5 Tex. Intell. Prop. L.J. 177

Texas Intellectual Property Law Journal
Winter, 1997

UNDERSTANDING THE ECONOMIC ESPIONAGE ACT OF 1996

James H.A. Pooley[a1] Mark A. Lemley[aa1] Peter J. Toren[aaa1]

Table of Contents

***178** 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 Lofgren[1]

I. Introduction

A significant gap has existed in trade secrets law for many years. Given the increasing 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 generally not been available at the local level. Federal law has not provided an effective remedy either, since the depression-era statute covering interstate transportation of stolen goods has been held inapplicable to "intangible" intellectual property.[2]

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 ***179** was estimated that almost two dozen foreign governments have established means of clandestine acquisition of U.S. industrial secrets.[3]

The Economic Espionage Act of 1996[4] was intended to address both the general need for a federal criminal deterrent against trade secret theft and the apparent threat of industrial espionage sponsored by foreign states. This Article examines the background of this new law, provides critical analysis of its most important terms, describes the process of referring trade secret theft to the federal authorities, and suggests practical strategies for businesses seeking to take advantage of this resource and for those seeking to avoid exposure to liability for the mishandling of information belonging to others.

II. Background: Need for Legislative Reform

A. 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 trade secrets.[5] Thus, 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),[6] and the Wire Fraud[7] and Mail Fraud[8] statutes. ***180** However, as we will be discuss, a recent court decision severely curtails the use of ITSP. Moreover, the use of the Mail Fraud and Wire Fraud statutes has always been limited because many thefts do not involve the use of mail or wire, as required by those acts. In addition, since most trade secret thieves merely copy information and do not necessarily "defraud" the victims permanently of the data, prosecutions are further limited. Finally, while some state criminal trade secret statutes do exist[9], 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 Fraud statute, and the Wire Fraud statute, as well as the need for specialized legislation in this area.

B. 18 U.S.C. § 2314

The ITSP provides, in pertinent part:

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

This statute was enacted by Congress in 1934 to fill an enforcement gap in the National Motor Vehicle Theft Act.[11] Both statutes were intended to aid individual states in the detection and punishment of criminals seeking to evade state authorities by fleeing in stolen vehicles or with stolen property over state lines. However, the ITSP was drafted at a time when information did not have the economic value it has today, and could not be quickly copied and instantaneously transmitted to any location in the world. Therefore, the Act 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*,[12] it is uncertain whether ITSP can be used to charge a person with trade secret theft where no tangible property has been transferred across state lines.[13] In particular, the decision in *Brown* casts serious doubt on whether the phrase ***181** "goods, wares and merchandise" contained in section 2314 covers intangible property.[14]

In that case, the grand jury indicted Brown for violating section 2314 based on allegations that Brown had transported computer programs, software and source code interstate from Georgia to New Mexico.[15] Brown moved to dismiss the indictment, arguing that under *United States v. Dowling*,[16] the government failed to allege that he transferred "physical goods, wares or merchandise" in interstate commerce, within the meaning of section 2314.[17] The government admitted that it would not be able to prove that Brown made a copy of the source code using, for example, the company's hard disk, or that Brown had in his possession any tangible property belonging to the company.[18] The trial court had 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."[19]

The appellate court agreed, citing *Dowling*.[20] In *Dowling*, the defendant was convicted of violating section 2314 following his interstate distribution of bootleg Elvis Presley records.[21] The Supreme Court reversed the conviction and held that it was not Congress's intention that the ITSP function as a criminalization of copyright infringement.[22] The Supreme Court emphasized that its decision did not necessarily extend to situations where the initial procurement was accomplished by theft or fraud, and that courts have never required that the items stolen and transported remain in entirely unaltered form.[23] However, the Court emphasized that

> these 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.[24] ***182** Quoting this language, the *Brown* court 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"[25] and, thus, "cannot constitute goods, wares, merchandise which have been stolen, converted or taken within the meaning of sections 2314 or 2315."[26] The *Brown* court also stated that *United States v. Riggs*[27] was in error in light of the *Dowling* decision.[28]

