Understanding the Economic Espionage Act of 1996¹

James H.A. Pooley,² Mark A. Lemley,³ & Peter J. Toren⁴

American companies have faced the fact, unfortunately, that our laws were written so long ago that they do not deal with the protection of ideas in the way that they should . . .

-- Rep. Zoe Lofgren⁵

I. INTRODUCTION

A significant gap has existed in trade secrets law for many years. Given the increasingly critical importance of trade secrets in the Information Age, one would expect to see strong and effective criminal laws protecting the investment of industry in research and development. Instead, only a minority of states have specifically criminalized the theft of trade secrets, under widely varying standards. Moreover, the specialized resources necessary to investigate and prosecute this sort of crime have not been generally available at the local level. Federal law has provided no effective remedy either, since the depression-era statute covering interstate transportation of stolen goods has been held not to apply to "intangible" intellectual property.⁶

Information is the core asset of many companies. Yet the modern environment of global competition and instant communications forces most organizations to entrust these assets to a more mobile and less loyal workforce. Outsourcing, collaborative engineering and the virtual corporation have substantially increased the risk of loss, through both inadvertence and espionage. With the end of the Cold War, large numbers of former military spies have been released to a commercial world presumably ready to use their skills in other ways. In a recent FBI study, it was estimated that almost two dozen foreign governments have established means of clandestine acquisition of U.S. industrial secrets.⁷

The Economic Espionage Act of 1996 was intended to address both the general need for a federal criminal deterrent against trade secret theft as well as the apparent threat from foreign state-sponsored industrial espionage. This article examines the background of this new law, provides critical analysis of its most important terms, describes the process involved in a reference of trade secret theft to the federal authorities, and suggests practical strategies for businesses to take advantage of this resource as well as to avoid exposure to liability for the mishandling of information belonging to others.

II. BACKGROUND

A. Need for Legislative Reform

1. Introduction

Prior to the passage of the Economic Espionage Act of 1996, there was only a single very limited federal statute that directly prohibited the misappropriation of a trade secret.⁸ When confronted with an allegation that an individual had misappropriated a valuable trade secret, federal prosecutors were forced to turn to a number of federal statutes that were clearly not designed to cover trade secrets. In particular, prosecutors attempted to use the depression-era Interstate Transportation of Stolen Property Act ("ITSP"),⁹ and the Wire Fraud¹⁰ and Mail Fraud¹¹ statutes. However, as will be discussed, a recent court decision severely curtails the use of ITSP and the use of the Mail and Wire Fraud statutes has always been limited because the theft often does not involve the use of mail or wire. In addition, since a thief usually merely copies information and does not necessarily "defraud" the victim permanently of the data, prosecutions are further limited. Finally, while some state criminal trade secret statutes do exist¹², the current patchwork of state statutes leaves prosecutors ill-equipped to deal with foreign espionage. The following section discusses the limitations on the use of ITSP, the Mail and Wire Fraud statutes and the need for specialized legislation in this area.

2. 18 U.S.C. § 2314

The ITSP provides, in pertinent part, as follows:

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 not more than \$10,000 or imprisoned not more than ten years, or both.

This statute was enacted by Congress in 1934 to fill an enforcement gap in the National Motor Vehicle Theft Act.¹³ Both statutes were intended to aid the states in their detection and punishment of criminals who sought to evade state authorities by fleeing in stolen vehicles or with stolen property over state lines. However, since ITSP was drafted at a time when information did not have the economic value it has today and at a time when information could not be quickly copied and instantaneously transmitted to any location in the world, it is not particularly well suited to deal with the theft of intangible property, such as trade secrets. Moreover, in light of *United States v. Brown*,¹⁴ it is uncertain whether ITSP can be used to charge a person with theft of trade secrets where no tangible property was transferred across state lines. In other words, *Brown* casts serious doubt on whether the phrase "goods, wares and merchandise" contained in section 2314 covers intangible property.

The grand jury indicted Brown for violating section 2314 by transporting computer programs, software and source code interstate from Georgia to New Mexico. Brown moved to dismiss the indictment arguing that under *United States v. Dowling*,¹⁵ the government failed to allege that he transferred in interstate commerce "physical goods, wares [or] merchandise" within the meaning of section 2314.¹⁶ The government admitted that it would not be able to prove that the defendant made a copy of the source code using, for example, the company's hard disk or that the defendant had in his possession any tangible property belonging to the company.¹⁷ The trial court ruled that the source code by itself "is not the type of property which is contemplated . . . within the language of the statute, goods, wares or merchandise."¹⁸

The appellate court agreed, citing *Dowling*. In *Dowling*, the defendant was convicted of violating section 2314 following his interstate distribution of bootleg Elvis Presley records. The Supreme Court reversed the conviction and held that it was not Congress' intention that ITSP function as a criminalization

of copyright infringement.¹⁹ The Supreme Court emphasized that its decision did not deal with a situation in which the initial procurement was accomplished by theft or fraud and that the courts have never required that the items stolen and transported remain in entirely unaltered form. The Court emphasized, however, that:

[T]hese cases and others prosecuted under § 2314 have always involved physical 'goods, wares [or] merchandise' that have themselves been 'stolen, converted or taken by fraud.' This basic element comports with the common-sense meaning of the statutory language: by requiring that the 'goods, wares [or] merchandise' be 'the same' as those 'stolen, converted or taken by fraud' the provision seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of the subject goods.²⁰

The *Brown* court, quoting this language, held that "[p]urely intellectual property" such as the source code appropriated by the defendants is not the type of property covered by section 2314: "It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible" and, thus, "cannot constitute goods, wares, merchandise which have been stolen, converted or taken within the meaning of sections 2314 or 2315."²¹ The *Brown* court also stated that the *United States v. Riggs*,²² decision was in error in light of the Supreme Court's decision in *Dowling*.²³

In *Riggs*, the defendants Robert J. Riggs and Craig Neidorf were indicted for wire fraud and interstate transportation of stolen goods. According to the indictment and pleadings, in 1988 Riggs gained unauthorized access to the Southern Bell Data Network (SBDN) and eventually to a sensitive portion of the computer that contained proprietary Southern Bell files, including the enhanced 911 (E911) file which is a universal service for handling emergency calls in a municipality and surrounding unincorporated areas. Riggs "downloaded" a copy of the E911 text file to his home computer located in Atlanta. He then made available a copy of the file to a friend, Craig Neidorf, who was the co-editor of a computer hacker newsletter known as "Phrack." Neidorf downloaded the copy to his home computer in his room at his fraternity house at the University of Missouri. After making various revisions to remove all references to Southern Bell from the text file, Neidorf published it in an issue of Phrack. Riggs and Neidorf were charged with two counts of wire fraud, 13 U.S.C. § 1343, two counts of the interstate transportation of

stolen property, 18 U.S.C. § 2314, and three counts of violating the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(6).

Neidorf challenged the indictment by arguing that the computerized text file could not be considered "goods, wares, [or] merchandise" under section 2314 because that section should be narrowly read and was never meant to cover the theft of intangible computer data. The *Riggs*' trial judge rejected defendant's "disingenuous" argument that he merely transferred electronic impulses across state lines. The court reasoned that in this case "the information in the E911 text file was accessible at Neidorf's computer terminal in Missouri before he transferred it. . . . The mere fact that the information actually crossed state lines via computer-generated electronic impulses does not defeat a charge under section 2314."²⁴ The court then framed the issue as not whether electronic impulses are "goods, wares or merchandise" within the meaning of section 2314, but "whether the proprietary information contained in Southern Bell's E911 text file constitutes a 'good, ware or merchandise' within the purview of the statute."²⁵ Not surprisingly after presenting the issue in this manner, the court reasoned held that "Neidorf's transfer of that information across state lines would clearly constitute the transfer of 'goods, wares, or merchandise' within the meaning of section 2314. This court sees no reason to hold differently simply because Neidorf stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferable, accessible, even salable form."²⁶ The court was thus unwilling to read a "tangibility requirement" into the definition of "goods, wares or merchandise."²⁷

An analysis of the two decisions strongly suggests that *Brown* and not *Riggs* was correctly decided. In particular, if the *Riggs* rationale was followed it would lead to some clearly unintended results. Specifically, the *Riggs* court opined that it was not necessary to resolve whether or not the E911 file constitutes goods, wares or merchandise, since the defendant and others had the ability to "access the information in viewable form from a reliable storage place which also makes the information tangible, transferable, salable and, in this court's opinion brings it within the definition of 'goods, wares, or merchandise' under section 2314." Here, the *Riggs* court was arguably elevating form over substance. In other words, there is no doubt that defendants Riggs and Neidorf misappropriated the computerized text file. However, section 2314 is not directed towards the act of theft, but to criminalize interstate *transfer* of

stolen goods, wares or merchandise. The computer text file was transmitted across interstate lines by Riggs in the form of electronic signals and only became tangible property when the electronic signals were printed on paper. Thus, the court in *Riggs* did not address the real issue, whether purely intangible property is goods, wares or merchandise, but instead determined that the acts of the defendants should be covered by section 2314 because logically, most types of stolen intangible property should not be treated differently from stolen tangible property. If this reasoning were applied to *all* intangible property, it would lead to results clearly not foreseen or intended by Congress. For example, accessing a computer from out of state would necessarily involve the transfer of property across state lines -- there would be no difference, in other words, between "access" and "transfer". Further, section 2314 would apply under certain circumstances, to the interstate transportation of patent-infringing goods. In other words, if a person "steals" an invention that is protected by a patent and then ships in interstate commerce an article manufactured in accord with the stolen patented specifications, he or she could be successfully prosecuted under § 2314 according to the reasoning of the *Riggs* court. Congress surely did not intend to criminalize patent infringement through the back door.)²⁸

If in fact the *Brown* decision was correctly decided and therefore would be followed by other circuits, federal prosecutors are prevented from charging a person with a violation of section 2314 for transporting in interstate commerce a valuable trade secret, if no tangible property was also stolen. The *Brown* decision limits the use by prosecutors of charging a violation of section 2314 to those situations in which a defendant illegally misappropriates a tangible item containing an intangible component. For example, a defendant can be prosecuted for violating section 2314, if the trade secret is written on paper which belongs to the victim and is misappropriated by the defendant. The *Brown* court suggested that such a situation violates section 2314, even where the value of the paper is insignificant and is almost wholly derived from the intangible component.²⁹ However, in an increasingly electronic environment where a thief can transmit the stolen trade secret anywhere in the world electronically, without misappropriating any tangible property owned by the victim, the scope of section 2314 is no longer sufficient. Further, there is no good reason why the law should treat two defendants who both misappropriate equally valuable trade secrets differently, merely because one of the defendants misappropriated the trade secret, for example,

using a computer diskette belonging to the victim. These short-comings of section 2314 underlie Congress's decision to enact the Economic Espionage Act of 1996.

