8 Tex. Intell. Prop. L.J. 159

Texas Intellectual Property Law Journal
Winter, 2000

THE ECONOMIC ESPIONAGE ACT: BEAR TRAP OR MOUSETRAP?

Chris Carr[a1] Jack Morton[aa1] Jerry Furniss[aaa1]

Table of Contents

***161 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 ***162** 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, ***163** "stealth" technologies, lasers, manufacturing processes and semi-conductors.[13] Victims were not just the naïve and unsophisticated--they included such corporate giants as GM, Intel, Lockheed Martin and Hughes Aircraft.[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.[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.[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 ***164** 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."[17] 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."[18] As also earlier noted, the FBI has reported that at least 23 countries actively engage in economic espionage activities against U.S. companies.[19] Disturbingly, some of these countries are our purported allies.[20] Indeed, with the end of the Cold War, it is no longer business as usual.[21]

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 ***165** customer list or confidential pricing information onto a computer disk, slip it into his or her pocket or briefcase, and walk out the door.[22] 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.[23]

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."[24]

*166 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* ***167** *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.[31]

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.[32] Such an admission can be embarrassing, adversely affect stock prices and market share and/or scare away customers and investors.[33] Many executives would rather bury such losses in earning statements than admit they "lost the family jewels."[34] 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.[35]

***168 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.[36] That statute provides for criminal penalties for the unauthorized disclosure of trade secrets by a *government* employee.[37] 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.[38] 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.[39] Unfortunately, the ITSP was passed at a time when information did not have the economic value and "form" that it has today.[40] The primary deficiency with the ITSP is that it only applies to """"goods, wares and merchandise," not intangibles such as trade secrets.[41] Further, the ITSP by its very terms does not apply to thefts of ***169** intellectual property that do not cross state lines or involve foreign commerce.[42] 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[43] and Wire Fraud[44] statutes criminalize any scheme involving the use of the mails or an interstate wire transmission to obtain "property" by false pretenses or representation.[45] 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).[46] Unfortunately, however, trade secret misappropriation often does not involve the use of interstate mail or wire, a requirement of these statutes.[47] 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.[48] Thus, as with the ITSP, these statutes are of little use in combating espionage and trade secret theft in today's business environment.

***170 3. State Laws**

Today the majority of states provide for some form of civil remedy for the theft of confidential and proprietary information.[49] One state model is based on section 757 of the *Restatement Second of Torts.*[50] 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.[51]

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.[52]

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.[53]

***171 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.[54]

1. Secrecy

As noted in the above definition, the owner of the information must take "reasonable measures" to keep it secret.[55] 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."[56] Thus, the critical question becomes, "What constitutes a reasonable measure under the EEA?" There is, of course, no definitive answer.[57] The drafters of the Act stated that "what constitutes ***172** reasonable measures in one particular field of knowledge or industry may vary significantly from what is reasonable in another field or industry."[58] While no "heroic or extreme measures" are necessary,[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."[60]

2. Value

In order for an item to qualify as a trade secret under the EEA, it must also have *value.*[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."[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.[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.[64] A career with a single company has become the exception, not the norm.[65] Consider the following:

> ***173** 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]

***174 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."[70] It can also involve "looking at or tasting a lawfully acquired product in order to determine its content."[71] "Parallel development" involves the creation or discovery of a trade secret as a result of one's own honest effort and hard work.[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.[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 *Smith vs. Dravo Corp.,*[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."[75] The U.S. Supreme Court has also stated that "trade ***175** secret law … does not offer protection against discovery by fair and honest means such as by independent invention."[76]

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.[77] Under this section, criminal penalties will occur when an accused:

> [I]intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing [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.[78]

Thus, this section encompasses the "knowing"[79] misappropriation of trade secrets by foreign governments and agents, as well as anyone acting on their behalf.[80] ***176** 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.[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"[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 ….[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."[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.[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.[86] Further, a court *may* order the forfeiture to the government of any property used to commit or facilitate the violation.[87] While the proceeds and property in question are forfeited to the United ***177** 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- ***178** Myers Squibb) because those documents contained the company's trade secrets.[97] 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.[98] 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.[99]

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.[100] 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.[101]

The district court agreed with Hsu.[102] The government appealed, and on August 26, 1998, the Third Circuit Court of Appeals *reversed* the district court's ruling.[103] 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.[104] 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 ***179** under such circumstances would deter the reporting of theft and prosecutions under the Act.[105]

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.[106]

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."[107] 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.[108] 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."[109] 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]

*180 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 ***181** months of imprisonment and three years probation.[119] Daniel Worthing also pled guilty and was sentenced to five years probation and six months of home detention.[120]

B. The *Hsu* Case[121]

Kai-Lo Hsu, a Taiwanese national, was a technical director for Taiwan's Yuen Foong Paper Company.[122] Chester Ho, also a Taiwanese national, was a biochemist and professor at Taiwan's National Chiao Tung University.[123] These two individuals were arrested in June 1997 at the Four Seasons Hotel in Philadelphia as a result of an FBI sting operation.[124]

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.[125] 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.[126] Hsu and Chou allegedly agreed to make a preliminary payment of $400,000 for the Taxol information.[127] Chester Ho accompanied Hsu to the June meeting at the Four Seasons Hotel to allegedly verify the value of the secret Taxol information.[128]

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).[129] Specifically, the indictment charged violations of sections ***182** 1832(a)(4) (the EEA's attempt provision) and 1832(a)(5) (the EEA's conspiracy provision).[130] 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.[131]

On March 31, 1999, Hsu pled guilty to one count of conspiring to commit trade secret theft.[132] He was sentenced to two years probation and fined $10,000.[133] All other charges against him were dropped.[134] In early 1999 the government dropped all charges against Chester Ho.[135] Chou, the person who allegedly sought out the secret Taxol information for Hsu, remains the subject of a federal arrest warrant.[136] 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.[137]

C. The *Four Pillars* Case[138]

Pin Yen Yang was the Chief Executive Officer of Four Pillars Enterprise Company, Ltd. of Taiwan.[139] Four Pillars manufactures and sells pressure sensitive devices, employs more than 900 people, and has an annual revenue of more than $150 million.[140] Hwei Chen Yang is Mr. Yang's daughter.[141] She is also a Ph.D. chemist, corporate officer, and employee at Four Pillars, and is believed to hold dual ***183** citizenship in the United States and Taiwan.[142] Avery Dennison Corporation is based in California, manufactures and sells adhesive products, and employs approximately 15,000 people world-wide.[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."[144] The Yangs were arrested in September 1997 as part of an FBI sting operation.[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.[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.[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.[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.[149]