In *Riggs*, the defendants, Robert J. Riggs and Craig Neidorf, were indicted for wire fraud and interstate transportation of

stolen goods.[29] According to the indictment and pleadings, Riggs gained unauthorized access to the Southern Bell Data Network (SBDN) and eventually to a sensitive portion of the computer that contained allegedly proprietary Southern Bell files, including the enhanced 911 (E911) file.[30] Riggs "downloaded" a copy of the E911 text file to his home computer located in Atlanta.[31] He then made a copy of the file available to a friend, Craig Neidorf, who was the co-editor of a computer hacker newsletter known as "Phrack."[32] Neidorf downloaded the copy to his home computer at the University of Missouri.[33] After making various revisions to remove all references to Southern Bell, Neidorf published the text file in an issue of Phrack.[34] Riggs and Neidorf were charged with two counts of wire fraud, two counts of violating the ITSP, and three counts of violating the Computer Fraud and Abuse Act of 1986.[35]

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 was never meant to cover the theft of intangible computer data.[36] However, the trial judge rejected Niedorf's "disingenuous" argument that he ***183** merely transferred electronic impulses across state lines.[37] 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 .... T he mere fact that the information actually crossed state lines via computer-generated electronic impulses does not defeat a charge under section 2314."[38] 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."[39] Not surprisingly, after presenting the issue in this manner, the court 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.[40]

The court was thus unwilling to read a "tangibility requirement" into the definition of "goods, wares or merchandise."[41]

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 the E911 file constituted "goods, wares, or merchandise," since the defendant and others had the ability to access the information in viewable form from a reliable storage place that "also [made] the information tangible, transferable, salable and, in this court's opinion, [brought] it within the definition of 'goods, wares, or merchandise' under § 2314."[42] Here, the *Riggs* court was arguably elevating form over substance. In other words, it is clear that defendants Riggs and Neidorf misappropriated the computerized text file. However, section 2314 is not directed toward the act of theft, but rather toward the criminalization of interstate *transfer* of stolen "goods, wares, or merchandise."[43] Thus, the court in *Riggs* did not address the issue of whether purely intangible property is "goods, wares or merchandise"; instead, it determined that the acts of the defendants should be covered by section 2314 because, in the court's opinion, most types of stolen intangible property should be treated the same as stolen tangible ***184** property.[44] If this reasoning were applied to *all* intangible property, though, 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." Furthermore, section 2314 would extend to other areas, such as the interstate transportation of patent-infringing goods. Thus, if a person "stole" a patented invention and then shipped an article manufactured in accord with the stolen patented specifications via interstate commerce, he or she could be successfully prosecuted under section 2314, according to the reasoning of the *Riggs* court. However, Congress surely did not intend to criminalize patent infringement through the back door.[45]

On the other hand, if the *Brown* decision were followed by other circuits, federal prosecutors would be prevented from charging a person with a violation of section 2314 for transporting a valuable trade secret via interstate commerce (provided no tangible property were also stolen). The *Brown* decision limits the prosecutor's ability to prosecute section 2314 violations to only those situations where a defendant illegally misappropriates a tangible item containing an intangible component. For example, a defendant could be prosecuted for violating section 2314, if the misappropriated trade secret were written on paper that belonged to the victim. The *Brown* decision suggests that such actions violate section 2314, even where the value of the paper is insignificant and is almost wholly derived from the intangible component.[46] However, in an increasingly electronic environment, where ***185** 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. Furthermore, there is no good reason why the law should treat two defendants (both of whom misappropriated equally valuable trade secrets) differently merely because one of the defendants misappropriated the trade secret by using a computer diskette

belonging to the victim and the other misappropriated the trade secret without taking any of the victim's tangible property. These short-comings of section 2314 underlie Congress's decision to enact the Economic Espionage Act of 1996.

C. 18 U.S.C. §§ 1341 and 1343

The federal Wire Fraud and Mail Fraud statutes proscribe any scheme, involving use of the mails or of interstate wire transmission, for obtaining "property" by false pretenses or representations.[47] 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.[48] The broader scope results from the use of the word "property" in section 1341 and section 1343 as compared to the narrower phrase "goods, wares and merchandise" used in section 2314. For example, in *United States v. Seidlitz*,[49] the defendant used knowledge of his former ***186** employer's computer system to enter the system and download computer data.[50] The appellate court upheld the trial court's determination that the software qualified as property within the meaning of the wire fraud statute.[51] The court held that the software was a trade secret (even though similar programs were in the public domain) because the 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.[52] 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.[53]

However, the Mail Fraud and Wire Fraud statutes do not completely close the enforcement gap created by *United States v. Brown*, because trade secret misappropriation often does not involve the use of interstate mail or wire. Moreover, since trade secret thieves often merely copy the information and do not necessarily "defraud" the victims permanently of the data, they cannot be charged with fraud.

