Lockheed Martin and Hughes Aircraft.\textsuperscript{14} Further, it was not only “high technology” that was the target of such theft. Proprietary business information such as customer lists and information, product development data, pricing data, sales figures, marketing plans, personnel data, bid information, manufacturing cost analyses and strategic planning information were also sought out by intelligence agents.\textsuperscript{15} As one would expect, the regions in the United States where such activity was believed to occur with the greatest frequency were those with large concentrations of high technology research and businesses—i.e., Boston, Dallas, Washington, D.C., and, of course, Silicon Valley.\textsuperscript{16}

In summary, the problem of economic espionage and the theft of corporate trade secrets had become real and severe. In Part II of this article, we begin by addressing the primary reasons behind this increase in economic espionage and trade secret theft. Part III discusses Congress’ solution to this problem—the passage of the EEA. Part IV analyzes the 18 criminal prosecutions brought by the government to date under the EEA. Part V highlights the lessons to be gleaned from these cases. Finally, Part VI provides important compliance recommendations that prudent businesses should adopt and implement in light of these recent case developments.

II. Why the Increase in Economic Espionage and Trade Secret Theft?

There is no one reason behind the increase in economic espionage and trade secret theft in recent years. Rather, a number of factors appear to have contributed to the problem: the end of the Cold War; increased access to and use of computers and the Internet; it’s profitable and often guilt free; the lack of company resources to investigate and pursue such illicit activity; the hesitancy to report such theft to the authorities; and finally, prior to the passage of the EEA, existing state and federal

\textsuperscript{13} See Freeh Statement, supra note 9, at 12; 142 CONG. REC. S12208, S12211 (Oct. 2, 1996); Lloyd M. Burchette, Jr., Economic Espionage is a Big Threat to National Security, GREENSBORO NEWS & REC. (N.C.), Mar. 6, 1994, at F1; Economic Espionage—Spies Come in From the Cold, Go After U.S. Business, SEATTLE TIMES, Nov. 6, 1991, at A3.

\textsuperscript{14} Farnham, supra note 1, at 114.

\textsuperscript{15} Ronald E. Yates, Cold War: Part II, Foreign Intelligence Agencies Have New Targets—U.S. Companies, CHI. TRIB., Aug. 29, 1993, at C1; Freeh Statement, supra note 9, at 14; Economic Espionage: Joint Hearing Before the Senate Select Committee on Intelligence and Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology, and Government Information, 104th Cong. 2d Sess. 26 (1996) (statement of John J. Higgins).

criminal laws were inadequate to address and deter such activity. Below we discuss each of these factors.

A. The End of the Cold War

As the legislative history of the EEA itself acknowledges: “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.” The Third Circuit Court of Appeals also recently recognized this shift: “[t]he end of the Cold War sent government spies scurrying to the private sector to perform illicit work for businesses and corporations … and by 1996, studies revealed that nearly $24 billion dollars of corporate intellectual property was being stolen each year.”

As also earlier noted, the FBI has reported that at least 23 countries actively engage in economic espionage activities against U.S. companies. Disturbingly, some of these countries are our purported allies. Indeed, with the end of the Cold War, it is no longer business as usual.

B. Increased Access to and Use of Computers and the Internet

Today the increased use of and access to computers and the Internet have made it easier than ever before to steal confidential and proprietary information. It is no longer necessary for an employee to stand over a copy machine and copy secret documents. Rather, in a matter of minutes, an employee can download a company’s


19 See Fresh Statement, supra note 9 and accompanying text.

20 To name a few: Canada, Israel, Germany, Japan, and France. See supra note 12 and accompanying text.

21 For an interesting book on this issue, see JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA (W. Norton 1997).
customer list or confidential pricing information onto a computer disk, slip it into his or her pocket or briefcase, and walk out the door. One commentator notes:

The Internet can now be used as a tool for the destruction of trade secret rights. Today, an item of trade secret information (such as computer source code, a biochemical formula, or technical schematics) can be as valuable to a company as an entire factory was even several years ago. Computers now make it extremely easy to surreptitiously copy and transfer this valuable trade secret information. An employee can now download trade secret information from the computer on a diskette, take it home and scan the information on the hard drive of a home computer, and then upload it to the Internet where it can be transmitted within minutes to any part of the world. The receiving party, in turn, can do the same thing within minutes. Within days, a U.S. company can lose complete control over its trade secret rights forever.

Computer networking has also contributed to the problem. As one commentator notes: “[E]very 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.”

---

22 See House Report, supra note 4, at 4 (“Ironically, the very conditions that make this proprietary information so much more valuable make it easier to steal. Computer technology enables rapid and surreptitious duplications of 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.”). Relatedly, today’s employees often have greater access to their company’s secrets than in the past. See Toren, supra note 7, at 60-61. Employees also have greater opportunities to benefit from the knowledge of trade secrets, either by becoming self-employed or changing jobs. Id. at 61 & n.7; See also Mark J. Foley & Michael E. Dash, Jr., Inevitable Disclosure Cases in the Information Age: THE LEGAL INTELLIGENCER, Aug. 9, 1999, at 9 (discussing the high degree of employee mobility in today’s society).


24 Behar, supra note 12, at 58. Edwin Fraumann notes that the dependence on computer networks and the like makes American corporations and the United States more vulnerable to economic espionage than other countries. See Edwin Fraumann, Economic Espionage: Security Missions Redefined, 57 PUB. ADMIN. REV. 303 (1997). Peter Toren also notes that computer hackers have the ability to steal information from a company’s computer system thousands of miles away. See Toren, supra note 7, at 62.
C. It’s Profitable and Guilt Free

Not only has confidential and proprietary information become easier to steal, but it has also become potentially lucrative. A group of Russian computer hackers recently stole $10 million from Citibank by infiltrating its computer network. 25 One businessman states, “If I wanted to steal money, a computer is a much better tool than a hand gun … it would take me a long time to get $10 million with a hand gun.” 26

Further, the anonymity of this type of theft via the computer can erase one’s feeling of guilt or remorse, thereby making it attractive to thieves. 27 One can simply “loop your message through a couple of different servers, including one that makes your return address ‘anonymous,’ and bingo, you’re in business.” 28 In short, if one wants to get away with a crime in today’s society, using a computer or the Internet may be the best way to go about doing it. 29

D. Lack of Company Resources to Investigate and/or Pursue Unlawful Misappropriations

A significant amount of economic espionage and trade secret theft goes undetected. 30 Further, as the Senate Judiciary Committee notes:

What State law there is protects proprietary economic information only haphazardly. The majority of States have some form of civil remedy for the theft of such information — either adopting some version of the Uniform Trade Secrets Act, acknowledging a tort for the misappropriation of the information, or enforcing various contractual arrangements dealing with trade secrets. These civil remedies, however, often are insufficient. Many companies chose to forgo civil suits because the thief is essentially judgement proof — a young engineer who has few resources — or too difficult to pursue — a sophisticated foreign company or government. In addition, companies often do not have the resources or time to bring the suit. They also frequently do not have the investigative resources to pursue the

27 See Jeffery Young, Spies Like Us, FORBES, June 3, 1996, available in Dow-Jones News (Publications Library).
29 Young, supra note 27 (“If you want to get away with a crime today, do it using a computer.”).
30 See Moyer, supra note 18, at 180 (“As staggering as these numbers are, there is a high probability that a great deal of theft and illicit taking (perhaps even the majority of these activities) remains undetected or is simply not reported.”).
case. Even if a company does bring suit, the civil penalties often are absorbed by the offender as a cost of doing business and the stolen information retained for continued use. Only a few States have any form of criminal law dealing with the theft of this type of information. Most such laws are only misdemeanors, and they are rarely used by State prosecutors.  

E. A Hesitancy to Report Such Theft

Another reason for the increase in economic espionage and trade secret theft is the hesitancy of victimized companies to report such activity to the authorities and/or pursue civil remedies. Many companies prefer not to disclose the fact that their trade secrets have been stolen or compromised. Such an admission can be embarrassing, adversely affect stock prices and market share and/or scare away customers and investors. Many executives would rather bury such losses in earning statements than admit they “lost the family jewels.” The following quote hits the mark on this issue:

[A]s management scrambles internally to prevent another loss, it often tries to keep news of the theft from shareholders, government officials, and other businesses. Many losses don’t even go beyond department walls. Managers are embarrassed to tell their supervisors that information has been stolen, and the silence continues up the chain of command. Executives fail to reveal intellectual property theft to their boards, much less Wall Street or the press. “Information loss is like the AIDS of corporate America. For a long time no one would talk about it, fearing the impact on their stock prices and confidence of customers.” [Quoting an executive.]. [This] code of silence means that only a small percentage of … disputes over information theft end up being investigated, much less taken to court.

---

32 See PETER SCHWEIZER, FRIENDLY SPIES 7 (1993); in accord Counter Intelligence News & Developments (Nat’l Counterintelligence Ctr.) (“Targeting”), Issue No. 1, (visited Jan. 15, 2000) <http://www.loyola.edu/dept/politics/hula/cind1.html> (noting that 42 percent of the surveyed corporations did not report suspected incidence of economic espionage to the authorities). See also Ruth Sinai, U.S. Intelligence Agencies Ponder Responses to Economic Espionage—Allies such as Japan, South Korea, and Germany Spy on American Firms, NEWS & OBSERVER (Raleigh, NC), Feb. 22, 1993, at A4 (noting that the General Accounting Office was unable to complete a survey on economic espionage due to the fact that so few companies responded).
35 Weld Royal, Too Much Trust?, INDUSTRY WK., Nov. 2, 1998, available in Lexis-Nexis (Business News). See also Heidi Przybyla, FBI-Industry Initiative Urges Business to Fight Economic Spying, J. OF COMMERCE, Feb. 11, 1999, at 4A (“Companies aren’t always forthcoming with the information to help the government fight economic espionage. ‘One of the biggest problems you have is the reluctance by many companies to indicate they’ve been affected by this’ [quoting an FBI spokesman]. Economic espionage, if made public can seriously affect the financial standing of a given company or sector, including their stock prices and/or image in the business community.”); Chaim A. Levin, Economic Espionage Act: A Whole New Ballgame, N.Y.L.J., Jan. 2,
F. The Inadequacy of Existing Federal and State Laws

Prior to the passage of the EEA, there was only one very limited federal statute that prohibited the theft of trade secrets. That statute provides for criminal penalties for the unauthorized disclosure of trade secrets by a government employee. However, due to the narrow applicability of this law, victims of espionage and trade secret theft were forced to resort to a variety of other statutes. Prosecutors often relied on the Interstate Transportation of Stolen Property Act (ITSP), Mail Fraud and Wire Fraud statutes, or various state laws based on either the Uniform Trade Secrets Act or Restatement of Torts. A brief discussion of each follows.

1. The Interstate Transportation of Stolen Property Act

The ITSP was passed in the 1930's as part of an effort during the Great Depression to prevent criminals from moving stolen property across state lines in an attempt to circumvent the jurisdiction of state and local law enforcement agencies. Unfortunately, the ITSP was passed at a time when information did not have the economic value and "form" that it has today. The primary deficiency with the ITSP is that it only applies to "goods, wares and merchandise," not intangibles such as trade secrets. Further, the ITSP by its very terms does not apply to thefts of

---


38 Pooley, et al., supra note 36, at 179.


Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud … shall be fined under this title or imprisoned not more that 10 years, or both.


41 For example, in United States v. Brown, the court held that trade secrets do not constitute physical "goods, wares or merchandise" as required by the ITSP. In Brown, the defendant worked as a computer programmer for a company called "The Software Link, Inc." (TSL). TSL suspected Brown of stealing computer programs and source code. An FBI investigation uncovered evidence that Brown had, in fact, stolen source code to a TSL product. Brown was indicted under the ITSP but the court determined that purely intangible property such as the source code at issue could not constitute a "good, ware or merchandise" under the ITSP. The court further determined that for information to constitute a "good, ware or merchandise" under the ITSP, the information at
intellectual property that do not cross state lines or involve foreign commerce. Thus, in today’s increasingly electronic world, the ITSP is of little use in combating espionage and trade secret theft.