3. Sections 1341 and 1343

The federal Wire and Mail Fraud statutes proscribe devising any scheme, involving use of the mails or of interstate wire transmission, for obtaining "property" by false pretenses or representations.³⁰ Appellate courts have upheld convictions under either one of the two statutes in situations involving the theft of trade secrets even where no violation of section 2314 was found.³¹ The broader scope results from the use of the word "property" in section 1341 and section 1343 as compared to the far narrower phrase "goods, wares and merchandise" used in section 2314. For example, in *United States v. Seidlitz*,³² the defendant used his knowledge of his former employer's computer system to enter the computer system and download computer data. The appellate court upheld the trial court's determination that the software qualified as property within the meaning of the wire fraud statute. The court held that the software was a trade secret, even though similar programs were in the public domain, because defendant's former employer had invested substantial sums to modify the system for his own needs, it was of competitive value and the employer took steps to prevent persons other than clients and employees from using the system.³³ Accordingly, there was sufficient evidence from which a jury could conclude that information stored in the computer system was "property" as used in section 1343.

However, the Mail and Wire Fraud statutes do not completely close the enforcement gap in this area created by *United States v. Brown* because the misappropriation often does not involve the use of interstate mail or wire. Moreover, since a thief often merely copies the information and does not necessarily "defraud" the victim permanently of the data, he cannot be charged with fraud.

4. State Law

State laws do not entirely fill the holes left by federal law. While the majority of states have some form of civil remedy for the theft of trade secrets, either by recognizing a tort for misappropriation of the information or by enforcing contracts governing the use of the information, these civil remedies are often inadequate to compensate a company for the loss of secrets that gave it a market edge. Further, many companies elect not to pursue civil remedies at all for a variety of reasons: defendants are often judgment proof; civil litigation can be extremely expensive and there is no guarantee of success; and private individuals and companies often lack the investigative expertise and resources necessary to prove that a defendant has misappropriated a trade secret. Moreover, only 23 states presently have criminal statutes specifically directed toward the theft of trade secrets³⁴ and the applicability of these state criminal laws is limited by jurisdiction and lack of state resources, particularly in cases with an international component. As a result, by 1995 there was a consensus among law enforcement officials that some sort of federal law was needed.

5. Conclusion

As noted in the legislative history of the Economic Espionage Act, problems with prosecuting the theft of trade secrets under then-current federal criminal law had led United States Attorney's Offices to decline matters that involved employees of U.S. corporations attempting to sell proprietary high technology information to foreign governments.³⁵ The ability to prosecute someone for theft of a valuable trade secret should not turn on whether the individual also stole from the victim a piece of otherwise worthless paper or whether he happened to use mail or some other specific means to transmit it. The only practical way to protect critical U.S. corporate information from thefts by foreign governments and unscrupulous competitors was to enact a single comprehensive scheme which could bring federal resources to bear against sophisticated defendants who steal proprietary information. In response to these concerns, Congressman McCollum introduced the Industrial Espionage Act of 1996 on June 26, 1996.³⁶ This bill was to eventually become the Economic Espionage Act of 1996. As originally written, it only applied to thefts of trade secrets which are committed to benefit a "foreign government, foreign instrumentality or foreign

agent." Concerns that such a law might violate a number of international trade treaties to which the United States is a signatory caused the bill to be rewritten at the last minute to include both foreign and domestic theft of trade secrets. On September 17, 1996, the House passed the bill, now known as the EEA.³⁷ On September 18, with certain amendments it passed the Senate. On September 28, 1996, the House amended the Senate version and passed it. On October 2, 1996, the Senate concurred in the House amendments. It went to President Clinton on October 4, 1996, who signed it on October 11, 1996.

III. ANALYSIS OF THE ACT

The structure of the EEA reflects its rather disparate origins, and the confusion that surrounded major changes made in the last days of the 1996 Congressional session. The EEA contains a definition of trade secrets³⁸ that is taken with only minor modifications from the definition in the Uniform Trade Secrets Act³⁹ adopted by 40 states and the District of Columbia.⁴⁰ At the same time, the sections defining misappropriation⁴¹ are entirely new, and have no parallels in existing trade secrets law. Finally, the remedial provisions are unique in their mix of civil and criminal penalties, and in their differential treatment of "domestic" and "foreign" misappropriation. In this section, we focus on a number of new rules and potential problems in the EEA.

A. Defining Trade Secrecy

The sine qua non of an action under the EEA is the existence of a "trade secret." Section 1839(3) defines that term as follows:

(3) 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 readily ascertainable through proper means by the public⁴²

This definition, which was added late in the Congressional session,⁴³ generally tracks the definition of trade secrets in the Uniform Act.⁴⁴ However, there are some important differences between the language of the two statutes.

First, the list of potential types of secrets is much more expansive in the EEA than in the Uniform Act, though it has been narrowed some from earlier versions of the statute.⁴⁵ It is not clear why Congress chose to expand upon the representative list in the Uniform Act. Because of the expansive interpretation already given to the Uniform Act definition,⁴⁶ it is likely that the EEA will apply to all the same types of information which qualify as trade secrets under the current civil standard. This in itself may be surprising to some; state criminal trade secrets statutes are frequently more limited in scope than their civil counterparts. For example, the California criminal trade secrets statute⁴⁷ until recently applied only to the theft of scientific or technical information.⁴⁸ By contrast, the language of section 1839 makes it clear that the theft of business or financial information (including perhaps some types of insider trading)⁴⁹ falls within the ambit of the new statute.

Second, the EEA expressly extends the definition of trade secrets to encompass information in any form, "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."⁵⁰ The references to intangible information and the "whether or how" language strongly suggest that not only information stored in electronic form, but also information "stored" only in an individual's memory, can be the subject of a prosecution for trade secrets theft. Thus, memorizing a trade secret is a means of misappropriating it under the EEA. This result is not too surprising -- courts have periodically found defendants liable under civil statutes even though the information they took was only in their heads.⁵¹ Further, we believe this language must be read in light of the repeated statements in the legislative history indicating that former employees will not be punished

under the EEA merely for taking with them the general skill, knowledge, and industry experience they have acquired on the job.⁵²

Third, the definition of reasonable precautions generally tracks that of the Uniform Act, with one possible exception. The EEA places the burden of taking such precautions on the "owner" of the secret.⁵³ Owner in turn is defined in section 1839(4) as "the person or entity in whom or in which rightful legal or equitable title to or license in the trade secret is reposed."⁵⁴ The import of the words "or license in" is not entirely clear. In context, the definition appears to assume a single rightful owner of the trade secret, and to contemplate that that "owner" might be an exclusive licensee. However, this provision is also subject to the construction that any licensee entitled to use the trade secret is an "owner" of that secret obligated under the statute to take reasonable precautions, and therefore that the failure of *any* licensee to take such precautions threatens the trade secret status of the information.⁵⁵ The effect of this wording may serve to make trade secret status of information more fragile by taking control over secrecy out of the hands of the trade secret owner to some extent.

While it is certainly true that public disclosure of a trade secret will terminate protection for it,⁵⁶ the "reasonable precautions" test seems aimed at different goals -- assuring that the trade secret owner does in fact consider the information to be valuable and secret, and putting potential defendants on notice that the information is in fact considered a secret. We think, therefore, that the test of reasonable precautions should continue to focus primarily on the actions of the trade secret licensor, and on the economic circumstances surrounding the industry.⁵⁷ Similarly, accidental disclosure under unpreventable or unforeseeable circumstances should not automatically destroy trade secrecy, even if the beneficiary of this disclosure is not criminally liable for her use or disclosure of the information.