D. 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 may have been crucial in establishing that company's "market edge." Furthermore, many companies elect not to pursue civil remedies for a variety of reasons: (1) defendants are often judgment proof; (2) civil litigation can be extremely expensive and there is no guarantee of success; and (3) private individuals and companies often lack the investigative expertise and resources necessary to prove that a defendant has misappropriated a trade secret. Moreover, only 24 states presently have criminal statutes specifically directed toward the theft of trade secrets,[54] and the applicability of these state criminal laws is limited by jurisdiction and lack of state resources, particularly in cases with international ramifications. As a result, by 1995 a consensus was reached among law enforcement officials that some sort of federal law was needed.

*187 E. Conclusion

As noted in the legislative history of the Economic Espionage Act, problems with prosecuting the theft of trade secrets under federal criminal law led United States Attorneys' Offices to decline matters that involved employees of U.S. corporations attempting to sell proprietary information to foreign governments.[55] Legislators realized that 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 that could bring federal resources to bear against defendants who steal proprietary information. In response to these concerns, Congressman McCollum introduced the Industrial Espionage Act of 1996 on June 26, 1996.[56] This bill was to eventually become the Economic Espionage Act of 1996 (EEA).[57] As originally written, it only applied to thefts of trade secrets committed to benefit a "foreign government, foreign instrumentality or foreign agent."[58] 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.[59] On September 18, with certain amendments, it passed the Senate. On September 28, 1996, the House amended the Senate version and passed it.[60] On October 2, 1996, the Senate concurred in the House amendments.[61] It went to President Clinton on October 4, 1996, and he signed it on October 11, 1996.[62]

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 secrets[63] that is taken, with only minor modifications, from the definition in the Uniform Trade Secrets Act (UTSA).[64] At the same time, the sections defining misappropriation[65] are entirely ***188** 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 public....[66]

This definition, which was added late in the Congressional session,[67] generally tracks the definition of trade secret in the UTSA.[68] 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 UTSA, though it has been narrowed some from earlier versions of the ***189** statute.[69] It is not clear why Congress chose to expand upon the representative list in the UTSA. Because of the expansive interpretation already given to the UTSA definition,[70] the EEA will probably apply to 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 statute,[71] until recently, applied only to the theft of scientific or technical information.[72] By contrast, the language of section 1839 makes clear that the theft of business or financial information (including perhaps some types of insider trading)[73] 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."[74] 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 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.[75] However, we believe that this language should be read in light of the repeated statements in the legislative history indicating that former employees should not be punished under the EEA merely for taking with ***190** them the general skill, knowledge, and industry experience they have acquired on the job.[76]

Third, the definition of reasonable precautions generally tracks that of the UTSA, with one possible exception. The EEA places the burden of taking such precautions on the "owner" of the secret.[77] "Owner" 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."[78] 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 this "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.[79] The effect of this wording may 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,[80] the "reasonable precautions"

test seems aimed at different goals, such as assuring that the trade secret owner does in fact consider the information to be valuable and secret and that the owner puts potential defendants on notice that the information is considered secret.[81] 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.[82] Similarly, ***191** 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 UTSA, information is "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."[83] Generally, this means that the question is whether one's competitors actually know or can easily discover the secret. By contrast, the EEA, without explanation, changes the relevant person from the competitor to "the public."[84] The import of this change 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 scientific circles, 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.[85]

One issue that is not addressed by the statute, but 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 (at least theoretically) may file a complaint and even proceed to trial without ever having specifically identified the trade secrets they claim were stolen.[86] Even in states that require plaintiffs to identify their trade secrets early in the litigation process,[87] parties regularly change the description of their trade secrets during litigation, and even during trial.[88] By contrast, the legislative history suggests that "particularity" in describing trade secrets will be important under the EEA. Indeed as one Congressman noted, "a prosecution under the EEA *must* establish a particular piece of information that a person has stolen or misappropriated."[89]

***192 B. Defining Misappropriation**

Although the EEA, with a few exceptions, stayed on the well-defined path of the UTSA in defining a trade secret, it created an entirely new definition of what constitutes misappropriation. In fact, the EEA 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 the defendant acted. In this section we examine first, the conduct covered by the EEA, and second, the actors who may be liable.