2. Federal Mail Fraud and Wire Fraud Statutes

Federal Mail Fraud and Wire Fraud statutes criminalize any scheme involving the use of the mails or an interstate wire transmission to obtain “property” by false pretenses or representation. The word “property” in these statutes, as compared to the narrower phrase “goods, wares and merchandise” used in the ITSP, is much broader (i.e., it includes intangible property such as trade secrets). Unfortunately, however, trade secret misappropriation often does not involve the use of interstate mail or wire, a requirement of these statutes. In addition, these statutes also require an “intent to defraud.” Since trade secret thieves often simply copy the information rather than “defraud” their victims, such intent is difficult for prosecutors to prove. Thus, as with the ITSP, these statutes are of little use in combating espionage and trade secret theft in today’s business environment.

issue must be embodied in a tangible object or medium. See Brown, 925 F.2d 1301, 17 U.S.P.Q.2d (BNA) 1929 (10th Cir. 1991).

42 See id.

43 18 U.S.C. § 1341 (1994). This section provides in pertinent part:

Whoever, having devised or intending to devise any scheme or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises … for the purpose of executing such scheme or artifice or attempting to do so, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Post Service, … or takes or receives therefrom any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is instructed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than five years, or both.

44 18 U.S.C. § 1343 (1994). This section provides in pertinent part:

Whoever, having devised or intending to devise any scheme or artifices to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice shall be fined under this title or imprisoned not more than five years, or both.

45 See Pooley, et al., supra note 36, at 185.

46 Id. at 185-86.

47 See id. One example would be information transmitted by a face to face meeting.

48 See id.
3. State Laws

Today the majority of states provide for some form of civil remedy for the theft of confidential and proprietary information. One state model is based on section 757 of the *Restatement Second of Torts*. According to the *Restatement*, a trade secret is defined as:

[Any] formula, pattern, device, or compilation of information which is used in one’s business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers.

An alternative model adopted by many states is based on the Uniform Trade Secrets Act (UTSA). The UTSA defines a trade secret as:

[I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Given the breadth of these trade secret definitions, state laws based on the *Restatement* and UTSA are a vast improvement over the ITSP and the Mail and Wire Fraud statutes in the fight against trade secret theft. However, they are still problematic. As earlier noted, the civil remedies they provide are often inadequate; the thief is often judgment proof or too difficult to sue; the company does not have the resources or time to pursue the case; civil penalties are often absorbed by the thief as a cost of doing business; or, for the states that do impose criminal penalties for this type of theft, the offenses are often only misdemeanors and/or such penalties are rarely used by state prosecutors.

---

49 See supra note 31 and accompanying quote in the text from the Senate Judiciary Committee. A state-by-state analysis of the differences between these state laws and the EEA is beyond the scope of this article.

50 See Simon, supra note 39, at 308.

51 4 *RESTATEMENT OF TORTS* § 757, cmt. b.

52 UNIF. TRADE SECRETS ACT § 1(4)(i)(a).

53 See supra note 31, and accompanying quote in the text from the Senate Judiciary Committee. For an example of a disheartening and naive attitude by one local prosecutor in Silicon Valley, see Dreyfuss, supra note 16, at 39 (statement of a Deputy District Attorney in the High Technology Unit of the Santa Clara County District Attorney’s Office: “It’s nonsense. … There isn’t any [economic espionage]. It doesn’t exist.”).
III. A Summary of the Economic Espionage Act

The EEA is contained in sections 1831 through 1839 of the United States Code. This section highlights and discusses the main provisions of the Act.

A. Trade Secret – What Is It?

The EEA defines trade secrets broadly:

The term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled or memorialized physically, electronically, graphically, photographically or in writing, if:

(A) the owner thereof 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 generally ascertainable through proper means by, the public.  

1. Secrecy

As noted in the above definition, the owner of the information must take “reasonable measures” to keep it secret. According to the legislative history of the EEA, “if the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it.” Thus, the critical question becomes, “What constitutes a reasonable measure under the EEA?” There is, of course, no definitive answer. The drafters of the Act stated 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.\textsuperscript{58} While no “heroic or extreme measures” are necessary,\textsuperscript{59} the owner of the material “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.”\textsuperscript{60}

2. Value

In order for an item to qualify as a trade secret under the EEA, it must also have value.\textsuperscript{61} The Act requires that the information must derive “independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means, by the public.”\textsuperscript{62} Establishing that an item has “independent economic value” may be more difficult than one would think. For example, what about an item that is in the very early developmental stage when it is misappropriated? Such an item, for example, a severely misguided marketing plan, might not have any potential economic value, let alone any actual economic value.\textsuperscript{63}

3. “General Knowledge, Skills and Expertise” – Not Covered

There is no question that the nature of the relationship between American employers and employees has dramatically changed in recent years.\textsuperscript{64} A career with a single company has become the exception, not the norm.\textsuperscript{65} Consider the following:

\textsuperscript{58} 142 CONG. REC. S12213 (Oct. 2, 1992).

\textsuperscript{59} Id.

\textsuperscript{60} Id.

\textsuperscript{61} There are three generally accepted methods used for assigning value to a trade secret: (1) the market approach (which compares the sales price of similar assets to the assets being valued); (2) the cost approach (which uses replacement cost as the indicator of value); and (3) the income approach (which measures the value of anticipated future economic benefits to be derived from the use of the asset in question). See Edwin Fraumann & Joseph Koletar, \textit{Trade Secret Safeguards}, SEC. MGMT., Mar. 1999, at 64.


\textsuperscript{63} Interestingly, many United States Attorneys’ offices have established guidelines that must be satisfied before they will prosecute a case under the EEA, one of which involves making sure that the case meets a certain economic threshold value. See Pooley, et al., supra note 36, at 214. See also Joseph N. Hosteny, \textit{The Economic Espionage Act: A Very Mixed Blessing}, INT. PROP. TODAY, Feb., 1998, available in Lexis-Nexis (Legal News).

\textsuperscript{64} See, e.g., Lawrence B. Ebert, \textit{More on the Economic Espionage Act of 1996}, INT. PROP. TODAY, Feb.1998, available in Lexis-Nexis (Legal News), noting:

The turmoil of downsizing and restructuring and the intensity of global competition have brought about a radical change in the nature of the relationship between the employee and the employer. ... The fate of intellectual property—either as trade secrets, patent details, or customer lists—is not clear in these uncertain times. As employees become disgruntled with their current employers and pursue better offers, often from competitors, this valuable information can walk out the door ....
Probably the most troublesome feature of the EEA relates to its applicability in instances in which an employee of company X, having knowledge of company X trade secret information, changes jobs to work for competitor company Y. When the employee performs work for company Y using skill and knowledge obtained during employment at company X, is the employee in violation of the EEA? How can company X protect itself from loss of its trade secrets? Conversely, how can the employee be expected to forget what he has learned when going to work for company Y? The problem is that the employee cannot simply forget the trade secrets of company X and must therefore attempt to compartmentalize the various bits of knowledge and expertise gained while in the employ of company Y.66

Fortunately, the EEA’s legislative history indicates that it was not intended to prevent a person from using general business knowledge to compete with a former employer. For example, it provides that employees “who change employers or start their own company should be able to apply their talents without fear of prosecution.”67 Moreover, “it 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.68 Further, to allay fears that the EEA might be used to stifle healthy competition or the transfer of “general knowledge, skills and expertise,” for the first five years after the passage of the Act, before a U.S. Attorneys’ Office can seek to return an indictment alleging a violation of the Act it must first seek the approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for the Criminal Division.69

---

65 See id. (“Gone are the expectations of a complete career with a single company, replaced by an attitude that both employee and employer must fend for themselves in this time of competitive change.”).
67 142 CONG. REC. S12213 (Oct. 2, 1996).
68 Id. See also Band, et al., supra note 54 (“[O]rdinary experience and skills that an employee acquires while working at a job do not qualify as trade secrets because they do not derive independent economic value from not being generally known or ascertainable. In addition, the EEA’s legislative history makes clear that former employees should not be prosecuted merely for changing jobs and using the general skills, knowledge and industry experience acquired at their previous position.”); Lawrence Pedowitz & Carol Miller, Protecting Your Client Under the Economic Espionage Act, BUSINESS CRIMES BULLETIN, available in Lexis-Nexis (Legal News) (“The EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skills or abilities. Employees who change employers or start their own company cannot be prosecuted solely because they were exposed to a trade secret while employed.”).
69 This mandate is not found in the text of the EEA, but is based on the following letter dated October 1, 1996 from Attorney General Janet Reno to Senator Orrin Hatch:

Hon. Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C.

Dear Chairman Hatch:

Thank for your support of the Economic Espionage Act of 1996 (“Act”). The need for this law cannot be understated as it will close significant gaps in federal laws, thereby protecting proprietary economic information and the health and competitiveness on the American economy.
4. Reverse Engineering and Parallel Development – Not Prohibited

Reverse engineering is generally defined as “a method of industrial engineering in which one begins with a known finished product and works backward to divine the processes and specifications involved in the product’s development and manufacture.”\(^\text{70}\) It can also involve “looking at or tasting a lawfully acquired product in order to determine its content.”\(^\text{71}\) “Parallel development” involves the creation or discovery of a trade secret as a result of one’s own honest effort and hard work.\(^\text{72}\)

According to the legislative history of the Act and Department of Justice (DOJ), neither reverse engineering or parallel development are prohibited by the EEA.\(^\text{73}\) Thus, even though the EEA does not provide an express statutory defense for reverse engineering or parallel development, the legislative history and DOJ’s position is consistent with traditional misappropriation defenses. For example, in \textit{Smith vs. Dravo Corp.},\(^\text{74}\) the Seventh Circuit Court of Appeals held that “it is unquestionably lawful for a person to gain possession, through proper means, of his competitor’s products and, through inspection and analysis, create a duplicate, unless, of course, the item is patented.”\(^\text{75}\) The U.S. Supreme Court has also stated that “trade secret law

The Department shares your concerns that this legislation be implemented in the accordance with the intent of Congress and therefore will require, for a period of five years after implementation of the Act, that the United States may not file a charge under Chapter 90, or use a violation of Chapter 90 as a predicate offense under any other law, without the personal approval of the Attorney General for the Criminal Division (or the acting Attorney Official in each of these positions if the position is filled by an Acting official). This requirement will be implemented by public regulation.

Violations of such regulations will be appropriately sanctionable. Any such violations will be reported by the Attorney General to the Senate and House Judiciary Committees.

Once again, thank you for your leadership in this critical area.

Sincerely,
Janet Reno

142 CONG. REC. S12214 (Oct. 2, 1996)

\(^{70}\) Rockwell Graphics Systems, Inc. vs. DEV Industries, Inc., 91 F.3d 914, 917 n. 3, 39 U.S.P.Q.2d (BNA) 1580, 1586 n. 3 (7th Cir. 1996) (citation omitted).

\(^{71}\) See Pooley, et al., supra note 36, at 195.


\(^{73}\) See id. See also 142 CONG. REC. S12213 (Oct. 2, 1996) (“If someone has lawfully gained access to a trade secret, and one can replicate it without violating copyright, patent, [or the EEA], then that form of ‘reverse engineering’ should be fine.”). Several commentators, however, point out that by prohibiting activities such as copying, duplicating, sketching, drawing, photocopying, downloading, and photographing, the EEA may have been intended to prohibit reverse engineering. See Pooley, et al., supra note 36, at 195-97.

\(^{74}\) 203 F.2d 369, 97 U.S.P.Q. (BNA) 98 (7th Cir. 1953).

\(^{75}\) Id. at 375, 97 U.S.P.Q. at 102.
… does not offer protection against discovery by fair and honest means such as by independent invention.”

B. Foreign Activity – Section 1831

Section 1831 of the EEA is the single most important reason the Act was passed, and is designed to address the problem of economic espionage by a foreign government. Under this section, criminal penalties will occur when an accused:

[I]ntending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing [it was] stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any [of these acts]; or (5) conspires with one or more persons to commit any [of these acts], and one or more of such persons [does] any act to effect the object of the conspiracy.

Thus, this section encompasses the “knowing” misappropriation of trade secrets by foreign governments and agents, as well as anyone acting on their behalf.