The Yangs were originally indicted on 21 counts of various charges.[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.[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.[152]

***184** By the end of the proceeding, 19 of the 21 charges against the Yangs were dropped (e.g., the mail and wire fraud charges).[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.[154] This was the first case to actually proceed to trial under the EEA.[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.[156]

D. The *Gillette* Case[157]

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

At Gillette's request, Wright Industries removed Davis from the project.[162] Thereafter, Davis downloaded 600 megs of secret data and drawings from the project onto his laptop computer.[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.[164]

***185** Davis was charged with violating section 1832 of the EEA and wire fraud.[165] 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.[166]

E. The *Deloitte & Touche* Case[167]

Mayra Trujillo-Cohen was a former consultant for Deloitte & Touche[168] The government filed a two count indictment against her for violating sections 1832(a)(2) and (4) of the EEA and wire fraud.[169] 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.[170] 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.[171]

F. The *Atlanta Journal & Constitution* Case[172]

Caroll Lee Campbell was a circulation manager for the *Gwinnett Daily Post,* a newspaper owned by Gray Communications, Inc.[173] Paul Soucy was the district circulation manager of the *Rockdale Citizen* (a sister paper to the *Gwinnett Daily Post*).[174]

In September 1997, the *Gwinnett Daily Post* and *Atlanta Journal & Constitution* (a rival to the *Post*) were involved in litigation regarding who had the ***186** right to publish Gwinnett County legal notices.[175] 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.*[176]

If the *Atlanta Journal & Constitution* was interested in his offer, it was to put certain ads in the “personals” section of its paper.[177] In cooperation with the FBI, the *Atlanta Journal & Constitution* did so.[178] Campbell subsequently met with an undercover agent at a local shopping center.[179] 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.[180] After Campbell obtained the $5,000, his wife, Susan Campbell, allegedly gave $1,500 to Soucy.[181] Soucy allegedly acted as a lookout for Campbell at the local shopping center meetings.[182]

The Campbells were charged with violating sections 1832(a)(1) through (5) of the EEA, as well as the federal mail fraud statute.[183] Soucy was charged with violating section 1832(a)(5) of the EEA.[184] Mr. Campbell eventually pled guilty to conspiring to steal trade secrets.[185] On August 25, 1998, he was sentenced to three months of imprisonment, three years supervised release, and $2,800 in restitution.[186] Soucy also pled guilty and was sentenced to three years probation, a $1,000 fine, and $500 restitution.[187] After Mr. Campbell was sentenced, the government dropped the charges against Mrs. Campbell.[188]

*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 ***188** Wilsonart to assist it in taking this technology to full scale application.[202] Vactec owns the coating machine that was used to test the coating process of press plates that Wilsonart developed.[203]

Michael Hadwin is the owner of Federal Industrial Services, Inc. (FIS), also a Michigan based business.[204] FIS was contacted by Amis regarding assistance in preparing his coating machine for use in testing the Wilsonart process.[205] 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.[206]

From 1992 through 1996, Wilsonart invested over $750,000 in research-related activities directly associated with the press plate coating technology.[207] 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.[208] Upon being contracted by Krumrei, CSR notified Wilsonart.[209]

Krumrei was arrested as a result of an undercover sting operation.[210] Krumrei was charged with violating section 1832(a)(2) of the EEA.[211] On July 27, 1999, he pled guilty.[212] Krumrei has not yet been sentenced.[213]

I. The *Indexx Labs* Case[214]

Caryn Camp was a chemist and technical service representative at Indexx Labs, a Maine-based manufacturer of veterinary products.[215] Steven Martin was a ***189** 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]

*190 J. The *Intel* Case[227]

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.[228] The computers had been stolen in April 1998 from an Intel facility in California.[229] 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.[230] 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.[231]

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.[232] It also sought the forfeiture of the truck that the defendants used in committing the alleged EEA violations.[233] Both defendants pled guilty.[234] Hallstead was sentenced to 77 months in prison and a $10,000 fine.[235] Pringle was sentenced to 60 months of imprisonment and a $50,000 fine.[236]

K. The *Joy Mining* Case[237]

John Fulton was a former employee of Joy Mining Machinery, Inc.[238] Fulton allegedly contacted a Joy employee and offered to purchase, for $1,500, confidential ***191** diagrams that he intended to use when he started his own competing business.[239] The FBI was alerted and Fulton was arrested as a result of an undercover operation.[240]

Fulton was charged with violating section 1832(a)(1) of the EEA.[241] He pled guilty and was later sentenced to five years probation and 12 months of home detention.[242]

L. The *RAPCO* Case[243]

Matthew Lange was an employee of Replacement Aircraft Parts Company, Inc. (RAPCO), a Wisconsin firm.[244] He had worked at the firm as a draftsmen/designer from June 1995 through May 1996.[245] Part of his job entailed copying to a removable data cartridge his employer's confidential engineering drawings.[246] After Lange left his employment, he attempted to sell these drawings--which belonged RAPCO--over the Internet to a RAPCO competitor for $100,000.[247] Lange sent an e-mail to a person that he believed was a potential buyer, but in reality was a confidential FBI informant.[248]

Lange was indicted on two counts of attempted trade secret theft, one count of copyright infringement, and three counts of wire fraud.[249] The indictment also contained a forfeiture allegation.[250] After a bench trial, in December 1999 Lange was found guilty on all counts.[251] A sentencing hearing has yet to be scheduled.[252]

*192 M. The *Preco* Case[253]

Preco Industries, Inc. is a Kansas based firm that designs, manufactures, and sells industrial equipment.[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.[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).[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).[257] The information alleges that Sindelar was the person responsible for providing these trade secrets to these competitors.[258]

Sindelar was charged with violating section 1832(a)(2) of the EEA.[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.[260]

N. The *Varian Associates* Case[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.[262] David Kern was an installation services manager for Varian Oncology Systems.[263] He worked for Varian from approximately 1991 through the time he was fired in 1995.[264]