Finally, the EEA changes the provision in the definition of a secret regarding the relevant public whose knowledge is tested. Under the Uniform Act, information is a secret if it is "not generally known to, and not readily ascertainable through proper means by other persons who can obtain economic value from its disclosure or use."⁵⁸ Generally this means that the question is whether one's competitors know or could easily discover the secret. By contrast, the EEA without explanation changes the relevant person from the competitor to "the public."⁵⁹ The import of this change in language is not entirely clear. One might read it

as a dramatic lowering of the threshold of secrecy, particularly in high-technology industries. After all, the principles of thermodynamics may be well-known in the circles where they are of use, but they are hardly "generally known" to the public at large. We think it unlikely that such a dramatic change was intended by Congress, however. Thus, we expect that the relevant test will continue to be whether those who have an economic interest in discovering the secret can easily do so.⁶⁰

One issue on which the statute is silent, but which is addressed in the legislative history, is the specificity with which trade secrets must be identified. Under civil trade secrets law in many states, plaintiffs (theoretically) may file a complaint and even proceed to trial without ever having specifically identified the trade secrets they claim have been stolen.⁶¹ Even in states such as California, which provide by statute that the plaintiff must identify its trade secrets early in the litigation process,⁶² parties regularly change the description of their trade secrets during litigation, and even during trial.⁶³ The Senate Report suggests that particularity in describing trade secrets will be important under the EEA, as it should be: "a prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated."⁶⁴

B. Defining Misappropriation

In contrast to the definition of a trade secret, where Congress with a few exceptions stayed on the well-defined path of the Uniform Act, the EEA creates an entirely new definition of what constitutes misappropriation. In fact, it establishes two sections, which define misappropriation in nearly identical terms, but which vary the penalties for trade secret theft depending on who the defendant is and the purpose for which they acted. In this section, we examine first the conduct covered by the EEA, and then the actors who are liable.

1. Prohibited Conduct

Sections 1831(a) and 1832(a) contain identical language regarding acts of misappropriation, punishing a specified individual who:

(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 the same to have been stolen or appropriated, obtained, or converted without authorization . . .⁶⁵

These provisions are in some respects significantly broader than corresponding civil trade secrets laws such as the Uniform Act.⁶⁶

Section (a)(1) lists a number of means of improper acquisition of a trade secret. In general, the provisions in this section seem to track the "improper means" of acquisition punished in civil cases.⁶⁷ In particular, the references to stealing, concealment, fraud, artifice and deception are reminiscent of the civil law's prohibition against both illegal and "immoral" business conduct.⁶⁸ However, the provision also makes it a crime to "appropriate" or "take" a secret without authorization from the trade secret owner. These terms might be thought to encompass the sort of lawful business espionage that has long been permitted by civil trade secrets law -- conduct on the order of observing a competitor's property from across the street. There is some suggestion in the legislative history that the EEA is not intended to inhibit robust competition.⁶⁹ While this might be enough to declare broad categories of competitive intelligence-gathering proper and therefore lawful, the ambiguity of some of the terms in section (a)(1) is troubling. However, from a practical standpoint it is extremely unlikely that a United States Attorney will prosecute a defendant for activities that are permitted under civil trade secrets law.

Broader still is section (2), which gives the trade secret owner the right to control a whole host of activities on the order of duplication, transportation, or destruction of a trade secret. This provision

encompasses more than its civil counterparts. Section (2) is not by its terms limited to secrets acquired by "improper means" like those listed in section (1). Even legally acquired secrets can be misappropriated under the EEA if they are analyzed or duplicated in one of the ways listed in section (2). The civil law does prohibit some such uses of a lawfully acquired trade secret, but limits its reach to disclosure or use of a secret in violation of a confidential relationship.⁷⁰ By contrast, there is no requirement of such a confidential relationship in the EEA. So long as the requirements of secrecy are satisfied, the trade secret owner is apparently entitled to seek the aid of the Justice Department in preventing the world from engaging in any of the enumerated acts in section (2), even if the secret is contained in a product that the defendant lawfully acquired.⁷¹ As a result, the EEA effectively implies a confidential relationship between the trade secret owner and the world at large, something trade secret law has never before attempted and an indication that Congress believes trade secrets law is based in property theory, not tort or contract.⁷² Further, some of the specific provisions in section (2), such as the prohibition against "altering" or "destroying" a trade secret, are outside the normal reach of trade secret law.⁷³ While these prohibitions might seem to apply to physical vandals and computer hackers as well as more traditional types of trade secret defendants, the requirement of section 1832 that the defendant act "with intent to convert a trade secret" arguably incorporates the criminal law relating to conversion. This would preclude prosecution of those who act for noneconomic motives, such as the defendant in *United States v. LaMacchia*.⁷⁴ For this reason, the EEA will be of limited use in many cases involving computer hackers.⁷⁵

The most troubling thing about section (2) is that it arguably prohibits many forms of heretofore lawful reverse engineering activity. While reverse engineering is not expressly prohibited under this section, neither is it expressly permitted. Rather, its legality appears to be judged according to whether the reverse engineer engages in any of the prohibited acts.⁷⁶ To be sure, some types of reverse engineering, such as looking at or tasting a lawfully acquired product in order to determine what is in it, will not be illegal under the EEA.⁷⁷ On the other hand, several of the restrictions in section (2) will if read literally encompass some forms of reverse engineering. For example, reverse engineering of computer software by "decompilation" almost always involves the making of a prohibited "copy" of the program.⁷⁸ Reverse engineering of mechanical devices and computer hardware may well involve prohibited "sketching,

drawing, or photographing" of the trade secret contained in the publicly sold device. And it is even possible that the prohibition against "altering" a trade secret will be interpreted to prevent chemical analysis of a trade secret product if such analysis involves the use of chemical reactants which bond to secret chemicals or which precipitate out certain elements from the formula.

The legislative history of the EEA is not encouraging to reverse engineers. The Senate Report suggests that "the important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has 'reverse engineered.' If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent *or this law*, then that form of 'reverse engineering' should be fine."⁷⁹ The Report goes on to suggest that observing a lawfully purchased product, or drinking a Coca-Cola, are legitimate activities.⁸⁰ On the other hand, there appears to be no reverse engineering defense protecting any of the forms of analysis suggested above. A computer programmer has the right to decompile a software program in certain circumstances under the Uniform Act, copyright law, and the common law without fear of civil liability.⁸¹ Under the EEA, though, that programmer has apparently committed a felony.

The inadequate explicit protection accorded reverse engineering in the EEA is particularly unfortunate given the vital importance reverse engineering has to many legitimate business activities. Courts and commentators alike have extolled the virtues of reverse engineering in a competitive economy.⁸² The Supreme Court sees reverse engineering as the economic centerpiece of state trade secret law, and indeed the primary thing that allows trade secrets to coexist peacefully with federal patent and copyright protection.⁸³ While there is no issue of federal preemption of the EEA, which is after all a federal statute, it is surprising that Congress has apparently permitted a major change in the balance traditionally struck in intellectual property law between owners and competitors, and done so for the first time with little or no fanfare in a criminal statute.⁸⁴ Given the stated intent of Congress not to endanger legitimate business competition⁸⁵ and to reach only "flagrant and egregious cases of information theft,"⁸⁶ it is our hope that these provisions will not be used by the Government as a weapon to strike at otherwise lawful acts of reverse engineering,⁸⁷ or that the law will be amended to expressly protect reverse engineering.

Finally, it is worth noting that sections (3)-(5) respectively punish the knowing receipt of misappropriated trade secrets, attempts to misappropriate trade secrets, and conspiring to appropriate trade secrets. Section (3) also punishes the knowing possession of a trade secret. In effect, this is likely to be comparable to section 1(2)(ii)(C) of the Uniform Act, which punishes the use or disclosure of information known to be acquired by accident or mistake. Because sections (3)-(5) are lumped together with the act of misappropriation, the penalties for such possession, attempt, or conspiracy are as severe as the penalties for successful misappropriation.

2. Affected Parties

Sections 1831 and 1832 differ in the parties to which they apply. Section 1831 punishes all of the acts listed above when knowingly undertaken by anyone "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."⁸⁸ This was originally the heart of the EEA, which was designed to cope with the problem of foreign business espionage.⁸⁹ The definitions of foreign "instrumentality" and "agent" are relatively narrow. Foreign companies or individuals do not fall within the ambit of section 1831 unless they are "substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government."⁹⁰ The Senate Report indicates that the intent of section 1831 is to target foreign government action, not any act of espionage undertaken by a foreign corporation.⁹¹ This distinguishes the EEA from section 337 proceedings in the International Trade Commission, which focus merely on the nationality of defendant companies.⁹²

However, the language of section 1831(a) makes liable not just foreign government and their agents, but anyone who misappropriates a trade secret "intending or knowing that the offense will benefit any foreign government."⁹³ The fact that only knowledge and not intent to benefit is required suggests that US citizens who act for purposes other than economic espionage may still fall within the scope of section 1831. For example, the computer hacker who posts the trade secrets of a defense contractor on the Internet arguably knows that the effect of his actions will be to benefit a foreign government, even if he posted the information for a completely different purpose. That hacker may be subject to the enhanced penalties of

section 1831, rather than the "normal" trade secret provisions of section 1832. On the other hand, because the statute requires that the actor know that a foreign government will benefit from the information, both those who act without knowing the consequences and those who intend to benefit foreign *corporations* rather than governments will not be liable under section 1831.