---


78 18 U.S.C. § 1831(a) (Supp. IV 1998). Note the breadth of this definition and activity. It has three aspects and covers anyone who: (1) takes (e.g., as in appropriates, steals, carries away, or conceals); (2) discloses (e.g., as in transmits, delivers, sends, mails, or communicates); or (3) acquires (e.g., as in receives, buys, or processes) the information or item at issue.

79 Pooley, et al., writes:

The Congressional Record suggests at one point that the government need only show “that the accused knew or had reason to know that a trade secret had been stolen or appropriated without authorization. … These statements cannot be reconciled with the language of the statute, which provides that the defendant must “knowingly” misappropriate the trade secret. The inconsistency may result from the late amendment of the bill. In any event, the language of the statute must take precedence over even express statements in the legislative history.

Pooley, et al., supra note 36, at 200, n.127 (emphasis in original).

80 The term “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.” 18 U.S.C. § 1839(1). Further, the legislative history of the EEA provides:

We do not mean for the test of substantial control to 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.
The criminal penalties for violating this section of the EEA are severe—for individuals, a fine of up to $500,000 or imprisonment of up to 15 years, or both; for an organization, a fine of up to $10 million.\textsuperscript{81}

C. Domestic Activity – Section 1832

Section 1832 provides for a general prohibition against domestic activity trade secret theft. This section imposes fines and imprisonment when anyone “knowingly”\textsuperscript{82} converts or conspires to convert:

[A] trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret….\textsuperscript{83}

Thus, unlike the foreign activity section of the EEA, which specifically focuses on criminal activity that benefits a foreign government, instrumentality, or agent, this section prohibits the unauthorized taking, copying, or receiving of trade secrets in the domestic context for any trade secret that is “related to or included in a product placed in interstate or foreign commerce.”\textsuperscript{84} The criminal penalties under this section of the EEA are also severe—for an individual, a fine of up to $250,000 or imprisonment of up to 10 years, or both; for an organization, a fine of up to $5 million.\textsuperscript{85}

D. Other Sanctions & Remedies

As with drug cases, when imposing a sentence under the EEA, a court must order that the person forfeit to the United States any property or proceeds obtained directly or indirectly from a violation of the EEA.\textsuperscript{86} Further, a court may order the forfeiture to the government of any property used to commit or facilitate the violation.\textsuperscript{87} While the proceeds and property in question are forfeited to the United

\footnotesize{142 CONG. REC. S10885 (Sept. 18, 1996) (Statement of Senator Kohl).}

\footnotesize{81 18 U.S.C. §§ 1831(a)(5) & (b) (Supp. IV 1998).}

\footnotesize{82 See supra note 79.}

\footnotesize{83 18 U.S.C. § 1832 (Supp. IV 1998).}

\footnotesize{84 Id.}

\footnotesize{85 18 U.S.C. § 1832(a)(5) & (b) (Supp. IV 1998).}

\footnotesize{86 18 U.S.C. § 1834(a)(1) (Supp. IV 1998).}

\footnotesize{87 18 U.S.C. § 1834(a)(2) (Supp. IV 1998).}
States,\(^{88}\) it appears that victims can seek restitution from the United States out of the forfeited proceeds.\(^{89}\)

Section 1836 provides that the Attorney General of the United States, in a civil action, may seek appropriate injunctive relief in response to a violation of the EEA.\(^{90}\) The Act’s legislative history and the terms of the Act itself do not appear to provide injunctive relief to private parties. Thus, private parties will need to seek such civil injunctive relief in state courts.\(^{91}\)

### E. Protective Orders

Ironically, and as earlier noted, one of the primary deterrents to a company bringing an action against the person or company who misappropriated a trade secret is that by bringing the action, the company may reveal the very trade secret it wishes to protect.\(^{92}\) Section 1835 of the EEA attempts to address this problem by providing that courts may “enter such orders and take such other action that may be necessary to preserve the confidentiality of trade secrets” consistent with the Federal Rules of Criminal and Civil Procedure.\(^{93}\)

In *United States vs. Kai-Lo Hsu*,\(^{94}\) the conflict between the victim company’s desire to keep the information secret and the criminal defendant’s constitutional right to a fair trial came to a head. The *Hsu* case will be discussed in greater detail below,\(^{95}\) but for purposes of this section and issue, the important facts are as follows:

Mr. Hsu was indicted under sections 1832(a)(4) (*attempt to steal trade secrets*) and 1832(a)(5) (*conspiracy to steal trade secrets*) of the EEA.\(^{96}\) During the proceeding the government filed a motion for a protective order to prevent the defendant from reviewing certain documents from the victimized company (Bristol-

---


\(^{89}\) 142 CONG. REC. S12213 (Oct. 2, 1996). With respect to the mechanics of such forfeiture proceeding, section 1834(b) provides that with a few exceptions, forfeitures shall be governed under the laws that apply to drug offenses. 18 U.S.C. § 1834(b) (Supp. IV 1998).


\(^{91}\) The point has already been made that in order for the EEA to be more powerful and effective, it needs to provide a private right of action. See Crock & Moore, *supra* note 6, at 77.

\(^{92}\) See *supra* notes 32-35 and accompanying text.


\(^{95}\) See *infra* notes 121-137 and accompanying text.

\(^{96}\) 982 F. Supp. at 1023, 44 U.S.P.Q.2d at 1647.
Myers Squibb) because those documents contained the company’s trade secrets.\(^7\) Government prosecutors argued, among other things, that to provide the defendant with the confidential documents at issue would defeat the purpose of the EEA, and in any event, such documents were not needed in an attempt and conspiracy case where proving the actual existence of the trade secret was not required.\(^8\) As part of their motion, the prosecutors proposed that the court review, *in camera*, all documents containing trade secrets and then release them to the defendant only after the court had made appropriate redactions of confidential material.\(^9\)

Mr. Hsu’s lawyers disagreed. They argued, among other things, that in order for Hsu to prepare for and receive a fair trial, they needed to view the confidential documents at issue.\(^10\) They proposed that the court adopt a broader protective order that provided that the government designate all trade secret material as “confidential;” that such designated material be shown only to those people necessary to help develop and provide a defense (e.g., counsel, experts, prospective witnesses, and presumably the defendant himself); that each person receiving access to such material be required to sign a confidentiality agreement; that such secret material be filed with the court under seal; that questions regarding the use of that confidential material be resolved at a hearing outside the presence of the jury; and finally, that all documents containing confidential material be returned or destroyed at the end of the case.\(^11\)

The district court agreed with Hsu.\(^12\) The government appealed, and on August 26, 1998, the Third Circuit Court of Appeals *reversed* the district court’s ruling.\(^13\) The Third Circuit held that Hsu was charged with the conspiracy and attempt to steal trade secrets, not their actual theft, and since he never had actual possession of the trade secrets at issue, he therefore did not need access to these materials in order to prepare his defense.\(^14\) The purpose of the EEA, the Third Circuit concluded, is to provide a solution to the problem of espionage and trade secret theft; it further held that to provide confidential information to the defense under such circumstances would deter the reporting of theft and prosecutions under the Act.\(^15\)

---

\(^7\) See id., 44 U.S.P.Q.2d at 1647-48.

\(^8\) See id. at 1023-29, 44 U.S.P.Q.2d at 1647-52.

\(^9\) See id. at 1023, 44 U.S.P.Q.2d at 1648.

\(^10\) See id. at 1023-29, 44 U.S.P.Q.2d at 1647-52.

\(^11\) See id. at 1023, 44 U.S.P.Q.2d at 1648.

\(^12\) See id. at 1029, 44 U.S.P.Q.2d at 1652.


\(^14\) See id. at 197-204, 47 U.S.P.Q.2d at 1790-96.

\(^15\) See id.
In summary, the Third Circuit’s decision in the *Hsu* case stands for the proposition that when only conspiracy and attempt are charged under the EEA, the government need not provide the actual trade secret at issue to the defendant during discovery. However, the Third Circuit left open the possibility that where the government charges a substantive trade secret offense in an EEA indictment, companies may have to turn over to defense attorneys the trade secret at issue and related confidential documents. Further, the Third Circuit failed to address whether alternate defense theories, such as entrapment or outrageous government misconduct, will require the secret material at issue to be made available to the defense. Thus, even after this case, the law on this issue remains uncertain and it may be risky for American companies to assume that federal judges will preserve the confidentiality of their trade secrets in an EEA proceeding.

**F. The Territorial Reach of the EEA**

The EEA has a very broad territorial reach. It extends beyond the borders of the United States. For example, section 1837 provides that the EEA applies not only to acts conducted entirely within the United States, but also to foreign schemes so long as any “act in furtherance of the offense was committed in the United States.”

For example, a trade secret theft involving the electronic transfer (by any means) of the secret through the United States on its way to another foreign locale would constitute a violation of the Act. Further, the EEA applies to foreign acts of trade secret theft if the defendant is a “natural person who is a citizen or permanent resident alien of the United States.” For example, if a U.S. citizen living abroad stole a Russian trade secret on behalf of the Chinese government, the EEA has been violated even though there is no other nexus between the misappropriation and the United States.

---


110 See Pooley, et al., supra note 36, at 204.
G. Preemption

Finally, section 1838 of the EEA provides that it shall not be construed to preempt or displace any other remedies, civil or criminal, relating to the misappropriation of trade secrets or the otherwise lawful disclosure of the information required by any other federal or state law (e.g., the disclosure of information pursuant to a lawful Freedom of Information Act (FOIA) request). 111

IV. Government Enforcement Efforts Under the EEA

To date, the government has prosecuted 18 cases under the EEA. The following is a summary of each case. Section V discusses the significance of these case developments.

A. The Worthing Case 112

Patrick Worthing worked at Pittsburgh based PPG Industries, Inc.’s fiberglass research center. 113 Worthing allegedly stole diskettes, blueprints and other confidential research materials from PPG valued at $20 million, which he then tried to sell to a PPG’s competitor, Owens-Corning Fiberglass, for $1,000. 114 His brother, Daniel Worthing, allegedly agreed to help for $100. 115 Owens-Corning notified PPG executives who then contacted the FBI. 116 The FBI initiated a sting operation and the two brothers were subsequently arrested. 117

The Worthings were charged with violating sections 1832(a)(1), (3), and (5) of the EEA. 118 Patrick Worthing pled guilty and in June 1997, was sentenced to 15...
months of imprisonment and three years probation. Daniel Worthing also pled guilty and was sentenced to five years probation and six months of home detention.

B. The Hsu Case

Kai-Lo Hsu, a Taiwanese national, was a technical director for Taiwan’s Yuen Foong Paper Company. Chester Ho, also a Taiwanese national, was a biochemist and professor at Taiwan’s National Chiao Tung University. These two individuals were arrested in June 1997 at the Four Seasons Hotel in Philadelphia as a result of an FBI sting operation.

Hsu was allegedly trying to obtain secret information on how to make Taxol, a powerful anti-cancer drug manufactured by Bristol-Myers Squibb that grossed $800 million for Bristol-Myers in 1996, so his company could expand into pharmaceuticals. One of Hsu’s associates, Jessica Chou, contacted an undercover FBI agent posing as a technology broker with the intent of purchasing secret information from a purportedly corrupt Bristol-Myers’ scientist. Hsu and Chou allegedly agreed to make a preliminary payment of $400,000 for the Taxol information. Chester Ho accompanied Hsu to the June meeting at the Four Seasons Hotel to allegedly verify the value of the secret Taxol information.