1. Prohibited Conduct

Sections 1831(a) and 1832(a) contain identical language regarding acts of misappropriation. Both sections punish any 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 ....[90]
These provisions are, in some respects, significantly broader than corresponding civil trade secrets laws, such as the UTSA.[91]

Subsection (a)(1) lists several means of improper acquisition of a trade secret. In general, the provisions of this section seem to track the "improper means" of acquisition punishable under civil law.[92] 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.[93] However, the provision also makes it a crime to "appropriate" or "take" a secret without authorization from the trade secret owner.[94] These terms might encompass the sort ***193** of lawful business espionage that has long been permitted by civil trade secrets law-- conduct such as 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.[95] While the legislative record alone might be sufficient to declare broad categories of competitive intelligence-gathering proper and therefore lawful, the ambiguity of some of the terms in subsection (a)(1) is troubling. From a practical standpoint, though, the issue may be moot, since 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 subsection (2), which gives the trade secret owner the right to control a whole host of activities such as duplication, transportation, or destruction of a trade secret.[96] This provision encompasses more than its civil counterparts. Subsection (2) is not, by its terms, limited to secrets acquired by "improper means," like those listed in subsection (1). Even legally acquired secrets can be misappropriated under the EEA if they are analyzed or duplicated in one of the ways listed in subsection (2). The civil law does prohibit some such uses of a lawfully acquired trade secret, but limits its reach to the disclosure or use of a secret in violation of a confidential relationship.[97] By contrast, there is no requirement of such a confidential relationship under 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 anyone from engaging in any of the enumerated acts in subsection (2), even if the secret is contained in a product that the defendant lawfully acquired.[98] 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. This indicates Congress's belief that trade secret law is rooted in property theory, as opposed to tort or contract.[99] Furthermore, some of the specific provisions in subsection (2), such as ***194** the prohibition against "altering" or "destroying" a trade secret, are outside the normal reach of trade secret law.[100] 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 based on noneconomic motives, such as the defendant in *United States v. LaMacchia*.[101] For this reason, the EEA will be of limited use in many cases involving computer hackers.[102]

***195** The most troubling aspect of subsection (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.[103] To be sure, some types of reverse engineering, such as looking at or tasting a lawfully acquired product in order to determine its content, will not be illegal under the EEA.[104] On the other hand, several of the restrictions in subsection (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.[105] 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 to bond to secret chemicals or to precipitate out certain elements from the formula.

The legislative history of the EEA is not encouraging to those who reverse engineer. The Congressional Record states 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.[106]
The Record goes on to suggest that observing a lawfully purchased product or tastetesting a Coca-Cola is a legitimate activity.[107] 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 USTA, copyright law, and the common law, without ***196** fear of civil liability.[108] However, under the EEA, the same programmer would apparently be committing a felony.

The inadequate 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.[109] The Supreme Court sees reverse engineering as the economic centerpiece of state trade secret law, and indeed the primary means by which trade secrets are allowed to coexist peacefully with federal patent and copyright protection.[110] While there is no issue of federal preemption of the EEA (since the Act is itself a federal statute), it is surprising that Congress has apparently permitted a major shift in the balance traditionally struck between intellectual property owners and competitors, and has done so for the first ***197** time with little or no fanfare in a criminal

statute.[111] Given the stated intent of Congress not to endanger legitimate business competition[112] and to reach only "flagrant and egregious cases of information theft,"[113] 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,[114] or, in the alternative, that the law will simply be amended to expressly protect reverse engineering.