Section 1832 is a general criminal trade secrets statute. Despite its inclusion in the Economic Espionage Act, there is no requirement of foreign espionage in this provision. Rather, it applies to anyone who knowingly engages in any act of misappropriation "with intent 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."⁹⁴ There is no requirement of any foreign connection, and the legislative history confirms that section 1832 is intended to be a law of general applicability.⁹⁵

Nonetheless, there are several limitations in scope evident in section 1832. First, section 1832 requires three different elements of intent. The defendant must "knowingly" commit one of the listed acts of misappropriation described above.⁹⁶ In addition, she must act "with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof,"⁹⁷ a requirement which appears to preclude prosecution both of those who act out of spite and those who act for some other noncommercial purpose, such as a belief that "information wants to be free." Finally, section 1832 requires that she act "intending or knowing that the offense will injure any owner of that trade secret."⁹⁸ The second and third provisions differ from the prevailing rule in civil cases. Under the Restatement and the Uniform Act, there is no requirement that a civil defendant be aware of the trade secrecy of the information, provided the information was secret and the defendant *should have known* of the claim to secrecy.⁹⁹ Further, there is no requirement in civil trade secrets law that the defendant intend or know of the potential economic loss to the plaintiff.¹⁰⁰ On the other hand, state criminal trade secrets statutes generally do require knowing misappropriation.¹⁰¹ The requirement of knowledge or intent serves to limit the applicability of the EEA in some "doubtful cases," where the defendant acted without knowledge that what he was doing was wrong.¹⁰²

The reach of section 1832 is also limited by the requirement that the secret be "related to or included in a product that is produced for or placed in interstate or foreign commerce."¹⁰³ This phrase

seems to impose two separate requirements on the trade secret owner, neither of which is commensurate with civil trade secrets law. First, the limitation to products sold in commerce seems to exclude the possibility of an EEA prosecution based on the misappropriation of trade secrets related to *services*. No reason for this limitation is offered, and it seems at odds with the spirit of the expansive definition of trade secrets offered in section 1839. Second, the statute seems to require that the trade secret owner have actually produced or sold in commerce a product containing or using the secret. This means that the EEA arguably does not cover either "negative know-how"¹⁰⁴ or information discovered but not used by a company, both of which qualify as trade secrets under the Uniform Act (though not the Restatement of Torts).¹⁰⁵ One effect of this limitation may be to restore the unfortunate rule of *SI Handling v. Heisley*,¹⁰⁶ under which employees who had an obligation to assign an invention could instead take it without trade secrets liability provided they had not in fact told their employer about it.¹⁰⁷ This limitation too is not explained in the legislative history, and does not appear to have been intended by Congress.

There may be ways around some of these limitations on the scope of section 1832. For example, the government might contend that a trade secret was "related to" a commercial product if it was in the same field of technology, even though it had not yet been incorporated in a product. Alternatively, it might argue that the *defendant's* incorporation of a secret into a commercial product triggered liability under the EEA. Both of these are possible readings of the statute which would avoid the unnecessarily limiting interpretation discussed above.¹⁰⁸

C. Penalties

Violations under both sections of the EEA are treated as serious crimes. Section 1832 provides for a term of up to 10 years in prison and unspecified fines for individuals violating the EEA,¹⁰⁹ and fines of up to \$5 million for corporations or other organizations that violate its provisions.¹¹⁰ The amount of the fine imposed on individuals is not specified, which means that the general maximum fine for felonies of \$250,000 should apply.¹¹¹ The legislative history suggests that the fine in cases of significant injury should be set at twice the value of the loss to the trade secret owner or the gain to the infringer pursuant to the

general federal fines provision, 18 U.S.C. § 3571(d).¹¹² The legislative history also suggests that organizations could be fined more than \$5 million in cases where the loss to the trade secret owner was particularly high, relying on section 3571(d) rather than section 1832(b).¹¹³ Section 1831 provides for an enhanced penalty in cases of foreign espionage -- the maximum prison term is raised to 15 years,¹¹⁴ and the maximum organizational fine is set at \$10 million.¹¹⁵ The maximum fine for individuals is set at \$500,000,¹¹⁶ rather than the normal felony maximum of \$250,000. The general approach of the statute is evidently to punish foreign espionage more severely than domestic trade secret theft.

Section 1834 additionally provides for forfeiture of a defendant's property during sentencing. Forfeiture of "any property constituting or derived from, any proceeds the person obtained, directly or indirectly,"¹¹⁷ from the theft is apparently mandatory -- the EEA provides that a court "shall order" forfeiture in addition to any other sentence imposed.¹¹⁸ By contrast, while the EEA also provides for forfeiture of "any of the person's or organization's property used . . . to commit or facilitate the commission" of the offense,¹¹⁹ forfeiture of such instruments is discretionary rather than mandatory.¹²⁰ The proceeds and instruments in question are forfeited to the United States, rather than to the victim of the crime.¹²¹ However, the Senate Report suggests that victims may be able to seek restitution from the United States out of the forfeited proceeds.¹²²

Section 1834(b) of the EEA provides that, with certain minor exceptions, the forfeiture of proceeds and instruments shall be governed under the laws relating to drug forfeitures.¹²³ Those laws vest title to the seized property in the United States, and provide that the Attorney General shall dispose of those assets "by sale or any other commercially feasible means."¹²⁴ Where the assets seized include the misappropriated trade secret itself -- say, embodied in a product -- the victim of the trade secret theft has a potential problem. Under section 1834, the government now has title to the product embodying the victim's trade secret, and indeed has a mandate to auction that product to the highest bidder. This is hardly consistent with the victim's interest in keeping the secret. The victim's best recourse in such a case appears to be to proceed under section 853(n) of the drug forfeiture statute, which specifies a procedure for the victim to petition the court for return of forfeited property which the victim claims belongs to it.¹²⁵ Alternatively, the victim could seek to have the infringing goods destroyed, as is done with drugs

themselves. One of these two options seems most probable. It is unlikely that the government, having acted to preserve a trade secret, would then risk destroying it by public sale of goods or documents embodying that secret.

A different sort of problem is presented by the seizure of a defendant's products which do not themselves incorporate a stolen trade secret, but which are indirectly derived from misappropriated knowledge. This is particularly likely in the case of certain classes of information, such as "negative know-how," for which direct incorporation in a defendant's product is unlikely. The broad language of the forfeiture statute requires the government to seize "any property constituting *or derived from*, any proceeds the person obtained, *directly or indirectly*, as the result of such violation."¹²⁶ This strongly suggests that such derivative products are subject to seizure and sale, despite the intervening contribution of defendant's own employees.

Finally, section 1836 provides that the Attorney General may file a civil action to obtain "appropriate injunctive relief" in federal district court against any violation of the EEA. Because this is a civil action, it might be stayed if there is also a pending criminal proceeding, as often happens in state civil trade secrets actions.¹²⁷ However, the government can use its injunctive power at the outset of a prosecution to maintain the status quo or prevent an imminent public disclosure of a victim's secret. On the whole, though, the deterrent effect of a pending criminal action is such that preliminary injunctive relief should rarely be necessary: no reasonable lawyer would advise her client to continue to engage in conduct which is the subject of an indictment. In some circumstances, such as those where the defendant's conduct does not rise to the level of a criminal violation, civil injunctive relief may prove to be an appropriate *substitute* for criminal punishment. In other cases, particularly those with foreign defendants, federal civil injunctive relief may be able to reach further than existing state trade secrets laws which already provide for injunctive relief.¹²⁸ For the majority of cases, however, section 1836 adds little besides federal court jurisdiction to what can already be accomplished using state law.

D. Territorial Scope of the EEA

Section 1837 governs the applicability of the EEA to conduct which occurs in whole or in part outside the United States. The territorial reach of the statute is extremely broad. It applies not only to acts conducted entirely within the United States, but also to a foreign scheme provided any "act in furtherance of the offense was committed in the United States."¹²⁹ This is consistent with the goal of reaching foreign espionage, much of which will of necessity occur outside the United States. It also hypothetically sweeps within its scope acts which are primarily foreign in nature. For example, if the government of Algeria acquires the secrets of a Tunisian company through espionage, the misappropriation is in violation of the EEA, and may be prosecuted in the United States, provided a single act in furtherance of the scheme occurred in the United States. Further, under section 1837(1) the EEA reaches even wholly foreign acts of misappropriation, provided the defendant is either a United States corporation or a citizen or permanent resident alien of the United States.¹³⁰ This means that if a United States citizen residing abroad steals a Russian trade secret on behalf of the Chinese government, that act is in violation of the EEA even though there is no other connection between the misappropriation and the United States.

The broad grant of extraterritorial jurisdictional power is probably necessary to ensure that acts of foreign espionage in which the United States has a legitimate interest are within the reach of the statute. However, we would expect that the Justice Department will require some showing of a national interest in or connection with the dispute before bringing an action under the EEA, both to conserve its resources and to avoid the danger of intervening in what is essentially an internal dispute in a foreign country.

E. Conclusions

There are a number of ambiguities in the EEA that will have to be resolved if the Act is to send a clear signal of the sort Congress apparently intended. There are also several problematic provisions of the EEA. Some of these provisions (such as not explicitly protecting reverse engineering) potentially expand the reach of trade secrets laws in unprecedented ways; others place inexplicable limitations on the power of the Justice Department to enforce the law. The harm caused by the overbroad provisions can be

ameliorated to some extent by the exercise of discretion not to prosecute in the Justice Department; we discuss such prosecutorial issues below. The loopholes in the statute cannot be removed so easily. However, the fact that state civil and criminal sanctions continue in force¹³¹ may help to solve what problems do exist.

IV. STRATEGIES

Unlike other forms of intellectual property, trade secrets require a great deal of self-help effort on the part of the owner as a predicate for court protection; and the boundary of this property is rarely defined in advance of a dispute. Coupled with the fact that trade secrets are difficult to define in any event, it is easy to see why laws regulating this interest can create their own uncertainty. In such an environment, it is extremely important that all parties involved -- government prosecutors, those who own secret information, and those who handle information belonging to others -- think through the issues strategically. In this section, we will examine, from a practical perspective, the issues facing government prosecutors, potential victims and potential defendants in the context of the EEA. Many of these issues do not greatly differ from those that arise in the civil litigation context; thus, some of the advice that follows comes from civil rather than criminal cases.