Although the case was brought against foreign nationals, it was brought under section 1832 of the EEA (the domestic activity section), not section 1831 (the foreign activity section, which targets defendants working on behalf of a foreign government or instrumentality). Specifically, the indictment charged violations of sections

---

119 See Seltzer & Burns, supra note 114; and Halligan Criminal Arrest List, supra note 113.
120 Halligan Criminal Arrest List, supra note 113.
123 Indictment, supra note 122, at ¶ 9.
124 Halligan Criminal Arrest List, supra note 113.
125 See, e.g., Indictment, supra note 122, at ¶ 2, 15-16; and Rovella, supra note 106, at B1, B2.
126 See, e.g., Indictment, supra note 122, at ¶ 12, 22 ; and Rovella, supra note 106, at B2.
127 Indictment, supra note 122, at p. 4. See also Halligan Criminal Arrest List, supra note 113.
128 Indictment, supra note 122, at ¶ 14. See also Halligan Criminal Arrest List, supra note 113.
129 See Indictment, supra note 122, at p. 1; Rovella, supra note 106, at B2.
182(a)(4) (the EEA’s attempt provision) and 1832(a)(5) (the EEA’s conspiracy provision).\footnote{See id.} The indictment did not allege that the defendants ever received the secret Taxol information. Hence, the indictment was attempt and conspiracy based. Hsu was also indicted on six counts of wire fraud, one count of general conspiracy, two counts of foreign and interstate travel to facilitate commercial bribery, and one count of aiding and abetting.\footnote{See id.}

On March 31, 1999, Hsu pled guilty to one count of conspiring to commit trade secret theft.\footnote{Halligan Criminal Arrest List, supra note 113.} He was sentenced to two years probation and fined $10,000.\footnote{ED PA Sentences Taiwanese Businessman to Probation in Taxol Theft Case, INT. PROP. LIT. RPR., July 21, 1991, at 7.} All other charges against him were dropped.\footnote{Halligan Criminal Arrest List, supra note 113.} In early 1999 the government dropped all charges against Chester Ho.\footnote{Halligan Criminal Arrest List, supra note 113; ED PA Sentences Taiwanese Businessman to Probation in Taxol Theft Case, INT. PROP. LIT. RPR., July 21, 1991, at 7.} Chou, the person who allegedly sought out the secret Taxol information for Hsu, remains the subject of a federal arrest warrant.\footnote{See id. See also United States v. Kai-Lo Hsu, et al., 155 F.3d 189, 193 n.2, 47 U.S.P.Q.2d (BNA) 1784, 1786 n.2; and Rovella, supra note 106, at B2.} It is believed that she now resides in Taiwan but cannot be extradited because Taiwan does not have an extradition treaty with the United States.\footnote{See id. See also United States v. Kai-Lo Hsu, et al., 155 F.3d 189, 193 n.2, 47 U.S.P.Q.2d (BNA) 1784, 1786 n.2; and Rovella, supra note 106, at B2.}

C. The Four Pillars Case\footnote{United States v. Pin Yen Yang, et al., Criminal Case No. 1:97-CR-288 (N.D. Ohio, filed Sept. 3, 1997); United States v. Victor Lee, Criminal Case No. 1:97-CR-271 (N.D. Ohio, filed Sept. 15, 1997).} Pin Yen Yang was the Chief Executive Officer of Four Pillars Enterprise Company, Ltd. of Taiwan.\footnote{See Yang Indictment at ¶¶ 3-4 (on file with the authors). See also Dean Starkman, Secrets and Lies: the Dual Career of a Corporate Spy, WALL ST. J., Oct. 23, 1997, at B1, B4; Halligan Criminal Arrest List, supra note 113; Department of Justice Press Release, Taiwanese Firm, Its President and His Daughter Indicted in Industrial Espionage Case, Oct. 1, 1997 [hereafter DOJ Press Release] (visited Dec. 13, 1999) <http://www.usdoj.gov/criminal/cybercrime.4pillar2.htm> (also on file with the authors).} Four Pillars manufactures and sells pressure sensitive devices, employs more than 900 people, and has an annual revenue of more than $150 million.\footnote{Halligan Criminal Arrest List, supra note 113.} Hwei Chen Yang is Mr. Yang’s daughter.\footnote{Yang Indictment, supra note 139, at ¶ 5. See also Halligan Criminal Arrest List, supra note 113.} She is also a Ph.D. chemist, corporate officer, and employee at Four Pillars, and is believed to hold dual
citizenship in the United States and Taiwan.\textsuperscript{142} Avery Dennison Corporation is based in California, manufactures and sells adhesive products, and employs approximately 15,000 people world-wide.\textsuperscript{143}

Ten Hong Lee, an Avery Dennison employee at Avery Dennison’s manufacturing facility in Ohio, had been allegedly giving Avery Dennison’s trade secret information concerning the manufacture of adhesive products to Four Pillars for a number of years and was reportedly paid over $150,000 during that time by Four Pillars as a “consultant.”\textsuperscript{144} The Yangs were arrested in September 1997 as part of an FBI sting operation.\textsuperscript{145} The sting operation was prompted as a result of information given to Avery Dennison by a Four Pillars employee who sought employment with Avery Dennison.\textsuperscript{146} Lee had attended a meeting at Avery Dennison in January 1997 when he was caught on closed circuit television sifting through Avery Dennison’s secret files.\textsuperscript{147} Lee was confronted by FBI agents in March 1997, admitted that he had been providing trade secrets to Four Pillars, pled guilty to wire fraud, and cooperated in an undercover capacity with the FBI to catch the Yangs.\textsuperscript{148} Federal prosecutors estimated that Avery Dennison’s research and development costs to develop the information obtained by the Yangs was between $50 million to $60 million.\textsuperscript{149}

The Yangs were originally indicted on 21 counts of various charges.\textsuperscript{150} They did not testify at trial and their attorney argued that Mr. Lee took Avery Dennison’s trade secrets on his own and the Yangs never ordered him to steal them.\textsuperscript{151} To bolster its case that the Yangs intentionally stole Avery Dennison’s trade secrets, prosecutors played a tape that showed the Yangs clipping confidential markings off papers they had received from Lee.\textsuperscript{152}

\textsuperscript{142} Halligan Criminal Arrest List, supra note 113. See also DOJ Press Release, supra note 139.
\textsuperscript{143} Yang Indictment, supra note 139, at ¶ 1.
\textsuperscript{144} Halligan Criminal Arrest List, supra note 113.
\textsuperscript{145} See id.
\textsuperscript{146} See id. See also Starkman, supra note 139, at B4.
\textsuperscript{147} Halligan Criminal Arrest List, supra note 113.
\textsuperscript{148} See id.
\textsuperscript{149} See id.
\textsuperscript{150} See Yang Indictment, supra note 139, at pp. 1-27.
\textsuperscript{151} Halligan Criminal Arrest List, supra note 113.
\textsuperscript{152} See id.
By the end of the proceeding, 19 of the 21 charges against the Yangs were dropped (e.g., the mail and wire fraud charges).\textsuperscript{153} However, the two EEA charges (1832(a)(4) and (5)) remained, and after deliberating over three days for 18 hours, the jury convicted the Yangs on both charges.\textsuperscript{154} This was the first case to actually proceed to trial under the EEA.\textsuperscript{155} Pin Yen Yang was sentenced to six months home confinement and a $250,000 fine, and Hwei Chen Yang was fined $5,000 and received one year probation.\textsuperscript{156}

D. The Gillette Case\textsuperscript{157}

Steven Davis was a process control engineer for Wright Industries, Inc., a Tennessee company that builds custom machinery.\textsuperscript{158} Wright Industries was assisting the Gillette Company in developing its new shaving system.\textsuperscript{159} Davis was assigned to be the lead process design engineer on the project,\textsuperscript{160} and also signed a nondisclosure agreement before beginning the project.\textsuperscript{161}

At Gillette’s request, Wright Industries removed Davis from the project.\textsuperscript{162} Thereafter, Davis downloaded 600 megs of secret data and drawings from the project onto his laptop computer.\textsuperscript{163} Angry with his supervisor, Davis, by fax and e-mail, disclosed this secret information to Gillette’s competitors, including Bic Corporation, American Safety Razor, and Warner-Lambert, who in turn advised Gillette.\textsuperscript{164}

\begin{flushright}
\textsuperscript{154} See id. See also FBI Press Release, Apr. 28, 1999 (visited Dec. 13, 1999) <http://www.fbi.gov/pressrm/pressrel/avery.htm> (also on file with the authors).
\textsuperscript{155} Halligan Criminal Arrest List, supra note 113.
\textsuperscript{156} See id.
\textsuperscript{157} United States v. Steven L. Davis, Criminal Case No. 97-00124 (M.D. Tenn. 1997).
\textsuperscript{158} Indictment at ¶ 1-2 (on file with the authors); Halligan Criminal Arrest List, supra note 113. Michael Davis, Engineer Faces Fraud, Theft Charges, THE TENNESSEAN, Sept. 27, 1997, at 1E.
\textsuperscript{159} Indictment, supra note 158, at ¶ 7.
\textsuperscript{160} See id. at ¶ 11.
\textsuperscript{161} See id. at ¶ 1.
\textsuperscript{162} Halligan Criminal Arrest List, supra note 113.
\textsuperscript{163} See id.
\textsuperscript{164} Indictment, supra note 158, at ¶¶ 11, 18 & 20. See also Halligan Criminal Arrest List, supra note 113; and Carrington Nelson, Ex-Engineer Jailed for Stealing Secrets, THE TENNESSEAN, April 29, 1998, at 2E.
\end{flushright}
Davis was charged with violating section 1832 of the EEA and wire fraud. He pled guilty and on April 17, 1998, was sentenced to 27 months of imprisonment, three years supervised release, and $1,271,171 in restitution.

E. The Deloitte & Touche Case

Mayra Trujillo-Cohen was a former consultant for Deloitte & Touche. The government filed a two count indictment against her for violating sections 1832(a)(2) and (4) of the EEA and wire fraud. Trujillo-Cohen allegedly stole software programs developed by Deloitte & Touche called “4FRONT for SAP” and “FASTRACK for SAP” by downloading them onto her personal laptop computer, subsequently deleting portions of the programs that referred to Deloitte & Touche, and then attempting to resell portions of the programs to a third-party company (who was not indicted) for $7 million. Trujillo-Cohen pled guilty and on October 26, 1998, was sentenced to 48 months of imprisonment, three years of suspended release, and $337,000 in restitution.

F. The Atlanta Journal & Constitution Case

Caroll Lee Campbell was a circulation manager for the Gwinnett Daily Post, a newspaper owned by Gray Communications, Inc. Paul Soucy was the district circulation manager of the Rockdale Citizen (a sister paper to the Gwinnett Daily Post).

In September 1997, the Gwinnett Daily Post and Atlanta Journal & Constitution (a rival to the Post) were involved in litigation regarding who had the

---

165 Indictment, supra note 158, at pp. 1, 5 & 8.
166 Halligan Criminal Arrest List, supra note 113.
168 Halligan Criminal Arrest List, supra note 113.
169 Halligan Criminal Arrest List, supra note 113. See also Indictment at pp. 1-2 (on file with the authors).
170 Halligan Criminal Arrest List, supra note 113; Seltzer & Burns, supra note 114.
174 See id.
right to publish Gwinnett County legal notices. Campbell allegedly offered to sell for $150,000 certain confidential and proprietary information to the Atlanta Journal & Constitution to assist it in its case against the Post.

If the Atlanta Journal & Constitution was interested in his offer, it was to put certain ads in the “personals” section of its paper. In cooperation with the FBI, the Atlanta Journal & Constitution did so. Campbell subsequently met with an undercover agent at a local shopping center. The initial payment to Campbell was $5,000, with the rest to be provided at a later date upon Campbell providing the remainder of the secret information. After Campbell obtained the $5,000, his wife, Susan Campbell, allegedly gave $1,500 to Soucy. Soucy allegedly acted as a lookout for Campbell at the local shopping center meetings.

The Campbells were charged with violating sections 1832(a)(1) through (5) of the EEA, as well as the federal mail fraud statute. Soucy was charged with violating section 1832(a)(5) of the EEA. Mr. Campbell eventually pled guilty to conspiring to steal trade secrets. On August 25, 1998, he was sentenced to three months of imprisonment, three years supervised release, and $2,800 in restitution. Soucy also pled guilty and was sentenced to three years probation, a $1,000 fine, and $500 restitution. After Mr. Campbell was sentenced, the government dropped the charges against Mrs. Campbell.