***193** 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 ***194** union bank account in Houston, Texas.[276] Tampoe pled guilty to the counts of attempted theft of a trade secret and forfeiture.[277] He was sentenced to 15 months of imprisonment, two years probation and a $100 special assessment.[278]

P. The *3Com* Case[279]

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

Eun Joong Kim was employed at 3Com as a software engineer.[283] In June 1993, another 3Com employee-engineer saw Kim sitting at a workstation that was outside the space where Kim normally worked.[284] The employee also noticed Kim copying files onto a computer disk.[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.[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.[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.[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 ***195** that 3Com would fire him if it discovered he had copied this source code.[289] He was then arrested in the airport and transported to the FBI's Chicago's office.[290] Kim has been charged with violating section 1832(a)(4) of the EEA.[291]

Q. The *Caterpillar* Case[292]

Jack Shearer is the owner of two Texas energy industry parts companies.[293] 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.[294] Shearer purportedly used this stolen information to build an $8 million business.[295] 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.[296] After Solar Turbine was tipped off that its plans were being stolen, it contacted government authorities.[297]

Shearer was charged with two counts of conspiracy to steal trade secrets.[298] He has admitted to corporate spying and pled guilty to EEA violations.[299] Two of Solar Turbine's employees have also agreed to plead guilty to EEA violations.[300] Sentencing is pending.[301] The third employee has yet to be charged.[302]

*196 R. The *Fina Oil* Case[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.[304] The information charges him with a single count of violating section 1832(a)(2) of the EEA.[305] Costello has pleaded not guilty.[306] According to the case docket sheet, a trial date was set for

February 22, 2000.[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.[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.[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."[310] Thus, to the extent that there were fears that the ***197** 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"[311] or that it would "destroy employee mobility."[312]

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.[313] 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.[314] 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.[315]

In several cases, the indicted individuals and/or important players were outside agents, independent contractors or temporary employees (versus full-time regular employees),[316] thereby confirming an ASIS report that such individuals often pose the greatest threat to a company's trade secrets.[317] 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 ***198** activities.[318] However, in light of the cases the government has filed thus far, this fear appears to have been misplaced.[319]

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.[320] 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.).[321] 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.

***199** 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 ***200** 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.[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[332] promulgated by the United States Sentencing Commission[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."[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 ***201** guidelines refer to the desire to motivate businesses to adopt "mechanisms" for the detection and prevention of trade secret theft.[335] 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]

***202** 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]

***203** 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.[345]

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.[346]

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 ***204** *have known through the exercise of due diligence, had a propensity to engage in illegal activities.*[347]

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.[348] 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.[349] 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.[350] 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.[351] 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 ***205** hiring.[352] Lastly, new employees should be required to sign appropriate nondisclosure, noncompete and nonuse agreements.

D. Effective Communication to Employees and Agents

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.[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.[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.[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 ***206** 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 ***207** documents at the time the Accutane trials were initiated, and in the years thereafter."[362]

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.[363]

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.

*208 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.[364]

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.[365]

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.[366]

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 ***209** 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.

Footnotes

a1 Assistant Professor of Business Law and Public Policy, California Polytechnic State University--San Luis Obispo. Of Counsel, Jencks Law Group, Arroyo Grande, California.

aa1 Professor of Business Law, University of Montana.

[aaa1] 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.

[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).

[4] Richard J. Heffernan & Dan T. Swartwood, *Trends in Intellectual Property Loss Survey, Sponsored by the American Society for Industrial Security,* Mar. 1996, at 4. *See also* H.R. REP. NO. 788, 104th Cong., 2d Sess., at 5-6 (Sept. 16, 1996) [hereafter *House Report*] (citing an ASIS survey); and Neal R. Brendel & Lucas G. Paglia, *The Economic Espionage Act,* PENN. LAW WEEKLY, July 7, 1997, at 12.

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

[6] Stan Crock & Jonathan Moore, *Corporate Spies Feel a Sting,* BUS. WEEK, July 14, 1997, at 77.

[7] *See, e.g.,* Peter J.G. Toren, *The Prosecution of Trade Secrets Thefts Under Federal Law,* 22 PEPP. L. REV. 59, 62 (1994) ($1.8 billion); House Judiciary Panel Backs Stiffer Penalties for Economic Spying, WALL. ST. J., Sept. 12, 1996 ($24 billion); 142 CONG. REC. S12211-12 (1996) (statement of Senator Kohl) ($63 billion); 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. 2 (1996) (statement of Senator Specter) [hereafter *Specter Statement*] (estimating a loss of $100 billion per year).

[8] *See U.S. Losing High-Tech Secrets to "Student" Spies,* STRAITS TIMES (Singapore), Apr. 8, 1997, *available in* Dow-Jones News (Publications Library) (reporting that the International Trade Commission estimates one million jobs lost); *Specter Statement, supra* note 7, at 2 (noting an ABC News report of six million jobs lost); Candace L. Preston, *Out-of-work Spies Find New Niche in Corporate Espionage: Economic Espionage Act of 1996,* BUSINESS FIRST-COLUMBUS, Nov. 28, 1997, *available in* Dow-Jones News (Publications Library) (also reporting six million jobs lost).

[9] *Hearing on Economic Espionage: Statement of Louis J. Freeh (Director of the Federal Bureau of Investigation) Before the Senate Select Committee on Intelligence and Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology, and Government Information,* Feb. 28, 1996 [hereafter *Freeh Statement*], at 12.

[10] Peter Schweizer, *The Growth of Economic Espionage: America is Target Number One,* FOREIGN AFF., Jan./Feb. 1996, at 11.

[11] *See id.*

[12] *CIA Fingers France, Israel for Economic Espionage,* ORLANDO SENTINEL TRIB., Aug. 15, 1996, at A12. *See also* Thomas J. Jackamo III, *From the Cold War to the New Multilateral World Order: The Evolution of Covert Operations and the Customary International Law of Non-Intervention,* 32 VA. J. INT'L L. 929, 944 & n.88 (1992) (stating that the Netherlands, Belgium, and Scandinavian countries also pose a significant threat to the United States); Richard Behar, *Who's Reading Your E-mail?,* FORTUNE, Feb. 3, 1997, at 61, 64 (adding Germany, Japan, Canada, and India to the list).