A. The Prosecutor's Perspective

United States Attorney's offices are very busy and handle a wide variety of cases, often involving defendants who are accused of committing heinous crimes.¹³² Additionally, scarce resources have forced many United States Attorney's offices to set monetary thresholds in white collar crime cases, including those involving intellectual property. Such guidelines may be keyed to the amount of defendants' financial gain or the amount of the victim's financial loss. Further, the much higher standard of proof in a criminal case, may mean that while a victim might have a very strong civil case, the matter is unsuitable for criminal prosecution and will be declined by a United States Attorney. In this section, we consider some of the

important differences between civil and criminal litigation, and how those differences will affect a United States Attorney's decision whether to prosecute a violation of the EEA.

1. Important Differences between Civil Litigation and Criminal Prosecution

a. Burden of Proof

In determining whether to refer the matter to the United States Attorney for criminal investigation and prosecution, civil litigants often fail adequately to consider the difference in the burden of proof between civil and criminal litigation. In a criminal case the government must prove "beyond a reasonable doubt" each and every element of each charge. By contrast, the burden of proof in a civil case is "by a preponderance of the evidence," which means that the jury or the judge must decide which of the party's version of the facts is more likely to be correct. Many victims and their lawyers, used to litigating in civil court, do not fully appreciate how difficult it is to convince the jury that the defendant is guilty beyond a reasonable doubt. This burden can even become more difficult in a trade secret case which involves complex technology not easily understood by the jury, or which implicates philosophical concerns about an individual's right to move to a new job.

b. Discovery and the Protection of Trade Secrets

Discovery in a criminal case is different than in a civil case. Because of the public nature of criminal trials, additional details about the trade secret kept from the public in civil litigation might be disclosed in a criminal case. But there are effective means of managing and limiting this risk. There are two types of disclosure at issue in an EEA case -- disclosure to the defendant and his lawyers, and disclosure to the general public. Referral of a matter involving the theft of a trade secret to federal law enforcement does not mean that the details of the trade secret will be disclosed to the public. Because of constitutional and statutory protections, and the nature of the federal criminal justice system, during the time that the matter is being investigated by a federal agency such as the FBI, and is being presented to a grand jury by a United States Attorney's office, the trade secret will not be disclosed to anyone. Additionally, because it can take a long time to investigate and return an indictment in a complex

matter such as the theft of trade secrets, and because of the short "shelf-life" of many trade secrets, it may no longer be important to the victim to keep the information secret.

The Constitution requires that federal felonies be charged by grand jury indictment.¹³³ The principal function of a federal grand jury, therefore, is to decide whether to approve or "return," an indictment proposed by a federal prosecutor charging federal felony violations, such as a violation of the Economic Espionage Act of 1996. To make that decision, the grand jury must determine whether there is probable cause to believe that a crime has been committed and that the individual charged in the indictment, the proposed defendant, or "target," committed it. Rule 6(f) of the Federal Rules of Criminal Procedure provides that the "indictment may be found only upon the concurrence of 12 or more jurors."

In making its decision whether to approve indictments, the grand jury may also perform an investigative function, for which its powers are broad.¹³⁴ It can compel the testimony of witnesses and the production of documentary and other physical evidence, subject to very few limitations.¹³⁵ This investigative role is essential. Although a prosecutor, working together with an investigative agency, generally directs the investigation, the prosecutor and investigative agency alone cannot compel the testimony of witnesses and the production of documentary and other physical evidence. They must work with the grand jury to secure evidence that would not otherwise be available.

For a variety of reasons, during the phase in which, the grand jury is assisting the investigators and prosecutors with the investigation, Rule 6(e) of the Federal Rules of Criminal Procedure makes it unlawful for anyone other than a grand jury witness to disclose "matters occurring before the grand jury."¹³⁶ While there are several exceptions to this rule,¹³⁷ from a practical standpoint, during the investigative stage, no details of the trade secret will be disclosed to the public. Once the grand jury has returned the indictment the victim should understand that the protections afforded by Rule 6(e) are lifted and some additional information may be disclosed because of broad federal criminal discovery rules.

Rule 16 of the Federal Rules of Criminal Procedure requires federal prosecutors to provide to the defense: (1) all recorded and written statements made by the defendant before or after his arrest; (2) the substance of any oral statements made by the defendant to any person then known to the defendant to be a government agent; (3) the defendant's prior arrest record; (4) documents and tangible objects to be

introduced by the government during its case-in-chief, material to the preparation of the defense, or taken from the possession of the defendant; and (5) reports of scientific tests and medical examinations. There is also a continuing duty upon the attorney for the government to exercise due diligence in disclosing additional information within these categories which may become known to him at any time before trial or during trial. Further, the government has a duty to disclose exculpatory evidence material to guilt or innocence or punishment.¹³⁸ Finally, under the "Jencks Act," the government must produce statements of all trial witnesses.¹³⁹ Taken together, these obligations mean that the government may be required to disclose certain details about the trade secret to the defense. For example, the government may have to disclose related technical information, if it could be used by the defense to argue that the trade secret was generally known in the industry. However, these disclosures would probably also be required in a civil case.

In drafting the Economic Espionage Act of 1996, Congress was concerned about additional disclosures of the trade secret to the public during a criminal prosecution. The Act provides that the court "shall enter such orders and take such action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws."¹⁴⁰ Accordingly, the victim should continue to work with federal prosecutors after the indictment has been returned to seek entry of orders that will preserve the status of the information as a trade secret and avoid unnecessary disclosure of the information.¹⁴¹ Further, where appropriate, federal prosecutors should be encouraged to seek pretrial orders requiring that: (1) the dissemination of the trade secret be limited to defense counsel and their employees; (2) defendants be required to view the secret only in the presence of counsel, or at counsel's office; (3) anyone not otherwise allowed to view the secret be required to obtain a court order before doing so; and (4) defense experts be required to provide to the court their name, employment history, and other relevant information.¹⁴²

Additionally, courts can limit the disclosure of information to the public even during the trial without necessarily violating the defendant's right to a public trial under the Sixth Amendment. While the right to a public criminal trial was incorporated into the Constitution by the Sixth Amendment, the right is

not absolute and may be limited in appropriate circumstances.¹⁴³ At least one circuit court has recognized the power to restrict access to that portion of the proceeding which would reveal trade secrets. In *Stamcarbon N.V. v. American Cyanamid Co.*,¹⁴⁴ on appeal of a criminal contempt conviction, the court held that based on a compelling claim, a district court may limit access if the court determines that (1) a party is likely to suffer irreparable injury if access to the proceedings were not limited, and (2) protection of the party's secrets can be achieved "with minimal disruption of the criminal proceedings."¹⁴⁵

Victims should make sure that prosecutors seek to prohibit the public disclosure of the trade secret during the trial, by, for example, requesting that the court deny public access during the testimony of an expert witness who is describing the details of the trade secret. Of course, a court order limiting public access to an expert witness testimony should include a similar limit on access to the transcripts.

2. Factors That Enter Into the Decision Whether to Prosecute

As noted above, limited resources have forced many United States Attorney's offices to set guidelines on what type of cases will be investigated and prosecuted. Such guidelines also may reflect the prosecutive philosophy of the current United States Attorney in that particular district. However, this does not mean that United States Attorney's offices are completely rigid in their application of such prosecutive guidelines. Failure to meet certain guidelines criteria does not necessarily mean that the United States Attorney's office will automatically decline the case; especially if there are other compelling reasons which warrant investigation and prosecution. This is particularly important in trade secret cases because strict adherence to such guidelines may underestimate the importance and seriousness of the criminal referral.

Further, unlike almost all other types of criminal matters, in which a United States Attorney's office almost always makes the final determination on whether to investigate and prosecute a case, before a United States Attorney's Office can seek to return an indictment alleging a violation of section 1833, the United States Attorney's Office first must obtain the approval of the Attorney General, Deputy Attorney General or Assistant Attorney General for the Criminal Division.¹⁴⁶ It is not clear how this approval authority will be exercised or what type of regulations will be issued, but it is expected that local

prosecutive guidelines will play an important role in determining which matters are investigated and prosecuted.

While the guidelines may vary from office to office, there are a number of general factors which, in most instances, are of universal concern in a trade secret case: (a) whether the information clearly was a trade secret; (b) whether the information was technical or scientific in nature; (c) evidence of criminal conduct and intent; (d) evidence of significant monetary value of the information; (e) availability of other remedies; and (f) whether the misappropriation was promptly reported. An analysis and understanding of these factors should be helpful to a victim when considering whether to refer a matter to a United States Attorney's Office and to maximize the chances for a successful referral.

a. Trade Secret

The issue of whether the information was secret before it was obtained by the defendant is a question of fact. Victims should understand that in this regard, the government has the very difficult burden of proving a negative, i.e., that the information was not generally available to the public. Federal prosecutors will need access to objective, independently verifiable evidence that the information was truly secret and why it was not readily apparent to, or discoverable by, other professionals or experts in that particular field. Further, the victim must be able to show that the trade secret had not been disclosed by a sub-contractor or licensee, or published in technical journals or other publications. Because of the nature of trade secrets, the victim will be the best initial source of this information. The victim therefore has the responsibility to provide all relevant data to the prosecutor, regardless of how inconsequential or damaging it may be. The odds of a successful prosecution are greatly increased if a victim makes full disclosure of all potential problems with the case.

In order for information to qualify as a trade secret, the owner must have taken reasonable measures to keep it confidential. Therefore, the victim should also furnish evidence to the United States Attorney on the steps taken to protect the information. Specifically, the victim must be able to establish to the prosecutor's satisfaction that the physical security, computer security and personnel policies regarding confidential information were reasonable under the circumstances to protect the information.¹⁴⁷ If it

becomes apparent, for example, that any employee in a large company could gain access to the information, the case will probably be declined.