176 Halligan Criminal Arrest List, supra note 113. See also Campbell Indictment at ¶ 3 (on file with the authors).

177 See id.

178 See id.

179 See id.

180 See id.

181 See id.

182 See id.

183 See id.

184 See Soucy Information at p. 2 (on file with the authors).

185 Halligan Criminal Arrest List, supra note 113.

186 See Case Docket Sheet at p. 6 (on file with the authors).


188 Heller, supra note 187.
G. The Roche Diagnostics Case 189

Huang Dao Pei is a Chinese-born naturalized U.S. citizen. 190 He also worked for Roche Diagnostics, a division of the healthcare giant Hoffman-La Roche, Inc, as a research scientist. 191 Roche had spent millions of dollars developing a market leading Hepatitis C diagnostic kit. 192 Pei hoped that his firm, LCC Enterprises, could develop a similar kit and sell it in China. 193 Pei allegedly tried to buy the information he needed to duplicate parts of the kit through a Roche employee who was cooperating with the FBI in a sting operation. 194 Pei was charged with violating section 1832(a)(4) of the EEA. 195 According to the docket sheet, a trial date has not yet been set. 196

H. The Vactec Case 197

Wilsonart is a Texas company that manufactures laminates such as kitchen and bathroom countertops, residential floors, decorative panels, and other items used in the construction of residential and commercial buildings throughout the world. 198 Wilsonart employs over 4,200 people worldwide and its sales during 1996 alone exceeded $500 million. 199

Vactec Coatings, Inc., is a Michigan company owned and operated by Robert Amis. 200 Amis was retained by Wilsonart as a consultant in March 1995 to assist Wilsonart in its research and development project in applying hard coatings on the laminate contacting surface of caul plates (press plates). 201 He was also retained by

---

190 Halligan Criminal Arrest List, supra note 113.
191 See id.; Savage & Stagnone, supra note 113; Plot to Steal Trade Secrets Alleged, The RECORD, (Bergen County, NJ), July 29, 1998, at L7.
193 See id.
194 See id.
195 Criminal Complaint at pp. 1-4 (on file with the authors).
196 Case Docket Sheet (on file with the authors).
198 Indictment at ¶ 1 (on file with the authors).
199 See id.
200 See id. at ¶ 3.
201 See id. at ¶ 2.
Wilsonart to assist it in taking this technology to full scale application. Vactec owns the coating machine that was used to test the coating process of press plates that Wilsonart developed.

Michael Hadwin is the owner of Federal Industrial Services, Inc. (FIS), also a Michigan based business. FIS was contacted by Amis regarding assistance in preparing his coating machine for use in testing the Wilsonart process. Defendant David Krumrei, Hadwin’s friend, was hired by Hadwin as an independent contractor to assist Amis in the assembly, cleaning, and preparation of the Vactec coating machine.

From 1992 through 1996, Wilsonart invested over $750,000 in research-related activities directly associated with the press plate coating technology. Krumrei, through his position, was able to gain unauthorized access to this technology and tried to sell it to a Wilsonart competitor, CSR Limited Timber Products Division, located in Australia. Upon being contracted by Krumrei, CSR notified Wilsonart.

Krumrei was arrested as a result of an undercover sting operation. Krumrei was charged with violating section 1832(a)(2) of the EEA. On July 27, 1999, he pled guilty. Krumrei has not yet been sentenced.

I. The Indexx Labs Case

Caryn Camp was a chemist and technical service representative at Indexx Labs, a Maine-based manufacturer of veterinary products. Steven Martin was a

---

202 See id.
203 See id. at ¶ 3.
204 See id. at ¶ 4.
205 See id.
206 See id. at ¶ 5, 12.
207 See id. at ¶ 6.
208 See id. at ¶ 11, 12, 13.
209 See id. at ¶ 13.
210 See id. at ¶ 22, 23.
211 See id. at p. 1.
212 Halligan Criminal Arrest List, supra note 113.
213 See id.
California veterinarian who purportedly owned two companies—DNA Vaccine and Maverck Technologies.\(^{216}\)

The two became acquainted over the Internet,\(^{217}\) and an Internet relationship developed. Martin allegedly told Camp that she was the type of person he would like to hire and that if his company was successful at marketing a veterinary diagnostic test similar to the one produced by Indexx Labs, “we’ll give you enough bonus money to buy your own house in cash. Maybe on a Lake.”\(^{218}\)

In July 1998, Camp inadvertently sent an e-mail to an Indexx co-worker that was intended to go to Martin that stated, “They know I have been stealing, so-to-speak, from the company and sending info to someone. Can I go to jail for this? I am so scared.”\(^{219}\) Camp had also written in an earlier e-mail to Martin, “Aren’t I awful? I’m liking this spy business way too much.”\(^{220}\)

Camp and Martin were charged with, among other things, violating section 1832 of the EEA, mail and wire fraud statutes, and the ITSP.\(^{221}\) After initially pleading innocent, Camp changed her plea to guilty after more than 200 incriminating e-mails were found in her computer.\(^{222}\) As part of her plea bargain, she agreed to testify against Martin.\(^{223}\)

On August 16, 1999, after deliberating a day and a half, the jury convicted Martin of four counts of wire fraud, two counts of mail fraud, one count of conspiracy to steal trade secrets, and one count of conspiracy to transport stolen goods.\(^{224}\) On December 20, 1999, Martin was sentenced to a year and a day of imprisonment.\(^{225}\) Martin was scheduled to report to prison on January 20, 2000.\(^{226}\)

---

\(^{215}\) Indictment at ¶ 1, 3 (on file with the authors); Halligan Criminal Arrest List, supra note 113; Portland Woman Faces Jail Term for E-mailing Company Secrets, THE ASSOCIATED PRESS STATE AND LOCAL WIRE, July 23, 1999, available in Lexis-Nexis (Wire Service Reports).

\(^{216}\) Indictment, supra note 215, at ¶ 7.

\(^{217}\) Indictment, supra note 215, at ¶ 8. See also Halligan Criminal Arrest List, supra note 113.

\(^{218}\) Indictment, supra note 215, at ¶¶ 8, 15, 30. See also Halligan Criminal Arrest List, supra note 113. Further, according to Halligan, not surprisingly neither of Martin’s companies had any assets or employees. And, when Camp met Martin for the first time (shortly before they were arrested), Martin appeared not as a successful business man, but with a long beard, wearing tie dyed clothes, and driving a VW van. Halligan Criminal Arrest List, supra note 113.

\(^{219}\) Indictment, supra note 215, at ¶ 37.

\(^{220}\) Indictment, supra note 215, at ¶ 34.

\(^{221}\) See Indictment, supra note 215, at pp. 1-15.


\(^{223}\) Halligan Criminal Arrest List, supra note 113.

\(^{224}\) See id.

\(^{225}\) See id.
J. **The Intel Case**

Steven Hallstead and an accomplice, Brian Pringle, contacted Cyrix Corp. (located in Texas) and offered to sell it five stolen “Slot II” computers belonging to Intel, Inc. The computers had been stolen in April 1998 from an Intel facility in California. When the defendants attempted to sell the stolen computers to Cyrix, Cyrix notified the FBI, which then set up a sting operation that ultimately resulted in the arrest of the two defendants. It was estimated that the loss to Intel could have been as high as $10 million if the stolen computers had been obtained by a competitor before Intel released them into the market.

The five count indictment charged the defendants with conspiracy, theft and attempted theft of trade secrets, transportation of stolen goods, and receipt of stolen goods. It also sought the forfeiture of the truck that the defendants used in committing the alleged EEA violations. Both defendants pled guilty. Hallstead was sentenced to 77 months in prison and a $10,000 fine. Pringle was sentenced to 60 months of imprisonment and a $50,000 fine.

K. **The Joy Mining Case**

John Fulton was a former employee of Joy Mining Machinery, Inc. Fulton allegedly contacted a Joy employee and offered to purchase, for $1,500, confidential

---

226 See id.


228 Indictment at ¶¶ 1-2 (on file with the authors). See also 2 Charged with Trying to Steal Intel Trade Secrets, THE FORT WORTH STAR-TELEGRAM, June 4, 1998, at Bus. p. 3. Cyrix Corp. is a division of National Semiconductor Corp. Id.


230 Indictment, supra note 228, at ¶ 2. See also Halligan Criminal Arrest List, supra note 113.

231 See Savage & Stagnone, supra note 113.


233 Indictment, supra note 228, at Count 5.

234 Halligan Criminal Arrest List, supra note 113.


236 See id.


238 See Savage & Stagnone, supra note 113.
diagrams that he intended to use when he started his own competing business. The FBI was alerted and Fulton was arrested as a result of an undercover operation. Fulton was charged with violating section 1832(a)(1) of the EEA. He pled guilty and was later sentenced to five years probation and 12 months of home detention.

L. The RAPCO Case

Matthew Lange was an employee of Replacement Aircraft Parts Company, Inc. (RAPCO), a Wisconsin firm. He had worked at the firm as a draftsmen/designer from June 1995 through May 1996. Part of his job entailed copying to a removable data cartridge his employer’s confidential engineering drawings. After Lange left his employment, he attempted to sell these drawings—which belonged RAPCO—over the Internet to a RAPCO competitor for $100,000. Lange sent an e-mail to a person that he believed was a potential buyer, but in reality was a confidential FBI informant.

Lange was indicted on two counts of attempted trade secret theft, one count of copyright infringement, and three counts of wire fraud. The indictment also contained a forfeiture allegation. After a bench trial, in December 1999 Lange was found guilty on all counts. A sentencing hearing has yet to be scheduled.

239 See Information (on file with the authors); Savage & Stagnone, supra note 113; and Halligan Criminal Arrest List, supra note 113.
240 See Savage & Stagnone, supra note 113.
241 See Information, supra note 239.
242 See Case Docket Sheet (on file with the authors).
244 Indictment at ¶ 1-2 (on file with the authors). See also Gretchen Schuldt, Man Charged with Selling Trade Secrets, MILWAUKEE JOURNAL SENTINEL, Sept. 9, 1999, at D1.
245 Indictment, supra note 244, at ¶ 2. See also Schuldt, supra note 244.
246 Indictment, supra note 244, at ¶ 3. See also Schuldt, supra note 244.
247 Indictment, supra note 244, at ¶¶ 4-6. See also Schuldt, supra note 244.
248 See Schuldt, supra note 244.
249 See Indictment, supra note 244, at pp. 1-9. See also Schuldt, supra note 244.
250 Indictment, supra note 244, at p. 10.
252 See Case Docket Sheet (on file with the authors).
M. The Preco Case\textsuperscript{253}

Preco Industries, Inc. is a Kansas based firm that designs, manufactures, and sells industrial equipment.\textsuperscript{254} David Sindelar was hired by Preco in January 1994 as Vice President of Corporate Development and later as Vice President for Sales–Western Region.\textsuperscript{255} In November 1997, Preco received a letter from one of its competitors (Edale) located in the United Kingdom that contained a copy of Preco’s Sales Order Forecasts (a trade secret).\textsuperscript{256} Several weeks later, Preco received a letter from another competitor (Rolt Engineering) located in the United Kingdom, which contained Preco’s Sales Order Forecast, as well as design and specification information on Preco’s Solid Phase Pressure Forming System (also a trade secret).\textsuperscript{257} The information alleges that Sindelar was the person responsible for providing these trade secrets to these competitors.\textsuperscript{258}

Sindelar was charged with violating section 1832(a)(2) of the EEA.\textsuperscript{259} On November 23, 1998, he pled guilty and pursuant to a plea bargain, in March 1999 he was sentenced to five years probation, $16,618.35 in restitution, and a $10,000 fine.\textsuperscript{260}

N. The Varian Associates Case\textsuperscript{261}

Varian Associates, Inc. is a California based firm that manufacturers, sells, installs, and services high-end radiation therapy machines through its business unit, Varian Oncology Systems.\textsuperscript{262} David Kern was an installation services manager for Varian Oncology Systems.\textsuperscript{263} He worked for Varian from approximately 1991 through the time he was fired in 1995.\textsuperscript{264}

\begin{footnotesize}
\item[254] Information at ¶ 1 (on file with the authors).
\item[255] See id. at ¶ 2.
\item[256] See id. at ¶ 3.
\item[257] See id. at ¶ 4.
\item[258] See id. at ¶ 5.
\item[259] See id. at pp. 1-3.
\item[260] See Case Docket Sheet (on file with the authors).
\item[262] See Superceding Indictment at ¶ 1 (on file with the authors).
\item[263] See id. at ¶ 2.
\end{footnotesize}
In May 1995, after Kern had been fired from Varian, he was hired as head of engineering by one of Varian’s customers, Radiological Associates of Sacramento (RAS). \(^{265}\) At RAS, Kern was in charge of maintaining and repairing Varian radiological devices at various hospitals and treatment sites in Northern California. \(^{266}\) In October 1996, a Varian service technician inadvertently left a Varian laptop computer at a Sacramento hospital after completing a service job. \(^{267}\) This laptop computer contained Varian’s trade secrets regarding its confidential methods and procedures for servicing its radiation therapy machines. \(^{268}\) Kern allegedly took this laptop computer without permission, hooked it up to his own computer, and downloaded the confidential information. \(^{269}\) Upon discovering that the information was encrypted, he then allegedly recruited a subordinate to steal a security key from a Varian technician. \(^{270}\) Kern then used this key to print out text that included Varian’s trade secrets. \(^{271}\)

Kern was charged with violating sections 1832 (a) (1) and (2) of the EEA and the fraudulent use of a computer. \(^{272}\) The case is still pending and a trial date has yet to be scheduled. \(^{273}\)

### O. The IBM Case \(^{274}\)

Little information is currently available regarding this case. The indictment and superceding indictment are short and sparse, but allege that between December 17, 1998 and February 25, 1999, Robin Tampoe violated sections 1832(a)(2) and (4) of the EEA by misappropriating or attempting to misappropriate source code and related computer software for the U.S. Postal Service point of sale project, owned by International Business Machines (IBM). \(^{275}\) The superceding indictment also seeks the forfeiture and recovery of $5,000 that Tampoe allegedly deposited into a credit

\(^{265}\) Superceding Indictment, supra note 262, at ¶ 4.