[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.

[14] Farnham, *supra* note 1, at 114.

[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).

[16] Timothy D. Foley, *The Role of the CIA in Economic and Technological Intelligence,* 18 FLETCHER F. WORLD AFF. 135, 143 (Winter/Spring 1994); Robert Dreyfuss, *Tinker, Tailor, Silicon Spy,* Cal. Law., at 39 (1996) (statement by an FBI agent that Silicon Valley is an "enormous target"); John Berthelsen, *Friendly Spies,* FAR E. ECON. REV., Feb. 17, 1994, at 28; Norm Alster, *The Valley of the Spies,* FORBES, Oct. 26, 1992, at 200.

[17] *House Report, supra* note 4, at 5. *See also* S. REP. NO. 359, 104th Cong., 2d Sess., at 7 (1996) [hereafter *Senate Report*].

[18] United States v. Kai-Lo Hsu, 155 F.3d 189, 194, 47 U.S.P.Q.2d (BNA) 1784, 1787 (3d Cir. 1998). For an excellent article on this issue, *see* Mark A. Moyer, *Section 301 of the Omnibus Trade and Competitiveness Act of 1988: A Formidable Weapon in the War Against Economic Espionage,* 15 J. INT'L L. & BUS. 178 (1994). *See also* Darren S. Tucker *The Federal Government's War on Economic Espionage,* 18 U. PA. J. INT'L ECON. L. 1109, 1113-14 (1997) ("Companies around the world have become more vulnerable to trade secret theft for several reasons. First, the end of the Cold War made available intelligence resources previously devoted to securing military technology."); James D. Veltrop, *Trade Secret Misappropriation a Federal Crime,* INT. PROP. TODAY, June 1997, at 6 ("The new 'Cold War' revolves around the battle for technology."); Farnham, *supra* note 1, at 114 ("The end of the Cold War did not spell an end to spying. It merely changed its focus. Foreign spooks, who otherwise would be out of work, have been assigned commercial tasks."); Mark Grossman, *Spying Eyes Are Watching You; Protecting Trade Secrets Is No Easy Task,* TEXAS LAW., Sept. 28, 1998, at 44 ("We also live in a post-Cold War world--in which some former military spies now find private employment and engage in economic espionage for foreign governments and companies.").

[19] *See Freeh 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).

[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).

[23] *See* the webpage of Attorney Mark Halligan at ‹http:// www.execpc.com/~mhallign/crime.html› at ¶ 5. Halligan is a Chicago attorney and teaches an advanced trade secrets course at John Marshall Law School. *See also* Veltrop, *supra* note 18, at 6 (noting the "burgeoning use of computers and the Internet to facilitate the theft and transmission of confidential databases and technology"). Cases involving the Church of Scientology and its efforts to protect its trade secret rights in scriptures also illustrate how trade secret rights can be lost over the Internet. *See, e.g.,* Religious Technology Center v. Lerma, et al., 897 F. Supp. 260, 36 U.S.P.Q.2d (BNA) 1649 (E.D. Va. 1995); Religious Technology Center v. F.A.C.T.NET, Inc., et al., 901 F. Supp. 1519, 36

U.S.P.Q.2d (BNA) 1690 (D. Colo. 1995); and Religious Technology Center v. Lerma, et al., 908 F. Supp. 1362, 37 U.S.P.Q.2d (BNA) 1258 (E.D. Va. 1995). The ASIS also notes that "The Internet and associated technologies are perceived as significant threats to every company's ability to protect the confidentiality of their proprietary information." *See* AMERICAN SOCIETY FOR INDUSTRIAL SECURITY/PRICEWATERHOUSECOOPERS, TRENDS IN PROPRIETARY INFORMATION LOSS: SURVEY REPORT (1998), at "Conclusions from the 1998 Survey" (visited Jan. 15, 2000) ‹ http:// www.pwcglobal.com/extweb/ncsurvres.nsf/DocID/36951F0F6E3C1F9E852567FD006348C5? OpenDocument› [hereafter *Survey Report*].

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.

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

26 Jon Swartz, *Modern Thieves Prefer Computers to Guns,* S. F. CHRON., Mar. 25, 1997, at A1, (statement of Daniel Greer, Director of Engineering for Open Market). *See also Richard J. Heffernan, Testimony with Regard to Economic Espionage Before the House Committee on the Judiciary, Subcommittee on Crime* (May 9, 1996) (noting a survey that found from 1982 to 1992, the market value of manufacturing companies represented by intangible assets rose from 38 percent to 62 percent). *See* S. RPT. NO. 359, 104th Cong., 2d Sess., at 6 (Aug. 27, 1996) (same); and Christopher A. Ruhl, *Corporate Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Proprietary Business Information,* 33 VAL. U. L REV. 763, 766 n.18 (1999) ("[O]btaining and exploiting other people's work rather than creating and developing information from scratch is more simple, easy, and cost effective.").

27 *See* Jeffery Young, *Spies Like Us,* FORBES, June 3, 1996, *available in* Dow-Jones News (Publications Library).

28 Susan E. Davis, *Gangster Tech.,* CAL. LAW., June 1996, at 45.

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.").

31 S. RPT. NO. 359, 104th Cong., 2d Sess., at 11 (Aug. 27, 1996) (emphasis added).

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).

33 *See* 142 CONG. REC. S12209 (Oct. 2, 1996); *Freeh Statement, supra* note 9, at 13. *See generally* Michael A. Epstein & Stuart D Levi, *Protecting Trade Secret Information: A Plan for Proactive Strategy,* 43 BUS. LAW. 887 (1988).

34 RICHARD EELLS & P. NEHEMKIS, CORPORATE INTELLIGENCE AND ESPIONAGE 118 (1984) (quoting a security consultant).

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, 1997, *available in* Lexis-Nexis (Legal News) ("[I]n certain larger disputes, the negative public relations resulting from an admission to the loss of valuable trade secrets or of interference with proprietary technologies, make litigation wholly undesirable.").

36 James H.A. Pooley, Mark A. Lemley & Peter Toren, *Understanding the Economic Espionage Act of 1996,* 5 TEX. INTELL. PROP. L. J. 177, 179 (1997).

37 18 U.S.C. § 1905 (1994 & Supp. IV 1998).