Finally, the Act requires that the trade secret derive "independent economic value . . . from not being generally known to . . . the public." 18 U.S.C. § 1839(3)(B). The government does not need to prove a specific jurisdictional amount lost. However, in order to satisfy the informal monetary threshold set by many United States Attorney's offices, the victim must be able to show with some degree of certainty that the trade secret either was developed at a high cost, or could be used to save a competitor a significant investment in research and development.

b. Type of information

The EEA protects all information, regardless of type, which meets that statutory definition of a "trade secret." The most obvious sort of valuable secret is represented by research, formulas and other scientific information. It is less likely that a United States Attorney will agree to investigate and prosecute the theft of business information such as sales forecasts, market studies, risk analysis, training materials, employee records, customer lists, and budgets. In most cases, this sort of data is not obviously valuable enough to reach the threshold amount required by many United States Attorneys. In addition, it is very difficult for the government to prove beyond a reasonable doubt that, for example, a customer list was not known to a competitor of the victim or was not legally obtainable. Further, most business information depreciates in value quickly. Finally, business information is inherently more difficult to qualify through independent experts, and its rather more speculative value makes convictions less certain. Except in unusual circumstances, such as the theft of a sealed contract bid, the misappropriation of business information is better suited for adjudication in the civil forum.

c. Evidence of theft and consciousness of guilt

In general, the EEA makes it a crime to obtain a trade secret by almost any means including copying. The EEA covers those situations where the lawful owner retains the original copy of the trade secret and is not deprived of its use. However, in order to overcome the potential problems of prosecuting the defendant's "mental recollections" or the defense that "great minds think alike," it is essential to establish tangible evidence of theft.

Additionally, tangible evidence of theft might also be necessary to overcome a reverse engineering defense. The Act does not expressly prohibit or permit reverse engineering. Rather, its legality, as described above, appears to be judged according to whether the reverse engineer engages in any of the prohibited acts. In most instances, this can only be proven through tangible evidence of the misappropriation. Without such evidence the defendant might be able to successfully claim that the information was lawfully obtained from the victim and the details of the trade secret discovered through reverse engineering. Alternatively, the defendant might plausibly claim to have independently developed the information.

Tangible evidence of misappropriation may include copies of proprietary documents in the possession of a competitor, e-mail messages describing proprietary information, or any other physical matter linking the defendant to the misappropriation. In exceptional cases the government might be able to establish misappropriation by showing that the defendant had access to the victim's trade secret and was attempting to sell a product that appeared to be directly based on the trade secret. However, without tangible evidence of theft it is unlikely that the federal government will prosecute the case.

This does not mean that victim should hesitate to report suspected trade secret thefts to the authorities. In many instances only law enforcement has the resources and legal authority to uncover the needed evidence. For example, the use of search warrants can lead to the discovery of tangible evidence of the theft, especially if the search warrant is executed shortly after the misappropriation. In order to obtain a warrant from a federal magistrate the government must establish probable cause, which the Supreme Court has defined as "a fair probability that contraband or evidence of a crime will be found in a particular place."¹⁴⁸ Thus, to assist the United States Attorney's Office in obtaining a search warrant, the victim must be able to describe very specifically what information was stolen and the tangible objects that probably contain the information. The victim will also have to establish why the information would probably be found at a particular location.

In cases in which the victim believes that the trade secret was obtained by a computer intrusion or was transferred over a computer network, the victim should carefully maintain all computer audit logs¹⁴⁹ which can document a defendant's criminal activities. However, before engaging in monitoring of a

suspect's computer transmissions, victims are urged to discuss the matter with counsel to avoid violating any of the provisions of the Electronic Communications Privacy Act.¹⁵⁰

Besides establishing the act of misappropriation, the evidence ideally will also reflect the defendant's consciousness of guilt. Furtive behavior, lying, attempted bribery and similar conduct will help demonstrate to a jury that the defendant knew his behavior was wrong. This element of intent is essential as both a technical and a practical matter.

d. Value of the information

As described above, the EEA does not require that the government prove that the trade secret have a certain monetary value in order for ~~its~~ criminal sanctions to apply. However, many, if not most, United States Attorney's offices have established monetary guidelines that must be met in white collar cases before prosecution will be considered. In other words, the monetary loss to the victim must be great enough to merit criminal investigation and prosecution. The minimum varies from one office to another, but in some large districts, the loss to the victim must exceed \$100,000.¹⁵¹ Because there is often no legitimate market for trade secrets, establishing *any* monetary loss is difficult; meeting the monetary guidelines of some United States Attorney's Offices is especially so. However, the difficulty in establishing a monetary value should not deter the victim from analyzing and presenting the case to the United States Attorney.

In some circumstances, the value of the trade secret can be established by showing what price the trade secret would have fetched on the open market. Civil cases will probably be used as reference points to help in the initial analysis of value. But the issue has come up in a criminal context. For example, in *United States v. Bottone*,¹⁵² the court held that the value of stolen chemical formulae could be based on what European drug manufacturers were will willing to pay. Similarly, in *United States v. Greenwald*,¹⁵³ the Sixth Circuit that the value of the misappropriated trade secret could be established from the "viable, albeit limited" market among chemical companies for the type of formulae misappropriated and from licensing agreements or sales for the chemical formulae that were misappropriate.¹⁵⁴ Thus, in cases where the victim has sold or licensed the protected information embodied in the trade secret, it should supply this information to the U.S. Attorney for use during the evaluation process.

In those instances where the victim cannot establish the value of the trade secret through evidence of its sale or licensing, it should furnish information to the government detailing the costs of development, research or production. In order to maximize the chances of a successful referral, the victim should be as specific as possible in the dollar value of the loss and avoid making generalized unsubstantiated claims that the trade secret was its "crown jewels," or that if the defendant is not prosecuted the victim will go out of business. While such claims might be true, there is a far greater chance that a U.S. Attorney will prosecute the theft if the victim can document the time, effort and money that went into development of the secret.

e. Availability of other remedies

Many United States Attorney's offices are reluctant to pursue matters criminally if the victim has civil remedies available. The government does not want to take sides in a business dispute. Therefore, the victim should be able to explain why civil remedies are inadequate. In this regard, the legislative history of the Act makes clear that in the past, many companies did not bring a civil suit because the defendant was judgment-proof, or the victim did not have the financial resources to investigate the theft and file a civil lawsuit. The presence of these factors is therefore important to note when making a criminal referral. Similarly, absence of a state criminal trade secret law or a jurisdictional problem may make federal prosecution more compelling.

f. Prompt reporting of the theft

Victims should report the theft of a trade secret to federal law enforcement as soon as practical for a variety of reasons. First, if a trade secret theft is not promptly reported the thief might claim that he discovered the trade secret through "reverse engineering" or "parallel development" in the intervening time. Second, as time passes it becomes more and more unlikely that tangible evidence of theft will be discovered.

Nevertheless, in most cases victims should first conduct their own internal investigation because this allows them to make an informed decision about whether the case should be referred to the authorities and if so, how it should be presented. Further, such an investigation can also be of benefit to the U.S. Attorney in evaluating the matter by providing it with evidence necessary to make a decision on whether to

prosecute the theft. However, victims must be careful not to allow the internal investigation to take so long that the trade secret becomes stale or tangible evidence of theft is lost.

Finally, when conducting an internal investigation, victims must be careful to avoid becoming a police agent for purposes of the Fourth Amendment, which might result in the suppression of evidence. The Fourth Amendment of the Constitution generally does not protect against searches of any type by private individuals,¹⁵⁵ unless they are acting as government agents.¹⁵⁶ Whether a private individual is acting as a government agent depends on (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether party performing the search intended to assist law enforcement or further his own ends.¹⁵⁷ Thus, once a victim has reported the theft to law enforcement, the victim should exercise great caution in investigating the theft any further.

B. The Owner/Victims' Perspective

1. Protecting Trade Secrets Before Misappropriation

Taking steps to protect trade secrets from theft makes good business sense for several reasons. First, preventing misappropriation from occurring in the first place is the most cost-effective way of enforcing trade secrets. Certainly, it is much less expensive than litigation. Second, the EEA tracks the Uniform Trade Secrets Act in requiring that, as a condition of protection, the owner of information must have "taken reasonable measures to keep such information secret". This reflects the common law reluctance of judges to help trade secret owners who have not first helped themselves. Finally, as noted above, government prosecutors may share that reluctance, refusing to intervene in cases where the victim's negligence contributed to the loss.

The standard of reasonable efforts is above all flexible. Guiding principles seem to boil down to simple cost-benefit analysis.¹⁵⁸ Within a very wide band of discretion, the trade secret owner is to consider the value of the secret, the nature of the threat to disclosure, and the cost of any particular security mechanism. No system is perfect, and the people who put it to use certainly are not perfect; some mistakes are permitted.¹⁵⁹ In the end the trier of fact will make a judgment about whether the owner's conduct

exhibited something more like excusable neglect than recklessness, measured on a continuum from Fort Knox secrecy to deliberate publication.