\(^{266}\) See id.

\(^{267}\) See id. at ¶ 10.

\(^{268}\) See id.

\(^{269}\) See id. at ¶¶ 11-13.

\(^{270}\) See id. at ¶ 14.

\(^{271}\) See id. at ¶ 15.

\(^{272}\) See id. at pages 1-7.

\(^{273}\) See Case Docket Sheet (on file with the authors).


\(^{275}\) Indictment (filed March 24, 1998) at pp. 1-2 (on file with the authors); Superceding Indictment (filed June 25, 1999) at pp. 1-4 (on file with the authors).
union bank account in Houston, Texas.\textsuperscript{276} Tampoe pled guilty to the counts of attempted theft of a trade secret and forfeiture.\textsuperscript{277} He was sentenced to 15 months of imprisonment, two years probation and a $100 special assessment.\textsuperscript{278}

\section*{P. The 3Com Case\textsuperscript{279}}

3Com Corporation manufacturers computer peripheral hardware, including modems, hand-held computing devices sold under the “Palm Pilot” name, and other electronic devices.\textsuperscript{280} Many of the devices manufactured and sold by 3Com are controlled by computer source code.\textsuperscript{281} This source code is 3Com’s proprietary property, is held in trade secret form, and is considered to be its “jewels.”\textsuperscript{282}

Eun Joong Kim was employed at 3Com as a software engineer.\textsuperscript{283} In June 1993, another 3Com employee-engineer saw Kim sitting at a workstation that was outside the space where Kim normally worked.\textsuperscript{284} The employee also noticed Kim copying files onto a computer disk.\textsuperscript{285} The employee asked Kim what he was doing; Kim claimed to be copying a particular type of software, but after Kim left the workstation the employee noticed on the computer screen a number of files that he recognized as 3Com’s source code trade secret.\textsuperscript{286} Kim was subsequently confronted by another 3Com employee, where he admitted that he was sorry, that he did it for personal reasons, that he had received a job offer from another company, and that he intended to use the source code for backup and for reference purposes.\textsuperscript{287}

Early in the morning of July 1, 1999, FBI agents spoke with Kim at O’Hare Airport in Chicago as he waited to board a flight for Seoul, South Korea.\textsuperscript{288} At that meeting, Kim made the same admissions to the FBI agents that he had made to 3Com, and also admitted that he knew the information he copied was proprietary and

\begin{thebibliography}{99}
\item \textsuperscript{276} See Superceding Indictment, supra note 275, at pp. 2-4.
\item \textsuperscript{277} See Case Docket Sheet at pp. 1, 9 (on file with the authors).
\item \textsuperscript{278} See id.
\item \textsuperscript{279} United States v. Eun Joong Kim, Criminal Case No. 99-CR-481 (N.D. Ill., filed July 1, 1999).
\item \textsuperscript{280} See Criminal Complaint at ¶ 5 (on file with the authors).
\item \textsuperscript{281} See id.
\item \textsuperscript{282} See id. at ¶ 6, 16.
\item \textsuperscript{283} See id. at ¶ 7.
\item \textsuperscript{284} See id. at ¶ 8.
\item \textsuperscript{285} See id.
\item \textsuperscript{286} See id. at ¶ 9-10.
\item \textsuperscript{287} See id. at ¶ 14.
\item \textsuperscript{288} See id. at ¶ 18.
\end{thebibliography}
that 3Com would fire him if it discovered he had copied this source code.\footnote{See id.} He was then arrested in the airport and transported to the FBI’s Chicago’s office.\footnote{See id.} Kim has been charged with violating section 1832(a)(4) of the EEA.\footnote{See id. at p. 1.}

\section*{Q. The Caterpillar Case\footnote{United States v. Jack Shearer, et al., Criminal Case No. 99-CR-433 (N.D. Texas, filed December 9, 1999).}}

Jack Shearer is the owner of two Texas energy industry parts companies.\footnote{Halligan Criminal Arrest List, supra note 113. See also Harvey Rice, Conroe Man Guilty of Corporate Spying, HOUSTON CHRON., Dec. 11, 1999, at Bus. p. 2.} From 1995 to 1998, he allegedly paid more than $100,000 to three employees at Caterpillar, Inc.’s California subsidiary (Solar Turbines, Inc.) to steal plans used to make parts for oil field and pipeline machinery.\footnote{See id. See also Information at pp. 1-2 (on file with the authors).} Shearer purportedly used this stolen information to build an $8 million business.\footnote{Halligan Criminal Arrest List, supra note 113.} He had instructed his employees to remove warnings stating that the plans were owned by Solar Turbines before transferring the plans to third party machine shops where counterfeit goods were made.\footnote{See id.} After Solar Turbine was tipped off that its plans were being stolen, it contacted government authorities.\footnote{See id.}

Shearer was charged with two counts of conspiracy to steal trade secrets.\footnote{See Information, supra note 294, at pp. 1-4.} He has admitted to corporate spying and pled guilty to EEA violations.\footnote{See id.} Two of Solar Turbine’s employees have also agreed to plead guilty to EEA violations.\footnote{Halligan Criminal Arrest List, supra note 113.} Sentencing is pending.\footnote{See id.} The third employee has yet to be charged.\footnote{See id.}
R. The Fina Oil Case\textsuperscript{303}

On October 28, 1999, Oliver Costello was charged with stealing oil and gas well logs and computer software for analyzing those logs from their owner, Fina Oil and Chemical.\textsuperscript{304} The information charges him with a single count of violating section 1832(a)(2) of the EEA.\textsuperscript{305} Costello has pleaded not guilty.\textsuperscript{306} According to the case docket sheet, a trial date was set for February 22, 2000.\textsuperscript{307} No other information is available on this case at this time.

V. An Analysis of the Cases – What Does It All Mean?

A number of important lessons can be gleaned from the 18 cases brought thus far by the government. Contrary to some predictions, the cases demonstrate that the government will, in fact, devote significant resources to the investigation, prosecution, and enforcement of the EEA.\textsuperscript{308} Granted, these cases only account for a small portion of the number of economic espionage and trade secret theft cases that some suggest exist and that the government was investigating leading up to the passage of the EEA.\textsuperscript{309} Nevertheless, the amount of work and resources that the government has invested thus far illustrates that it sees the EEA as a priority.

Further, none of the cases involve a situation of reverse engineering, parallel development, or a former employee who was relying on his or her “general knowledge, skills or expertise.”\textsuperscript{310} Thus, to the extent that there were fears that the


\textsuperscript{304} Information at p. 1 (on file with the authors).

\textsuperscript{305} See id.

\textsuperscript{306} See id.

\textsuperscript{307} See Case Docket Sheet at p. 4 (on file with the authors).

\textsuperscript{308} For an example of a prediction that the government would not devote resources to the EEA, see Charles M. Sennott, Business of Spying, STAR TRIB. (Minneapolis-St. Paul), Feb. 4, 1997, available in Dow-Jones News (Publications Library) (“Will the FBI and the Justice Department really devote resources to this? … My hunch is they won’t unless it involves theft of major trade secrets with national security implications.”). For a sample of several commentators in accord, see Tucker, supra note 18, at 1148 (“It does not appear that the U.S. government will only use the EEA to prosecute theft implicating national security.”); Irvin B. Nathan & Nancy L. Perkins, U.S. Economic Espionage Act: Tough EEA Enforcement Reveals Need for Strict Compliance, BUSINESS CRIMES BULLETIN: COMPLIANCE & LITIGATION, Jan. 1998, at 4 (“Judging from these cases, the government is willing to use its full panoply of investigative tools, including sting operations, to enforce the statute.”).

\textsuperscript{309} See discussion in Part I, supra. See also Karen Sepura, Economic Espionage: The Front Line of a New World Economic War, 26 SYRACUSE J. INT’L L & COM. 127, 140 (1998) (“Despite the presence of the Economic Espionage Act, however, it does not appear that it is being used to its fully capacity. The few cases that have actually been brought to trial account for only a miniscule portion of a large number that are believed to exist.”).

\textsuperscript{310} For a discussion of whether the Act was designed to cover reverse engineering, parallel development, or general knowledge, skills and expertise, see Part III. A. supra.
government might act overzealously and pursue such activities, thereby inhibiting the flow of labor, knowledge, and/or competition, such fears have been misplaced. Further, there is no evidence in any of the cases that would support predictions that the EEA was “designed to employ foreign spies” or that it would “destroy employee mobility.”

In each case the issue of criminal wrongdoing was also clear-cut. Many of these cases arose out of FBI sting operations where the evidence accumulated against the defendant was impressive. Moreover, there was little dispute in any of the cases as to whether the defendant had the requisite criminal intent to satisfy the terms and requirements of the threshold elements needed to prove criminal liability under the Act. Stated differently, these were not the riskiest of cases for the government to pursue. In fact, only three cases went to trial. No case has involved a defendant who could credibly argue that they he or she had acted “inadvertently,” “negligently” or “unintentionally” in disclosing the trade secrets at issue.

In several cases, the indicted individuals and/or important players were outside agents, independent contractors or temporary employees (versus full-time regular employees), thereby confirming an ASIS report that such individuals often pose the greatest threat to a company’s trade secrets. For those in the competitive intelligence industry, there was also fear that the risk of prosecution under the EEA would fundamentally alter how competitive intelligence professionals conduct their research.

---

311 For example, one commentator suggests that the EEA is an overreaction to inflated statistics, and is really a ruse to employ an obsolete intelligence force. See Rochelle Cooper Dreyfuss, Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996, 9 FORDHAM L. MEDIA & ENT. J. 1 (1998); Robert Dreyfuss, Spy vs. No-Spy: The New Espionage Scare, NEW REPUBLIC, Dec. 23, 1996, at 9-10.

312 See Dan Goodin, Busting Industrial Spies, THE RECORDER, Sept. 25, 1996, available in Lexis-Nexis (Legal News), stating:

[One Silicon Valley intellectual property lawyer] said that the proposed federal law could make it harder on employers in Silicon Valley—where executives are known to go from company to company—trying to recruit top talent. Some high-tech outfits, and their prospective new employees, might fear getting entangled in a trade secrets prosecution. [That same attorney stated,] “The Valley in my view has really thrived on the exchange of ideas. … If you have hanging over your head this criminal law, that could chill mobility, chill innovation and could put a cloud—depending on what the terms of the law are—over the Valley.”

313 In accord see Hosteny, supra note 63 (“Cases brought thus far under the Economic Espionage Act appear consistent with the notion that egregious criminal activity will be required to justify a prosecution ….”).

314 The Four Pillars, Indexx Labs, and RAPCO cases.

315 In accord see Seltzer & Burns, supra note 114.

316 E.g., the Worthing, Gillette, Deloitte & Touche, and Vactec cases.

317 This is consistent with the conclusions reached by the ASIS in its most recent report. See Survey Report, supra note 23, at “Conclusions from the 1998 Survey.”
activities. However, in light of the cases the government has filed thus far, this fear appears to have been misplaced.