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

39 *See* Spencer Simon, *The Economic Espionage Act of 1996,* 13 BERKELEY TECH. L. J. 305, 306 (1998). The ITSP provides in pertinent part:
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.
18 U.S.C. § 2314 (1994).

40 Simon, *supra* note 39, at 306-07. *See also* Pooley, et al., *supra* note 36, at 180. Relatedly, attorney Mark Halligan notes an exponential increase in trade secret disputes in recent years. In running an Internet search, he found that only four trade secret related stories ran in 1970. In 1980, that number increased to 166. By 1996, it jumped to 3,067. *See* Victoria Slind-flor, *New Spy Act to Boost White-Collar Defense Biz,* NAT'L L. J., July 28, 1997, at A1.

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 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.*

[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)(ii).

[53] *See supra* note 31, and accompanying quote in the text from the Senate Judiciary Committee. For an example of a disheartening and naïve 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.").

[54] 18 U.S.C. § 1839(3) (Supp. IV 1998). Note that unlike the ITSP, this definition specifically includes intangible information such as a trade secret. Further, Congress intended this definition to be read broadly by the courts. *See House Report, supra* note 4, at 11-12. For example, the misappropriation of information stored in an individual's memory could violate the EEA. *See* Jonathan Band, Jamie A, Levitt & Mani Adeli, *The Economic Espionage Act: Its Application in Year One,* THE CORPORATE COUNSELOR, Nov. 1997, *available in* Lexis-Nexis (Legal News). Yet, while this definition *is* broad, the information at issue must still be "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832(a) (Supp. IV 1998). I.e., it appears to exclude the possibility of prosecuting someone for the misappropriation of a trade secret that is related to a *service. See* Pooley, et al., *supra* note 36, at 200.

[55] This is the "threshold issue in every [trade secret misappropriation] case." Microbiological Research Corp. vs. Mung, 625 P. 2d 690, 696, 214 U.S.P.Q. (BNA) 567, 572 (Utah 1981). Note that the EEA also defines the term "owner" broadly. The owner of a trade secret is "the person or entity in whom or in which rightful legal or equitable title to, *or license in,* the trade secret is reposed." 18 U.S.C. § 1839(4) (Supp. IV 1998) (emphasis added).

[56] *See House Report, supra* note 4, at 7.

[57] For a more detailed discussion of how a company might satisfy this "reasonable means" hurdle, *see* discussion in Part VI, *infra.*

[58] 142 CONG. REC. S12213 (Oct. 2, 1992).

[59] *Id.*

[60] *Id.*

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, *Trade Secret Safeguards,* SEC. MGMT., Mar. 1999, at 64.

62 18 U.S.C. § 1839(3)(B) (Supp. IV 1998).

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, *The Economic Espionage Act: A Very Mixed Blessing,* INT. PROP. TODAY, Feb., 1998, *available in* Lexis-Nexis (Legal News).

64 *See, e.g.,* Lawrence B. Ebert, *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 ….

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.").

66 Gerald J. Mossinghoff, J. Derek Mason & David A. Olson, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection,* 79 J. PAT. & TRAD. OFF. SOC'Y 191, 201 (1997).

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.
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.

72 United States Department of Justice Attorneys' Manual, Federal Prosecutions of Violations of Intellectual Property Rights, May 1997, *available at* ‹http://www.usdoj.gov/› (Publications & Documents, U.S. Attorneys' Manual: Title 9--Criminal Resource Manual) [hereafter *DOJ Attorneys' Manual*].

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.

76 Kewanee Oil Co. v. Bicron Corp., et al., 416 U.S. 470, 476, 181 U.S.P.Q. (BNA) 673, 676 (1974). *See also* 142 CONG. REC. S12212 (Oct. 2, 1996) ("[P]arallel development of a trade secret cannot and should not constitute a violation of this statute.").

77 *See* 142 CONG. REC. S12207-08 (Oct. 2, 1996) (Statement of Senator Specter).

78 18 U.S.C. § 1831(a) (Supp. IV 1998). Note the broadness 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 precedent 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.
142 CONG. REC. S10885 (Sept. 18, 1996) (Statement of Senator Kohl).

[81] 18 U.S.C. §§ 1831(a)(5) & (b) (Supp. IV 1998).

[82] *See supra* note 79.

[83] 18 U.S.C. § 1832 (Supp. IV 1998).

[84] *Id.*

[85] 18 U.S.C. § 1832(a)(5) & (b) (Supp. IV 1998).

[86] 18 U.S.C. § 1834(a)(1) (Supp. IV 1998).

[87] 18 U.S.C. § 1834(a)(2) (Supp. IV 1998).

[88] 18 U.S.C. § 1834(a) (Supp. IV 1998).

[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).

[90] 18 U.S.C. § 1836 (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.

[93] 18 U.S.C. § 1835 (Supp. IV 1998). For some good examples of the type of steps a court might take to preserve the confidentiality of such secret information, *see* Gary E. Weiss & K. Alexandra McClure, *Trade Secret Prosecution Risks Further Losses of IP,* NAT'L L.J., June 21, 1999, at C7.

[94] 982 F. Supp. 1022, 44 U.S.P.Q.2d (BNA) 1646 (E.D. Pa. 1997), *rev'd* 155 F.3d 189, 47 U.S.P.Q.2d (BNA) 1784 (3d Cir. 1998).

[95] *See infra* notes 121-137 and accompanying text.

[96] 982 F. Supp. at 1023, 44 U.S.P.Q.2d at 1647.

[97] *See id.,* 44 U.S.P.Q.2d at 1647-48.

[98] *See id.* at 1023-29, 44 U.S.P.Q.2d at 1647-52.

[99] *See id.* at 1023, 44 U.S.P.Q.2d at 1648.

[100] *See id.* at 1023-29, 44 U.S.P.Q.2d at 1647-52.

[101] *See id.* at 1023, 44 U.S.P.Q.2d at 1648.

[102] *See id.* at 1029, 44 U.S.P.Q.2d at 1652.

[103] United States vs. Kai-Lo Hsu, 155 F.3d 189, 47 U.S.P.Q.2d (BNA) 1784 (3d Cir. 1998).

[104] *See id.* at 197-204, 47 U.S.P.Q.2d at 1790-96.