Notwithstanding the vagueness of the foregoing, some guidelines have emerged from the civil case law. The trade secret owner must act reasonably, but "heroic" measures are not necessary.¹⁶⁰ The most commonly cited example of this proposition is *E.I. DuPont deNemours & Co. v. Christopher*,¹⁶¹ in which the defendant had learned secrets about DuPont's process technology by aerial photography of a plant under construction. Other cases have noted that avoiding excessive expenditures on physical security is part of the encouragement to investment in research that is provided by trade secret law.¹⁶² It is conduct in trying to protect the secret that matters. Mere subjective intent that something be considered and treated as secret may be relevant, but does not by itself satisfy the "reasonable efforts" standard.¹⁶³

Nondisclosure agreements are one of the more common ways in which confidential information is protected by trade secret owners. Many cases that deal with the sufficiency of secrecy programs mention them, in particular with reference to employees. However, as with other tools and methods of enforcing confidentiality, nondisclosure agreements are subject to no hard and fast rules. In certain cases, having employees sign them was apparently considered sufficient, along with very little else, to support a conclusion of "reasonable efforts".¹⁶⁴ In other cases, the trade secret owner was held to have met the standard of care even though no written agreements were obtained from any employees.¹⁶⁵ As a matter of practice, employee nondisclosure agreements are a useful part of any information protection program, since they enhance protectibility in litigation and they provide notice to the employees that trade secrets are an important asset of the company.

The most effective way to demonstrate "reasonable efforts" is to implement a comprehensive trade secret protection plan. An information protection program may take many forms, but should at a minimum include the following elements:

1. *Nondisclosure agreements.* NDAs constitute a cheap and effective technique for controlling employee misconduct, and should be used at virtually all levels of the enterprise, and with vendors, contractors and customers.

2. A policy for *document protection*, retention and destruction, including provisions for marking confidential documents.¹⁶⁶

3. Visitor (and employee) *access controls*.

4. Procedures for controlling access to *computer networks* and for the registration and control of laptops. Computer security also must include employee training in the area of "social engineering."¹⁶⁷

5. *Background checks* on employees, vendors and contractors. This is one of the most overlooked but effective means of controlling risk of loss.

6. *Education*. Training and awareness are without a doubt the single most cost effective part of any protection program. The keys to successful training are first, that it is on-going, rather than an initial splash that is not followed up; and second, that accountability be established for management of the function.

2. Whether To Make A Criminal Referral

a. Advantages

A trade secret owner who discovers (or strongly suspects) a theft has a threshold choice of remedy. The most obvious advantage to criminal prosecution over a civil lawsuit is cost. The victim can seek to have the government do for it what it would have to pay investigators and lawyers to do. These costs can run to the tens or hundreds of thousands of dollars, and are a serious impediment to seeking remedies through civil proceedings. In addition, criminal cases can be faster to trial, reflecting the requirements of the Speedy Trial Act as well as constitutional imperatives. Perhaps most important, criminal indictment most effectively communicates to the defendant (and to others similarly situated) the seriousness of the owner's commitment to its intellectual property rights. As a result, the "victim" will become known as being intolerant of this sort of behavior, reducing the chance that others will trifle with its rights and generally enhancing the value of its intellectual property portfolio.

b. Disadvantages

Criminal prosecution is not always the obvious choice, however. The most significant negative factor is loss of control over the process, including settlement. The authorities act in the interest of the government and the people it represents, and only indirectly in the interest of the victim. One cannot force a prosecutor to dismiss a case because the defendant has expressed a willingness to stipulate to an injunction or otherwise compromise the claim. A second major disadvantage consists of the impact of the criminal case on any civil proceedings. Because the defendants are entitled to invoke the Fifth Amendment protection against self-incrimination, a civil lawsuit can be effectively stayed as the result of a criminal filing. Therefore, victims who are considering criminal referral of a case should consider a simultaneous filing in the civil courts, with an immediate request for injunctive relief that will provide valuable protection during the time it might take to sort out the procedural conflicts. Alternatively, a victim might work with the prosecuting attorney to seek a protective injunction in the context of a collateral civil proceeding brought by the government.¹⁶⁸ In any event, recovery of damages will likely be delayed and possibly impaired.

3. Federal Versus State Referral

Some states have laws specifically directed at trade secret theft.¹⁶⁹ Moreover, there are jurisdictions that have committed specific resources to prosecuting units with special experience in the field of technology crime. However, states are jurisdictionally limited in the crimes that they can investigate and prosecute. Further it is difficult to match the resources of the FBI and the Department of Justice for the investigation and prosecution of almost any matter.¹⁷⁰ Therefore, although victims of theft should consider prosecution under state laws, especially in jurisdictions where the local prosecutor has experience dealing with this sort of crime, as a general matter the agency of choice will likely be the U.S. Attorney's office. Keep in mind, however, that some cases may not be accepted for prosecution by a U.S. Attorney, while a local district attorney might be willing to take on the case. Also, consider that at least during the first five

years of the EEA, final decisions to prosecute will have to be made at the highest administrative levels within the Department of Justice.¹⁷¹

4. How to Make a Referral

We have examined above the general guidelines that likely will be followed by the government in assessing a case under the EEA. In preparing to present a matter to the prosecutor, that information should be considered, along with the following checklist of practical hints:

- Be realistic. Don't oversell the case. The prosecutor will be judging credibility at the same time as legal requirements. Moreover, a failed case can produce negative consequences, including civil litigation by the accused. In general, prosecutors can be expected to be less concerned about business information than technology and scientific information, so the presentation should reflect this aspect of the stolen information.
- Clearly define what was taken. This may be difficult to do in detail, in part because proof of the theft is usually circumstantial, and trade secrets are difficult to describe both thoroughly and with particularity. However, it is important that the prosecutor be informed to the greatest extent possible, in order to determine that the information can adequately be distinguished from that which is publicly available. Consider offering "inside experts" to explain in layman's terms the fine technical points.
- Establish the monetary value and importance of the information. Show how difficult it would be to discover the secret legitimately; how important the secret is in the context of the victim's business; and how the target's conduct threatens the public interest.
 - Show how the victim has taken reasonable steps to protect the stolen information.
- Present facts which reflect the intent of the accused: i.e., the theft was no mistake; they knew the information was valuable and not theirs to use.
- If there will be a parallel civil case, be clear about what must be done in that context, and about the victim's commitment to the criminal process and its limitations.

C. The Defense Perspective

The presence within a business of data which does not belong is comparable to infection by a virus. Undetected and unchecked, it can become part of a company's process, product or database. Because the law applies to the mere unauthorized possession of information, possibilities for infection are extensive. They start with each employee, especially new hires who often bring with them a personal collection of disks, files and documents, or who just know a lot about the competitor where they used to work. This common situation is usually innocent, since the information stays at home or in the head, or is used only for format rather than content. However, when pressed to complete a project, some otherwise honest people will turn to their personal data cache for short cuts; or will try to improve their position in the company by giving documents to someone else who can use them and who is willing to turn a blind eye to their provenance.

Information also enters through people with less tenure and loyalty. Temporary workers, those "on loan" from another company, and vendor sales personnel are examples. Consultants are a particularly dangerous source, since their value is often measured by their competitive experience; indeed, they can be working simultaneously for a number of competitors. Even the most honest and cautious consultant faces a challenge of separating and protecting large amounts of closely related data.

In today's massively wired network of business relationships, information flows daily among affiliates, partners, customers and suppliers all over the world. Using tools like the Internet, organizations depend for survival on instant access to relevant data. With so many ports opened to the outside, unauthorized information can easily enter the typical business enterprise.

1. Preventive Measures

Avoiding exposure to liability under the EEA requires that businesses take a close look at all their procedures involving confidential information. Standards of contracting authority and rules for entering into nondisclosure agreements should be reviewed, in order to control the process of assuming, tracking

and enforcing confidentiality obligations towards third parties. Hiring practices should be reviewed, to avoid hiring tainted employees and consultants, and to emphasize respect for intellectual property rights as a part of the company's training program. Perhaps most importantly, the company must examine its business relationships, in order to determine the procedures and behaviors of those who may create vicarious liability under the EEA.

The central feature of a strategy for avoiding criminal liability is the "compliance plan." Compliance plans are helpful means of preventing others' trade secrets from entering the workplace. They take on a special significance in the context of the EEA, however, because federal prosecutors will focus in part on the existence and enforcement of compliance plans in deciding whether corporations are guilty of knowing theft of trade secrets, and because under the Federal Sentencing Guidelines courts applying the EEA will take them into account in assessing punishments.¹⁷²

a. Who Should Create a Compliance Plan: A Checklist

The EEA applies to organizations of all types, and in the abstract every company can benefit from implementing a compliance plan. However, some businesses are more exposed than others, and the following checklist should be considered in determining how important it is for any specific company.

- **High competitive visibility**

The more competitive the market and the more visible the company within that market, the more likely that others (competitors and prosecutors) will care about perceived violations. Success in highly competitive markets breeds envy and makes one a target for those who may be motivated to go to the authorities and encourage prosecution as a way to level the playing field.

- **Focus on technology and information**

Although the EEA applies to all sorts of business information, prosecutors are likely to focus their efforts on the protection of technical data, leaving disputes over customers lists to be solved in the civil courts. The more that a company relies on, deals in, or produces valuable technical information, the more likely it is to be involved (either as victim or accused) in trade secret theft.

- **Rapid growth through hiring**

It has long been recognized that most information loss occurs through employees. A corollary of that principle is that these employees complete the act when they pass on the information to someone else. Companies that are in a period of frenzied growth, or in intense competition for qualified employees, are prone to be less cautious than they might about who is hired and how well they are screened and trained to avoid incoming data infection.

- **Significant reliance on consultants and temporary workers**

As noted above, temporary help and consultants present a particularly high risk of infection, since their loyalties are unclear and their perceived utility increases with the variety of their past exposure to other businesses. The more that a company relies on this sort of resource, especially in the sensitive areas of research and development, the more it is exposed to trade secret theft problems.