Interestingly, all of the cases involved section 1832 (the domestic activity section), not section 1831 (the foreign activity section). Thus, we have yet to see a section 1831 case brought by the government, even though that was the single most important reason behind the passage of the Act. Moreover, in nine of the cases, the government linked the EEA with other federal statutes (e.g., the fraudulent use of a computer, the interstate transportation of stolen property act, wire and mail fraud statutes, etc.). This pattern is consistent with a strategy often implemented by government prosecutors where the violation of multiple criminal statutes is alleged, thereby upping the ante for the defendant who wishes to go to trial, and then using that leverage to “encourage” the defendant to plead guilty to lesser charges. What is also interesting is that in only three cases, the Intel case, RAPCO case, IBM case, did the government pursue the criminal forfeiture option under section 1834 of the EEA.


Your industry is crawling with criminals. And you may be one of them. So might your company. … Cases involving a customer list used to be a concern only with private lawyers; now they can be investigated by the FBI and prosecuted by the Department of Justice. All of this came about with the enactment of the [EEA] … the fact of its passage will surely lead to greater interest in federal jurisdiction over civil trade secret disputes.


The [EEA] makes theft of trade secrets a federal crime with stiff penalties of up to $10 million and 15 years of prison for violations. Under current standards of business practice, a sales representative, indoor consultant, market researcher, or curious employee could subject an organization to an FBI raid and investigation leading to Federal prosecution.


319 See Richard Horowitz, The Economic Espionage Act: The Rules Have Not Changed, 9 COMP. INTELL. REV. 30-38 (1998) (contending that competitive intelligence professionals who are properly trained and abide by the SCIP Code of Ethics should not run afoul of trade secret law or the EEA because clearly criminal activities that the EEA targets have always been prohibited under state law and unacceptable under the SCIP Code of Ethics. See also SCIP POLICY ANALYSIS ON COMPETITIVE INTELLIGENCE AND THE ECONOMIC ESPIONAGE ACT (1999), at 3-11 (same) (on file with the authors).

320 See supra note 77 and accompanying text.

321 E.g., the Hsu, Yung, Gillette, Deloitte & Touche, Atlanta Journal & Constitution, Indexx Labs, Intel, RAPCO and Varian Associates cases.
For those who wanted to see the EEA used to punish defendants who steal valuable trade secrets, the EEA has proven to be a disappointment. 322 For example, in the Hsu case, the trade secret at issue was worth enough to the defendant that he offered to make a preliminary payment of $400,000 for the information, yet he only received two years probation and a fine of $10,000; in the Four Pillars case, the lead defendant was only sentenced to six months home confinement and a $250,000 fine, even though the research and development costs alone to develop the information he stole were valued between $50 million and $60 million. 323 In the Worthing case, the lead defendant only received 15 months of jail time and three years probation, even though the trade secret at issue was valued at $20 million. 324 In the Atlanta Journal & Constitution case, the lead defendant was sentenced to only three months of imprisonment, three years supervised release and $2,800 in restitution. 325 In the Joy Mining case, the defendant was sentenced to five years probation and 12 months of home confinement. 326 In the Preco case, the defendant was only sentenced to five years probation, $16,618.35 in restitution, and a $10,000 fine. 327

Finally, the Third Circuit Court of Appeals’ ruling in the Hsu case is of significant import. As earlier noted, the Hsu court held that when only conspiracy and attempt are charged under the EEA, the government need not provide the actual trade secret at issue to the defendant in discovery. 328 However, the Hsu court also left open the possibility that where the government charges a substantive offense in an EEA indictment, a company may very well be required to turn over to defense attorneys the trade secret at issue. 329 Of course, one of the downsides of an EEA proceeding for a victimized company is that unlike a civil case, control over the case is relinquished to the government. 330 Among other things, the government controls the actual charges filed and pursued. Thus, if government prosecutors elect to charge a substantive offense versus the charge of attempt or conspiracy to steal a trade

322 See also Crock & Moore, supra note 6, at 76 (“Companies that want to see people suffer greatly are going to be disappointed.”).

323 See supra notes 133 and 156 and accompanying text.

324 See supra note 119 and accompanying text.

325 See supra note 186 and accompanying text.

326 See supra note 242 and accompanying text.

327 See supra note 260 and accompanying text.

328 See supra notes 104-106 and accompanying text.

329 See id.

330 See, e.g., Hosteny, supra note 63. Hosteny, a former U.S attorney, states: “Another shortcoming of federal prosecution is that the protection of your trade secrets must be largely delegated to the federal prosecutor, and to the demands of the criminal justice system.” Id. See also Stephen S. Hodgson, Trade Secrets, The U.S. Economic Espionage Act and You, CHEMICAL ENGINEERING, Dec. 1998, at 89 (“After referring a case to a government prosecutor, a trade secret owner essentially loses control of the case, since it is the government prosecutor who makes the decision on prosecuting the case.”).
secret, there may be little, if anything, the victim can do to protect the trade secret. Only time will tell if the Hsu decision ultimately deters a significant number of companies from reporting trade secret theft to the government. If so, the very purpose and goal behind the EEA will have been thwarted.

VI. An EEA Trade Secret Compliance Program – Recommendations for Business

The EEA has significantly raised the stakes with respect to protecting trade secrets. In light of its penalties, businesses must take careful notice of its provisions. An understanding of the Act is critical, both for victims and for potential defendants of trade secret theft. Under the Act businesses have three major responsibilities: (1) establish reasonable safeguards to protect company trade secrets; (2) prevent the contamination of the firm through the inadvertent misappropriation of the trade secrets of others; and (3) institute measures to prevent employees from intentionally stealing the trade secrets of others.

A recent survey by the ASIS found that most American companies have serious shortcomings in their efforts to fulfill these responsibilities.\textsuperscript{331} For the prudent company, addressing these issues will entail the development of a Trade Secret Compliance Plan (TSCP). Although there is no federal mandate that companies develop a TSCP, the Federal Sentencing Guidelines\textsuperscript{332} promulgated by the United States Sentencing Commission\textsuperscript{333} provide ample reason for doing so. According to the Commission’s Sentencing Guidelines for Organizations, “Culpability generally will be determined by the steps taken by the organization prior to the offense to prevent and detect criminal conduct, the level and extent of involvement in or tolerance of the offense by certain personnel, and the organization’s actions after an offense has been committed.”\textsuperscript{334}

Although the guidelines create a basis for establishing criminal liability, they are also an excellent benchmark for formulating an effective TSCP. In fact, the

\textsuperscript{331} See Survey Report, supra note 23, at “Key Survey Findings.”


\textsuperscript{333} The Introduction to the United States Sentencing Commission states:

Duties of the Commission: The Sentencing Reform Act created the United States Sentencing Commission, an independent federal agency in the judicial branch of government. The Commission’s duties include developing guidelines for sentencing in federal courts; collecting data about crime and sentencing; and serving as a resource to Congress, the Executive Branch, and the Judiciary on crime and sentencing policy.

The sentencing guidelines went into effect on November 1, 1987, and have increased uniformity and fairness in federal sentencing <http://ussc.gov/intrusc.htm> (visited Jun. 15, 2000).

\textsuperscript{334} See Sentencing Guidelines, supra note 332, at “Introductory Commentary.”
guidelines refer to the desire to motivate businesses to adopt “mechanisms” for the
detection and prevention of trade secret theft. The guidelines encourage a
company’s TSCP to contain the following elements:

1. Compliance standards and procedures reasonably capable of reducing the prospect of
criminal conduct;
2. Assignment of compliance responsibility to high-level personnel;
3. Use of due care not to delegate substantial discretionary authority to individuals with a
propensity to engage in illegal activities;
4. Effective communication of standards and procedures to all employees and other
agents;
5. Reasonable steps to achieve compliance with its standards;
6. Consistent enforcement of the standards; and
7. Appropriate response to any known violation, including any necessary modifications to
the compliance program.336

Below we address each of these elements.

A. Reasonable Compliance Standards and Procedures

The organization must have established compliance standards and procedures
to be followed by its employees and other agents that are reasonably capable of
reducing the prospect of criminal conduct.337

There is no one TSCP that will fit all businesses. The complexity of the
compliance program will vary depending on the size of the business, the type of
intellectual property, whether international transactions are involved, and the nature
of the business. The process involved in developing reasonable compliance standards
and procedures should include:

1. An audit of the firm’s trade secrets;
2. A determination of the value of the trade secrets;
3. A risk assessment to determine the likelihood of theft or contamination; and
4. Implementation of an appropriate level of security.338

---

335 The guidelines state: “This chapter is designed so that the sanctions imposed upon organizations and their
agents, taken together, will provide just punishment, adequate deterrence, and incentives for organizations to
maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.” Id.


337 See id. at § 8A1.2, Commentary: 3(k)(1).
Assuming that the company’s audit has revealed sufficiently valuable trade secrets that are at risk of being compromised, the company may consider a number of steps that may be considered to protect those secrets. Steps that may provide a “reasonable” level of security include computer passwords and firewalls,339 a review of all announcements and speeches by members of the firm,340 placing a “Confidential-Do Not Copy” or similar notation on sensitive documents,341 controlling access to and the duplication of sensitive documents, implementing appropriate destruction of sensitive documents to discourage “dumpster diving,”342 providing locks for computer drives, using encryption devices, controlling access to and the use of the company’s laptop computers, and restricting employee and guest access to areas of the premises containing sensitive materials.

Departing employees are an obvious source of trade secret loss. Reasonable protective measures that may minimize the risk of such loss include noncompetition, nondisclosure and nonuse agreements relating to identified trade secrets.343 It is also prudent to have all employees agree that upon departure, they will return all company documents, purge their computers of company information, not recruit present employees, and provide “pre-clearance” for future employment.344

338 See Fraumann & Koletar, supra note 61, at 63-66. With respect to the second factor (value), the ASIS reports that few companies even regularly review the value of their intellectual property. For those firms that do value their intellectual property, most use in-house counsel rather than a management executive to do so. See Survey Report, supra note 23, at “Question No. 12.” See also Austin J. McGuigan & William W. Kahle, Can You Keep a Secret?, CONN. LAW TRIB., July 27, 1998, available in Lexis-Nexis (Legal News) (“[C]orporate counsel and companies should contemplate establishing systematic, proactive programs that anticipate problems relating to the theft or misappropriation of trade secrets and developing procedures with counsel to detect immediately and to investigate the actual or suspected theft or misappropriation of trade secrets”); and the website of Long & Long (a Chicago intellectual property and technology law firm) (visited Jan. 15, 2000) at <http://www.patents-tm.com/secretdefinitions.htm#audit> (essentially stating the same). Relatedly, attorney Mark Halligan points out that for a company to ensure that its information will, in fact, qualify as a trade secret under the EEA, it should analyze the following issues: (1) how many people know it (the fewer the number the more likely it is to be a secret); (2) is it known in the trade (if so, then even if it is not known by the general public, it is not a trade secret); (3) have reasonable security measures been taken to protect it; (4) can the information be easily duplicated by competitors; (5) what is its value to the company; and (6) how much time, effort and money was spent developing it? See Halligan webpage at <http://www.exepc.com/~mhallign/protect.html> (visited Jan. 15, 2000).


340 Farnham, supra note 1, at 118.

341 Daniel P. Powell, An Introduction to the Law of Trade Secrets, 23 Col. Law. 2125, 2127 (1994) (“It is of utmost necessity in implementing any trade secrets protection program to mark all internal memoranda, manuals, drawings, blueprints, schematics, software, floppy diskettes, tape cartridges or any other item that may contain a business’ trade secret information, as being ‘confidential.’”).


344 See id. Pre-clearance provides the firm with the opportunity to send a warning to prospective employers notifying them of the liability for accepting trade secrets from the new employee.
In extreme circumstances, it may even be appropriate for the company to consider seeking injunctive relief to prevent a former employee from working for a competitor. Under the “inevitable disclosure doctrine,” some courts have been willing to provide such injunctive relief in situations where it has been shown that there is a strong likelihood that trade secrets will be divulged to the competitor during the course of the employee’s employment.  

B. Assignment of Compliance Responsibility to High-Level Personnel  

Specific individual(s) within high-level personnel of the organization must have been assigned overall responsibility to oversee compliance with such standards and procedures.  