[105] *See id.*

[106] For several interesting articles on the *Hsu* case and this important development under the EEA, see Austin J. McGuigan & William W. Kaliff, *Can You Keep a Secret?,* CONN. LAW TRIBUNE, July 27, 1998, *available in* Lexis-Nexis (Legal News); Efrem M. Grail, W. Thomas McGough, Jr. & Jeffrey M. Klink, *Trade Secrets,* NAT'L L. J., Aug. 17, 1998, at B5; Efrem M. Grail, W. Thomas McGough, Jr. & Jeffrey M. Klink, *Would-Be Thieves: Discovery Not Always Allowed,* NAT'L L. J., Oct. 19, 1998, at C21; Mark D. Seltzer, *Trade Secret Information May Still Be Discoverable to Defend Completed EEA Violations Under Recent Third Circuit Case,* WHITE-COLLAR CRIME REPORTER, Jan, 1999, at 1; and David E. Rovella, *Trial Nears for Untested Secrets Law,* NAT'L L. J., Mar. 8, 1999, at B1.

[107] 18 U.S.C. § 1837(2) (Supp. IV 1998).

[108] *See* Simon, *supra* note 39, at 314.

[109] 18 U.S.C. § 1837(1) (Supp. IV 1998).

[110] *See* Pooley, et al., *supra* note 36, at 204.

[111] 18 U.S.C. § 1838 (Supp. IV 1998).

[112] United States v. Patrick Worthing and Daniel Worthing, Criminal Case No. 97-CR-9 (W.D. Pa., filed Dec. 9, 1996). This was the first case filed by the government under the EEA.

[113] *See* Mark Halligan webpage, *Reported Criminal Arrests Under the Economic Espionage Act of 1996* [hereafter *Halligan Criminal Arrest List*], (visited Feb. 14, 2000) ‹http://www.execpc.com/~mhallign/indict.html›; *15 Months for Selling Secrets,* PITTSBURGH POST-GAZETTE, June 6, 1997, at C3; Joseph R. Savage Jr. & Lauren A. Stagnone, *You Can't Hide Your Spying Eyes: EEA Issues Emerge,* BUSINESS CRIMES BULLETIN (Dec. 1998), *available in* Lexis-Nexis (Legal News).

[114] *See 15 Months for Selling Secrets,* PITTSBURGH POST-GAZETTE, June 6, 1997, at C3; *Halligan Criminal Arrest List, supra* note 113; and Mark D. Seltzer & Angela A. Burns, *The Criminal Consequences of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Your Company's Trade Secrets from Theft and Render Civil Remedies Obsolete?,* SOFTWARE LAW BULLETIN, Feb. 1999, *available in* Lexis-Nexis (Legal News).

[115] *Halligan Criminal Arrest List, supra* note 113.

[116] *See id. See also* Seltzer & Burns, *supra* note 114.

[117] Savage & Stagnone, *supra* note 113.

[118] Criminal Complaint at pp. 1-3 (on file with the authors).

[119] *See* Seltzer & Burns, *supra* note 114; and *Halligan Criminal Arrest List, supra* note 113.

[120] *Halligan Criminal Arrest List, supra* note 113.

[121] United States v. Kai-Lo Hsu, Chester S. Hou and Jessica Chou, Criminal Case Nos. 97-323, 97-1965 (E.D. Pa., filed June 16, 1997).

[122] Indictment at ¶ 7 (on file with the authors). *Halligan Criminal Arrest List, supra* note 113. Frances A. McMorris, *Corporate Spy Case Rebounds on Bristol,* WALL ST. J., Feb. 2, 1998, at B5; Rovella, *supra* note 106at B2; *FBI Charges Taiwanese Tried to Steal Taxol Secrets from BMS,* PHARMACEUTICAL LIT. RPTR., July 1997, at 12413; *ED PA Sentences Taiwanese Businessman to Probation in Taxol Theft Case,* INT. PROP. LIT. RPTR., July 21, 1991, at 7.

[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.

[130] *See id.*

[131] *See id.*

[132] *Halligan Criminal Arrest List, supra* note 113.

[133] *ED PA Sentences Taiwanese Businessman to Probation in Taxol Theft Case,* INT. PROP. LIT. RPTR., July 21, 1991, at 7.

[134] *Halligan Criminal Arrest List, supra* note 113.

[135] *Halligan Criminal Arrest List, supra* note 113; *ED PA Sentences Taiwanese Businessman to Probation in Taxol Theft Case,* INT. PROP. LIT. RPTR., July 21, 1991, at 7.

[136] *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.

[137] *See id.*

[138] 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).

[139] *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).

[140] *Halligan Criminal Arrest List, supra* note 113.

[141] Yang Indictment, *supra* note 139, at ¶ 5. *See also Halligan Criminal Arrest List, supra* note 113.

[142] *Halligan Criminal Arrest List, supra* note 113. *See also DOJ Press Release, supra* note 139.

[143] Yang Indictment, *supra* note 139, at ¶ 1.

[144] *Halligan Criminal Arrest List, supra* note 113.

[145] *See id.*

[146] *See id. See also* Starkman, *supra* note 139, at B4.

[147] *Halligan Criminal Arrest List, supra* note 113.

[148] *See id.*

[149] *See id.*

[150] *See* Yang Indictment, *supra* note 139, at pp. 1-27.

[151] *Halligan Criminal Arrest List, supra* note 113.

[152] *See id.*

[153] *See* Penny Arevalo, Steve Andersen & Bruce Rubenstein, *Circuit by Circuit,* CORPORATE LEGAL TIMES, July, 1999, *available in* Lexis-Nexis (Legal News).

[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).

[155] *Halligan Criminal Arrest List, supra* note 113.

[156] *See id.*

[157] United States v. Steven L. Davis, Criminal Case No. 97-00124 (M.D. Tenn. 1997).

[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.

[159] Indictment, *supra* note 158, at ¶ 7.

[160] *See id.* at ¶ 11.

[161] *See id.* at ¶ 1.

[162] *Halligan Criminal Arrest List, supra* note 113.

[163] *See id.*

[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.

[165] Indictment, *supra* note 158, at pp. 1, 5 & 8.

[166] *Halligan Criminal Arrest List, supra* note 113.

[167] United States v. Mayra Justine Trujillo-Cohen, Criminal Case No. H-97-251SS (S.D. Texas, filed Nov. 14, 1997).