- **Extensive outsourcing, joint ventures, other "collaborative" or "virtual" business**

The extraordinary pace of change in modern commerce, coupled with vastly improved means of communication, has led to such phenomena as "collaborative engineering", the "virtual corporation" and the "empowered employee". All of these presumably useful organizational techniques involve broad sharing of information among entities and individuals that may have different agendas and reporting responsibilities. Trying to keep track of who should be in possession of what data is extremely difficult. It is precisely this sort of high-risk environment, however, where good faith attempts to manage and to prevent violations are most important even where they cannot be completely effective.

- **Foreign subsidiaries/affiliates and other foreign operations**

The EEA started its journey in Congress as a statute focused on foreign state-sponsored industrial espionage. Given that history, and the increased penalties that apply to cases involving foreign entities (many of which may be under at least indirect control of their local governments), compliance plans are especially indicated for businesses with foreign facilities, subsidiaries, affiliates or venture partners.

b. Objectives of a Compliance Plan

- **Prevent infection**

A compliance plan should not exist exclusively, or even primarily, to keep the company from being indicted or sued. Rather, the critical purpose is to prevent unauthorized secrets from entering the company's knowledge base. In short, the plan must be designed to work, not just to look good.

- **Prevent loss**

Although a plan's primary objective is to prevent information from entering the facility, a by-product should also be that the company's own valuable information is retained. Good compliance plans will generally raise the level of awareness within the organization about the importance of intellectual assets. Being more careful about the handling of others' data usually leads to greater care for one's own. Considering that the vast majority of trade secret loss occurs through employee inadvertence, the compliance plan looks to be an extremely cost-effective way to protect investment in research and other secrets.

- **Increase chance of early discovery and reporting**

Information loss is inherently difficult to detect, because the original property remains intact, apparently untouched. Only surrounding circumstances, such as an employee's furtive behavior or a competitor's inexplicably quick product development, may provide clues. The same applies to a company that might have received trade secrets through (for example) a new hire. With a program in place to sensitize the organization to how data can be compromised, violations are most likely to be spotted at an earlier time. Internal investigations will be more focused, and the company will be more likely to contain the problem, before it gets out of hand and management becomes less inclined to report it.

- **Protection against exposure to criminal liability**

Companies don't go to jail, but their officers do. And fines can be substantial. Just the expense, diversion and embarrassment of defending against criminal charges are significant enough to justify measures taken to prevent getting involved in this sort of nightmare. A compliance plan is no guarantee against indictment, but a good plan properly implemented makes it much more likely that the authorities will view the company sympathetically and decide not to prosecute, or to concentrate exclusively on the

culpable individuals. The EEA requires a *knowing* theft,¹⁷³ and compliance procedures can effectively isolate those who have the requisite knowledge and intent.

- **Reducing punishment for criminal conduct**

Federal sentencing guidelines have been published to assist courts and prosecutors in deciding how to punish crimes, and to achieve some uniformity in sentencing. Chapter 8 of these detailed guidelines (found in the last three volumes of Title 18 of the United States Code) applies to criminal activity by a corporation. In effect, the guidelines are a sort of scorecard by which an organization's culpability is measured. Various criteria such as the value of the property stolen, management knowledge, speed of reporting, cooperation and the like are all assigned point levels. Bad conduct or circumstances will increase the points, and good conduct will decrease them. The point total then becomes the most important determinant of fines and jail time.¹⁷⁴ A central feature of the guidelines for corporations is the existence of a "compliance plan" that recognizes the possibility of criminal behavior within the enterprise and seeks to prevent it. A good compliance plan can take off a lot of points at sentencing, but it can also be the key to convincing a federal prosecutor that the company found to possess trade secrets has in fact been victimized by an errant employee.

- **Protection against exposure to civil liability**

Lawsuits for trade secret theft have been a regular part of the commercial scene (especially in technology-related industries) and they are on the rise. Heightened competition in most markets means that even slim advantages provided by secret information will be worth fighting for. Just as in the criminal context, having a compliance plan is not insurance against lawsuits, but it will make them less likely. When unauthorized secrets are discovered and reported early, a business solution almost always results. Relationships are preserved, and the expense and diversion of emotional litigation is avoided. Institutionalization of ethics pays.

c. Elements of a Compliance Plan

- **Custom design**

The Sentencing Guidelines require that compliance plans be designed for the specific organization and the real world risks that it faces. There is no one-size-fits-all solution. Among the factors that must be considered are size of the company (the larger the company, the more formal the plan); risks inherent in the business (for example, a specialty fabricator that necessarily handles a lot of customers' secret information); past history of security problems or trade secret theft; and any applicable industry or government standards related to information security.

- **Standard of conduct**

The company must describe with specificity the kind of behavior it wants, and the kind it will punish. Employees and agents cannot be guided effectively by general principles. Wherever there are kinds of risk peculiar to the operations or environment of the enterprise, those should be singled out and direction given on avoiding them. Knowing what conduct will not be tolerated, however, is only half of the picture. The plan must also communicate what is expected when a problem is discovered: who should be notified and what sort of investigation should be conducted. Finally, the disciplinary consequences of noncompliance must be spelled out.

- **High level responsibility**

Compliance plans designed and managed by relatively low-level functionaries will not impress prosecutors or judges. A key aspect of the guidelines requires that "high-level personnel of the organization" be a part of defining and enforcing the plan. In general, ultimate responsibility for this function should lie with someone in the executive ranks who has authority to influence compliance in a meaningful way.

- **Communication and education**

There is no value to a compliance plan that lies on the shelf. It is essential that the plan not only be communicated but also "sold" to the appropriate constituencies (employees, contractors, consultants, vendors, affiliates) as an important part of the corporate ethic. This effort focuses initially on the screening and initiation of new employees; but it must be ongoing because of employee turnover and other changed circumstances. Keep in mind that education is inexpensive relative to the cost and difficulty of solving

problems after they occur. And to the extent that the plan is meant to ward off indictment of the company, it will count for little if it has not been promoted.

- **Monitoring**

There are two basic aspects to monitoring. One addresses the company's operations: monitoring behavior sufficiently that violations are likely to be discovered and reported within the organization. Records should be maintained to demonstrate that the company took all reasonable steps (i.e., within bounds of common sense and individual privacy rights) to observe activity that might indicate a misappropriation of trade secrets. The second part of monitoring consists of auditing and assessing the compliance system for effectiveness, making changes as indicated.

- **Implementation**

In considering the sufficiency of a compliance plan the authorities will first look at the plan itself, but ultimately it is the company's action to implement the plan that matters. Indeed, a comprehensive program on paper that is not followed in practice may be worse than having none at all, since it will reflect a clear understanding of the problem coupled with a conscious decision to ignore it. Implementation must be a clear part of the duties of assigned management, whose performance should be measured with this part of their responsibilities in mind.

- **Discipline**

The company's records must show that any violations have been the subject of appropriate discipline. This includes failures to detect and report an offense, since the effectiveness of the plan will be judged in large part on how well it motivates individuals to provide the necessary self-enforcement. Exactly what sort of discipline should be meted out for specific violations of the standards of behavior is not specified in the guidelines. It should be sufficient that thoughtful consideration has been given to the question in the context of the organization's culture, experience and other disciplinary standards.

- **Reporting**

Law enforcement depends heavily on organizations to be self-policing. This means that an effective compliance plan should require that individuals report violations (and suspected violations) to

responsible management. It also means that company management, following investigation to confirm the existence of a probable violation, should be encouraged not only to notify the owner of the stolen secret, but also in an appropriate case to contact the authorities.

2. Defense of an EEA Prosecution

a. Importance of Criminal Procedure

Those who have become targets of a criminal investigation must above all recognize the special seriousness of the situation. Although trade secrets are a species of intellectual property, a criminal charge of trade secret theft is unlike most other kinds of intellectual property disputes. The wide sweep of the law, the difficulty in defining the subject matter with precision, the emotional (and perhaps political) content of the problem, and the extraordinary consequences of violation create a high level of risk. Companies accustomed to resolving legal issues in the civil arena have to understand their need for specialized advice in dealing with the arcana of criminal procedure.

b. Joint Defense and Indemnification Agreements

In many cases arising under the EEA there may be several targets of a criminal investigation and ultimate indictment. These can consist of employees and other individuals, a company and its affiliates or business partners. All of these share an interest in defense of the potential or actual charges, and may find it useful and cost-effective to share information and strategies. This should occur only under a joint defense agreement, which preserves the attorney-client privilege and work product protections. In addition, individuals and entities may have rights of indemnity (for example, a company officer operating within the scope of his employment) at least for the cost of defense, and these rights should be examined and asserted as appropriate. [NOTE: is there a risk of one defendant "turning" on the others? Peter?]

c. Civil Litigation and Other Business Issues

The defendant in a civil case should always consider the possibility of a criminal referral relating to the conduct in issue, and should explore with qualified counsel the consequence of active participation in the civil matter. This is especially true where technical trade secrets are involved, or where there is a plausible connection with some foreign government. Although a civil compromise may not prevent or derail a criminal proceeding, it is typically useful to explore settlement at the earliest opportunity, since the authorities will as a practical matter be less interested if the matter has been resolved to the victim's satisfaction before substantial investment of investigative or prosecutorial resources.

Where a company before being sued discovers that one of its employees has compromised trade secrets belonging to someone else, the best strategy (following an appropriate investigation) is usually to provide prompt notification to the owner of the secret. Full disclosure, expressions of regret, and offers to make amends can avert both civil and criminal processes.

V. CONCLUSION

The EEA has raised the stakes in the business of protecting trade secrets. A federal criminal prosecution is a powerful weapon, and one that is not invoked lightly. The breadth of the EEA and the strength of its penalties require that anyone with an actual or potential trade secrets dispute take careful notice of its provisions. Understanding the Act, and understanding how it is likely to be applied, are critically important both for victims and for potential defendants.