A TSCP with no one in charge will likely accomplish little. It is therefore imperative that high-level personnel be in charge of the TSCP, and that this person have sufficient organizational authority and clout to promote change in the activities of the marketing, human resource, information systems, and even the maintenance/janitorial aspects of the firm’s activities. The assignment of such oversight responsibility to an individual who lacks sufficient authority within the organization will not impress a court. Compliance standards should be clear and understood by the assigned individual, whose performance should be measured against the fulfillment of his or her oversight responsibilities.

C. Use of Due Care in Delegating Discretionary Authority  

The organization must have used due care not to delegate substantial discretionary authority to individuals whom the organization knew, or should
have known through the exercise of due diligence, had a propensity to engage in illegal activities.\footnote{See id. at § 8A1.2, Commentary: 3(k)(3).}

A company’s Human Resources (HR) Department should avoid hiring an employee in any position that increases the possibility that sensitive information will be brought into the organization.\footnote{See, e.g., Protecting Trade Secrets Requires Many Approaches: Economic Espionage Act a New Tool in War on Intelligence Theft, CORPORATE LEGAL TIMES, Oct. 1998, at 54 (discussing an example of how Heinz decided not to hire an individual coming from a competitor due to the risk of contamination).} An inventory of the applicant’s exposure to trade secrets prior to entering the firm should be taken. Care must be exercised not to have the prospective employee reveal the exact nature of the information; rather, any revelation should be limited to the overall category or classification of the information. In fact, it is important for the HR Department to make it clear that the company does not want to know the trade secrets of others.\footnote{See Victoria Cundiff, IP Pitfalls: Don’t Let the Economic Espionage Act Penalize You, INT. PROP. STRATEGIST, Jan. 1998, available in Lexis-Nexis (Legal News) [hereafter IP Pitfalls] (“Make it clear that ‘we do not want others’ secrets.’”). See also Victoria Cundiff, Hiring Competitors’ Employees: A Trade Secrets Perspective, CORPORATE COUNSEL, Nov. 17, 1997, at S7 [hereafter Hiring Competitors] (“Companies should routinely advise all applicants at the outset that they are interested in learning about the applicant and seeing whether there is a fit, not in learning anyone’s confidential information.”)} Once hired, it may be necessary for new employees to go through a “decontamination” process with the HR Department prior to allowing them to work alongside other company employees. This decontamination process should involve having an HR employee conduct an initial interview, at which time new employees should be warned against revealing any other firm’s trade secrets to company employees.

A review of prospective employees’ prior noncompete, nondisclosure and nonuse agreements should also be undertaken.\footnote{Cundiff, Hiring Competitors, supra note 349, at S7.} Asking prospective employees for copies of any such agreements, plus warning them that the firm’s TSCP requires prior notification to the former employer, will send a strong compliance message to everyone involved. Once the employment period begins, the company should also avoid placing new employees in areas of the firm where the chances for the inappropriate use of the secrets could result in contamination of the firm. Thus, an inventory of these likely areas should be made and tracked.\footnote{See id. at S7, S12.} Employee promotions and transfers should also be monitored to avoid contamination problems.

The HR Department should also integrate new employees into ongoing education programs and provide orientation for such employees at the time of
hiring.\textsuperscript{352} Lastly, new employees should be required to sign appropriate nondisclosure, noncompete and nonuse agreements.

D. Effective Communication to Employees and Agents

\textit{The organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents, e.g., by requiring participation in training programs or by disseminating publications that explain in a practical manner what is required.}\textsuperscript{353}

It is essential to properly communicate the terms and implications of the TSCP to the appropriate audience. Employees that are involved in a company’s competitive intelligence activities particularly need to be integrated into the communication and education process.\textsuperscript{354} The mechanisms for communication vary and include the use of newsletters, required attendance at training workshops, company announcements, and recommendations from outside consultants. Most of the communication will likely be funneled through the HR Department, particularly communications aimed at employees entering and exiting the firm.

Communicating trade secret protection procedures to all employees and agents will often be a difficult but necessary task. Potential “agents” may include subcontractors, suppliers, joint venture partners, consultants, and even researchers and universities. Researchers and universities are particularly problematic given their inherent tendency and incentive to disseminate information to others. Developing a strong “in-house” TSCP is of little value if these numerous “outside” agents have the ability to disclose secrets with impunity. Consultants and suppliers both tend to thrive on their ability to pick up scraps of information at one business and then spread that information to the next firm. Companies must closely scrutinize and reevaluate the ways in which they deal with such agents.

The increased use of outside agents and temporary employees presents serious EEA issues. Most U.S. companies fail to conduct background investigations of such individuals.\textsuperscript{355} These hires not only pose a risk for trade secret loss, but also present the same contamination issues as permanent hires. However, the EEA places an onerous burden on HR managers in this regard. The significant burdens of background checks, noncompetition and noncompete agreements, as well as post-employment follow-up, are exponentially compounded when applied to such individuals. Perhaps the best precaution is to, whenever possible, restrict the use of

\textsuperscript{352} See id.

\textsuperscript{353} See \textit{Sentencing Guidelines, supra} note 332, at § 8A1.2, Commentary: 3(k)(4).

\textsuperscript{354} See Cundiff, \textit{IP Pitfalls, supra} note 349.

\textsuperscript{355} See \textit{Survey Report, supra} note 23, at “Question 17(d).”
such individuals to activities not involving sensitive information. Unfortunately, at
many U.S. businesses, such individuals have nearly the same access to sensitive
company information as regular employees.\(^{356}\)

An excellent example of the problems that can occur with outside agents is
illustrated in *Hoffmann-La Roche, Inc. v. Yoder*.\(^{357}\) Hoffmann-La Roche (Roche) is a
pharmaceutical manufacturer. Roche worked with Dr. Yoder, an independent
physician, in clinical trials of the new drug called “Accutane.” Dr. Yoder utilized the
drug in his private practice from 1977 to 1983. During the clinical trials, Roche
provided Dr. Yoder with substantial technical information relating to the drug. Only
three of approximately 550 contested pages provided by Roche were stamped
confidential. In 1996, Dr. Yoder placed an advertisement in *The Washington Post*
offering to sell his entire collection of Accutane documents by sealed bid, with a
minimum bid of $9.5 million. His advertisement indicated that his collection
included a never before released document possibly linking Accutane to birth
defects.\(^{358}\)

Roche sought an injunction to prevent the sale, arguing that the documents
constituted trade secrets and were therefore protected under Ohio’s state trade secrets
laws. A key issue in the case was whether Roche had taken reasonable efforts to
maintain secrecy. Although Roche had taken what the court considered to be
“extraordinary efforts”\(^{359}\) to keep the material confidential within the firm, there was
nearly a total absence of controls placed on outside agents, such as Dr. Yoder. Roche
had no confidentiality agreement, written or oral, with Dr. Yoder, and only after he
published an article critical of Roche did Roche indicate a need for confidentiality.\(^{360}\)

Although there were approximately 20 such drug trials being conducted around
the country, Roche was unable to confirm through documentation any efforts to
maintain secrecy outside the organization. In addition, it had no policy regarding the
retrieval of documents upon completion of drug trials, nor could it document for the
court the location within the country of all copies of the documents claimed to be
trade secrets.\(^{361}\) The court found that Roche had lost its statutory and common law
trade secret protection because it had failed to “maintain the secrecy of the contested

\(^{356}\) See *id.* at Item 17(l).

\(^{357}\) 950 F. Supp 1348 (S.D. Ohio 1997).

\(^{358}\) See *id.* at 1350-52.

\(^{359}\) *Id.* at 1360.

\(^{360}\) See *id.* at 1360-64.

\(^{361}\) See *id.* at 1363.
documents at the time the Accutane trials were initiated, and in the years thereafter.  

As this case illustrates, the consequences of failing to follow reasonable trade secret procedures, with outside agents in particular, can be devastating.

E. Reasonable Steps to Achieve Compliance

The organization must have taken reasonable steps to achieve compliance with its standards, e.g., by utilizing monitoring and auditing systems reasonably designed to detect criminal conduct by its employees and other agents and by having in place and publicizing a reporting system whereby employees and other agents could report criminal conduct by others within the organization without fear of retribution.

The compliance process involves two types of monitoring. First, one must evaluate the company’s operations and monitor behaviors so that violations are likely to be discovered. In this regard, records should be maintained to demonstrate that the company took reasonable steps to notice any activity that might suggest the misappropriation of a trade secret. Second, the compliance process should assess the effectiveness of the system on a regular basis and make any necessary changes.

An effective TSCP will also encourage employees and agents to notify management of any violations or inappropriate activities with no negative consequences to the person so reporting. Very likely, this will involve reporting not to the individual in the normal chain of authority, but to an individual specifically designated as a recipient of such concerns. Resolving this issue will require close coordination between the firm’s HR Department and the executive in charge of trade secret compliance. Just as it would be a simple task for the FBI to conduct a “sting” operation by sending an anonymous package containing a competitor’s purported trade secrets on computer disk, the firm could just as easily let its employees know that it will conduct its own internal “sting” operations and reward employees who respond appropriately.

The company should also strive to raise awareness of the significant liability that attaches for failing to comply with the law. This effort should be directed to persons at all levels of the organization. All employees and agents should be apprised of how to identify possible problems, and what to do if they come across improper information. Such a plan must be specific, not general. Specificity will help not only guide employees and agents, but also will make the audit and control function much easier.

362 Id. at 1364.

F. Consistent Enforcement

The standards must have been consistently enforced through appropriate disciplinary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense. Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific. 

Discipline should be a matter that is well thought out and consistent with other serious disciplinary matters within the organization. Disciplining an employee’s negative behavior is as important as rewarding positive behavior. A TSCP that provides no disincentives for stealing or accepting a competitor’s trade secrets will likely be frowned upon by the courts. Again, the need for close coordination between the trade secret compliance officer and the HR Department becomes apparent. Management must be as willing to punish noncompliance as it is to reward compliance.

G. Appropriate Response to Known Violations

After an offense has been detected, the organization must have taken all reasonable steps to respond appropriately to the offense and to prevent further similar offenses—including any necessary modifications to its program to prevent and detect violations of law. The Sentencing Guidelines clearly place a responsibility upon the firm to have a program designed to detect its own violations of the EEA. The commentary to the guidelines provide the following analogous examples:

If because of the nature of an organization’s business there is a substantial risk that certain types of offenses may occur, management must have taken steps to prevent and detect those types of offenses. For example, if an organization handles toxic substances, it must have established standards and procedures designed to ensure that those substances are properly handled at all times. If an organization employs sales personnel who have flexibility in setting prices, it must have established standards and procedures designed to prevent and detect price-fixing. If an organization employs sales personnel who have flexibility to represent the material characteristics of a product, it must have established standards and procedures designed to prevent fraud.

Factors to be considered in determining criminal sanctions include whether the company “within a reasonably prompt time after becoming aware of the offense, reported the offense to appropriate governmental authorities, fully cooperated in the investigation, and clearly demonstrated recognition and affirmative acceptance of

364 See id. at § 8A1.2, Commentary: 3(k)(6).
365 See id. at § 8A1.2, Commentary: 3(k)(7).
366 See id. at § 8A1.2, Commentary: 3(k)(7)(ii).
responsibility for its criminal conduct .” 367 This also means that the company should notify the owner of the stolen secret at issue. This type of self-policing by a company cannot be overemphasized. It can help minimize penalties, and where applicable, may even help convince government prosecutors that the company was the victim of a renegade employee or agent.

VII. Conclusion

The plain language of the threshold elements needed to establish an EEA violation, coupled with Congress’ intent to narrowly construe the statute and its application, reveals a statute that while predicted to be a powerful tool to combat trade secret theft, has thus far proven to have a fairly narrow application. However, despite this narrow application, the EEA has nevertheless filled a significant gap in the protection of trade secrets and has been an important and positive step forward in the battle against trade secret theft. It will be interesting to see if over time the government loosens the leash on the Act and becomes more aggressive in its enforcement efforts, such as by bringing actions under section 1831 (the foreign activity section). Should that occur, that will be yet another reason for American companies to familiarize themselves with the EEA and adopt the applicable TSCP recommendations noted herein.

367 See id. at § 8C2.5(g)(1) (culpability score).