[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.

[171] *Halligan Criminal Arrest List, supra* note 113. *See also Woman Pleads Guilty,* HOUSTON CHRON., July 31, 1998, *available in* Dow-Jones News (Publications Library).

[172] United States v. Caroll Lee Campbell, Jr. and Susan Campbell, Criminal Case No. 1:98-CR-064 (N.D. Georgia, filed Feb. 6, 1998); United States vs. Paul Edward Soucy, Criminal Case No. 1:98-CR-059 (N.D. Georgia, filed Feb. 6, 1998).

[173] *See Halligan Criminal Arrest List, supra* note 113; and Kelvin Childs, *Feds Arrest Two for Newspaper Espionage,* EDITOR & PUBLISHER MAG., Feb. 21, 1998, at 10.

[174] *See id.*

[175] *Halligan Criminal Arrest List, supra* note 113. *See also Man Offering to Sell Secrets to Rival Newspaper Sentenced,* THE ASSOCIATED PRESS STATE & LOCAL WIRE, Aug. 25, 1998, *available in* Lexis-Nexis (Wire Service Reports).

[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] Campbell Indictment, *supra* note 176, at pp. 1-14.

[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).

[187] Larry Hartstein, *Man Sentenced for Conspiracy,* THE ATLANTA JOURNAL & CONSTITUTION, June 4, 1998, at 13JJ; Emily Heller, *Stolen Plan No Big Secret, But Scheme Costs 90 Days,* FULTON COUNTY DAILY REPORT, Aug. 27, 1998, *available in* Lexis-Nexis (U.S. News, Southeast Regional Sources).

[188] *Heller, supra* note 187.

[189] United States v. Huang Dao Pei, Criminal Case No. 98-M-4090 (D. N.J., filed July 27, 1998).

[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.

[192] *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).

[197] United States vs. David T. Krumrei, Criminal Case No. 98-CR-300-SOM (D. Hawaii, filed May 14, 1998) (transferred on October 28, 1998 to the Eastern District of Michigan, Criminal Case No. 98-CR-80943-1).

[198] Indictment at ¶ 1 (on file with the authors).

[199] *See id.*

[200] *See id.* at ¶ 3.

[201] *See id.* at ¶ 2.

[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.*

[214] United States v. Caryn L. Camp and Steven R. Martin, Criminal Case No. 98-CR-48-P-H (D. Maine, filed Sept. 18, 1998).

[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.

[222] *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). *See also Halligan Criminal Arrest List, supra* note 113.

[223] *Halligan Criminal Arrest List, supra* note 113.

[224] *See id.*

[225] *See id.*

[226] *See id.*

[227] United States v. Steven Craig Hallstead and Brian Russell Pringle, Criminal Case No. 4:98-CR-0041 (E.D. Texas, filed June 2 1998).

[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.*

[229] *See 2 Charged with Trying to Steal Intel Trade Secrets,* THE FORT WORTH STAR-TELEGRAM, June 4, 1998, at Bus. p. 3. *See also Halligan Criminal Arrest List, supra* note 113.

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

[231] *See* Savage & Stagnone, *supra* note 113.

[232] *See* Indictment, *supra* note 228, at pp. 1-8. *See also 2 Charged with Trying to Steal Intel Trade Secrets,* THE FORT WORTH STAR-TELEGRAM, June 4, 1998, at Bus. p. 3.

[233] Indictment, *supra* note 228, at Count 5.

[234] *Halligan Criminal Arrest List, supra* note 113.

[235] *Men Sentenced for Trying to Sell Prototype Computers,* THE ASSOCIATED PRESS STATE AND LOCAL WIRE, Dec. 4, 1998, *available in* Lexis-Nexis (Wire Service Reports).

[236] *See id.*

[237] United States v. John Fulton, Criminal Case No. 98-CR-0059 (W. D. Pa., filed April 17, 1998).

[238] *See* Savage & Stagnone, *supra* note 113.

[239] *See* Information (on file with the authors); Savage & Stagnone, *supra* note 113; and *Halligan Criminal Arrest List, supra* note 113.

[240] *See Sa*vage & Stagnone, *supra* note 113.

[241] *See* Information, *supra* note 239.

[242] *See* Case Docket Sheet (on file with the authors).

[243] United States v. Matthew Lange, Criminal Case No. 99-CR-174 (E.D. Wis., filed Sept. 8, 1999).

[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.

[251] *See Judge Convicts Man in Trade-Secret Case,* MILWAUKEE JOURNAL SENTINEL, Dec. 10, 1999, at 4.

[252] *See* Case Docket Sheet (on file with the authors).

[253] United States v. David F. Sindelar, Criminal Case No. 98-20070 (D. Kan., filed Oct. 16, 1998).

[254] Information at ¶ 1 (on file with the authors).

[255] *See id.* at ¶ 2.

[256] *See id.* at ¶ 3.

[257] *See id.* at ¶ 4.

[258] *See id.* at ¶ 5.

[259] *See id.* at pp. 1-3.

[260] *See* Case Docket Sheet (on file with the authors).

[261] United States v. David B. Kern, Criminal Case No. 99-CR-15 (E.D. Cal., filed Jan. 21, 1999).

[262] *See* Superceding Indictment at ¶ 1 (on file with the authors).

[263] *See id.* at ¶ 2.

[264] *See id.* at ¶ 2. *See also* Torri Still, *A Lesson for the Valley: Thou Shalt Not Steal,* THE RECORDER, Oct. 7, 1999, at 5.

[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).

[274] United States v. Robin Carl Tampoe, Criminal Case No. H-99-158 (S.D. Texas, filed Mar. 23, 1999).

[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).

[276] *See* Superceding Indictment, *supra* note 275, at pp. 2-4.

[277] *See* Case Docket Sheet at pp. 1, 9 (on file with the authors).

[278] *See id.*

[279] United States v. Eun Joong Kim, Criminal Case No. 99-CR-481 (N.D. Ill., filed July 1, 1999).

[280] *See* Criminal Complaint at ¶ 5 (on file with the authors).

[281] *See id.*

[282] *See id.* at ¶¶ 6, 16.

[283] *See id.* at ¶ 7.

[284] *See id.* at ¶ 8.

[285] *See id.*

[286] *See id.* at ¶¶ 9-10.

[287] *See id.* at ¶ 14.

[288] *See id.* at ¶ 18.

[289] *See id.*

[290] *See id.*

[291] *See id.* at p. 1.

[292] United States v. Jack Shearer, et al., Criminal Case No. 99-CR-433 (N.D. Texas, filed December 9, 1999).

[293] *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.

[294] *See id. See also* Information at pp. 1-2 (on file with the authors).

[295] *Halligan Criminal Arrest List, supra* note 113.

[296] *See id.*

[297] *See id.*

[298] *See* Information, *supra* note 294, at pp. 1-4.

[299] *Halligan Criminal Arrest List, supra* note 113.

[300] *See id.*

[301] *See id.*

[302] *See id.*

[303] United States v. Oliver P. Costello, Jr., Criminal Case No. H-99-623 (S.D. Texas, filed October 28, 1999).

[304] Information at p. 1 (on file with the authors).

[305] *See id.*

[306] *See id.*

[307] *See* Case Docket Sheet at p. 4 (on file with the authors).

[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.").

[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.").

[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.*

[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 I. P., MEDIA & ENT. L. 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."

[318] *See, e.g.,* Peter Schweizer, *New Spy Law Could Cramp Economy,* USA TODAY, Feb. 20, 1997, at 15A; Slind-for, *supra* note 40, at A1; Arnold B. Calmann & Bruce I. Goldstein, *Go Directly to Jail: New Federal Law Protects Trade Secrets,* N. J. L. J., Mar. 9, 1998, at 32; Nathan & Perkins, *supra* note 308, at 4; N. Fine, *The Economic Espionage Act: A Wake-Up Call,* SCIP SECOND ANNUAL SYMPOSIA ON ETHICS AND THE LAW PROCEEDINGS, Feb. 1998, at 15; N. Fine, *The Economic Espionage Act: Turning Fear into Compliance,* 8 COMP. INTELL. REV. 20 (1997). Some of the assertions provide:

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.

James Pooley, *Criminal Consequences of Trade Secret Theft: The EEA and Compliance Plans,* 8 COMP. INTELL. REV. 13 (1997).

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.

Economic Espionage Act of 1996: Implications and Protective Measures to be Addressed at CSI NetSec, Feb. 25, 1997, PR NEWSWIRE, *available in* Lexis-Nexis (Wire Service Reports).

[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, Yang, Gillette, Deloitte & Touche, Atlanta Journal & Constitution, Indexx Labs, Intel, RAPCO* and *Varian Associates* cases.

[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.").

331 *See Survey Report, supra* note 23, at "Key Survey Findings."

332 *See* 1998 Federal Sentencing Guidelines, 18 U.S.C.A. at "Chapter 8--Sentencing of Organizations" [hereafter *Sentencing Guidelines*] (visited Jan. 15, 2000) ‹http://www.ussc.gov/1998guid/98chap8.htm›.

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/intrussc.htm› (visited Jan. 15, 2000).

334 *See Sentencing Guidelines, supra* note 332, at "Introductory Commentary."

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.*

336 *Sentencing Guidelines, supra* note 332, at § 8A1.2, Commentary: 3(k)(1)-(7).

337 *See id.* at § 8A1.2, Commentary: 3(k)(1).

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. Kaliff, *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.patentstm.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).

339 Arthur J. Schwab & David J. Porter, *Federal Protection of Trade Secrets; Understanding the Economic Espionage Act of 1996,* PENN. LAW WEEKLY, Aug. 17, 1998, at 14.

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."DD').

[342] *See generally* Harry Wingo, *Dumpster Diving and the Ethical Blindspot of Trade Secret Law,* 16 YALE L. & POL. REV. 195 (1997).

[343] *See Protection of Trade Secrets, Confidential Information, and Goodwill--Beyond the Basics,* Berkent Report, Berkent Legal Services, P.C. (visited Jan. 15, 2000) ‹http://www.berkent.com/art-tsc3.htm›.

[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.

[345] *See* David. J. Berger, James A. Diboise & Monica Mucchetti, *Inevitable Disclosure Law Remains Unsettled,* NAT'L L. J., May 12, 1997, at C38-C40. For example, in Pepsico, Inc. v. Redmond, 54 F.3d 1262, 35 U.S.P.Q.2d (BNA) 1010 (7th Cir. 1995), the court affirmed the granting of a preliminary injunction that prevented the defendant, William Redmond, a general manager of Purchase, Pepsico's New York-based new age and sports drinks, from accepting a similar position with Quaker Oats' Gatorade division. The court held that Illinois' trade secret law permits a plaintiff such as Pepsico to "prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him to rely on plaintiff's trade secrets." 54 F.3d. at 1269, 35 U.S.P.Q.2d at 1016. The court also found that "unless Redmond possessed an uncanny ability to compartmentalize information, he would necessarily be making decisions about Gatorade and Snapple by relying on his knowledge of [Pepsico's] trade secrets." *Id.* The court coupled this finding with its skepticism that Redmond would be able to keep his promise not to violate Pepsico's trade secrets and that Quaker Oats would be able to ensure that none of Pepsico's trade secrets were used. *Id.* at 1270-71, 35 U.S.P.Q.2d at 1017. But for an excellent article that criticizes the expansion of trade secret protection through the inevitable disclosure doctrine, *see* Susan Street Whaley, *The Inevitable Disaster of Inevitable Disclosure,* 67 U. CIN. L. REV. 809 (1999).

[346] *See Sentencing Guidelines, supra* note 332, at § 8A1.2, Commentary: 3(k)(2).

[347] *See id.* at § 8A1.2, Commentary: 3(k)(3).

[348] *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).

[349] *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."DD'). *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.")

[350] Cundiff, *Hiring Competitors, supra* note 349, at S7.

[351] *See id.* at S7, S12.

[352] *See id.*

[353] *See Sentencing Guidelines, supra* note 332, at § 8A1.2, Commentary: 3(k)(4).

[354] *See* Cundiff, *IP Pitfalls, supra* note 349.

[355] *See Survey Report, supra* note 23, at "Question 17(d)."

[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.

[362] *Id.* at 1364.

[363] *See Sentencing Guidelines, supra* note 332, at § 8A1.2, Commentary: 3(k)(5).

[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).

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