Finally, it is worth noting that subsections (3)-(5) of the EEA punish the knowing receipt of misappropriated trade secrets, attempts to misappropriate trade secrets, and conspiring to appropriate trade secrets, respectively.[115] Subsection (3) also punishes the knowing possession of a trade secret.[116] In effect, this is likely to be comparable to subsection 1(2)(ii)(C) of the UTSA, which punishes the use or disclosure of information known to be acquired by accident or mistake.[117] Because subsections (3)-(5) of the EEA 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."[118] This was originally the heart of the EEA, and was designed to cope with the problem of foreign business espionage.[119] 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 ***198** "substantially owned, controlled, sponsored, commanded, managed or dominated by a foreign government."[120] The Congressional Record indicates that the intent of section 1831 is to target foreign government action, not any act of espionage undertaken by a foreign corporation.[121] This distinguishes the EEA from section 1337 proceedings in the International Trade Commission, which focus merely on the nationality of defendant companies.[122]

However, the language of section 1831(a) does not only make foreign governments and their agents liable, but rather anyone who misappropriates a trade secret "intending or knowing that the offense will benefit any foreign government."[123] The fact that only "knowledge" and not "intent to benefit" is required suggests that U.S. citizens who act for purposes other than economic espionage may still fall within the scope of section 1831. For example, a 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 the information was posted for a completely different purpose. That hacker may be subject to the enhanced penalties of section 1831 rather than the "normal" trade secret sanctions 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* (as opposed to foreign governments) cannot be held 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 ***199** that the offense will, injure any owner of that trade secret."[124] 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.[125]

Nonetheless, there are several limitations in scope evident in section 1832. First, section 1832 requires three different elements of intent.[126] The defendant must "knowingly" commit one of the listed acts of misappropriation.[127] In addition, the defendant must act "with intent to convert a trade secret ... to the economic benefit of anyone other than the owner thereof,"[128] 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 should be free." Finally, section 1832 requires that the defendant act "intending or knowing that the offense, will injure any owner of that trade secret."[129] The second and third provisions differ from the prevailing rule in civil cases. Under the Restatement and the UTSA, there is no absolute 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.[130] Furthermore, there is no requirement in civil trade secrets law that the defendant intend or know of the potential economic loss to the ***200** plaintiff.[131] On the other hand, state criminal trade secrets statutes generally do require knowing misappropriation.[132] The requirement of knowledge or intent serves to limit the applicability of the EEA in "doubtful cases," where the defendant acts without knowledge that his actions are wrong.[133]

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."[134] 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 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"[135] or information discovered but not used by a company, both of which qualify as trade secrets under the UTSA (though not the Restatement of Torts).[136] One effect of this limitation may be to restore the unfortunate rule of *SI Handling v. Heisley*,[137] where employees who had an obligation to assign an invention were allowed to retain it without trade secret liability provided they had not actually told their employer about it.[138] This ***201** limitation is also not explained in the legislative history, nor does it 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 could 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, the government might argue that the *defendant's* incorporation of a secret into a commercial product triggered liability under the EEA. Both of these readings are possible under the Act, and would avoid the limiting interpretation discussed above.[139]

C. Penalties

Violations under both sections of the EEA are treated as serious crimes. Section 1832 provides for a term of up to ten years in prison and unspecified fines for individuals violating the EEA,[140] and fines of up to $5 million for corporations or other organizations that violate its provisions.[141] The amount of the fine imposed on individuals is not specified, which means that the general maximum fine for felonies ($250,000) should apply.[142] The legislative history suggests that, pursuant to the federal fines provision (18 U.S.C. § 3571(d)), the fine in cases of significant injury should be set at the greater of twice the value of the loss to the trade secret owner or twice the gain to the infringer.[143] 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, by relying on section 3571(d) rather than section 1832(b).[144] Section 1831 provides for an enhanced penalty in cases of foreign espionage-- the maximum prison term is raised to fifteen years,[145] and the maximum organizational fine is set at $10 million.[146] The maximum fine for individuals is set at $500,000,[147] rather than the normal felony maximum of ***202** $250,000. Evidently, the general approach of the statute is to punish foreign espionage more severely than domestic trade secret theft.

Section 1834 additionally provides for forfeiture of a defendant's property during sentencing.[148] Forfeiture of "any property constituting, or derived from, any proceeds the person obtained, directly or indirectly,"[149] from the theft is apparently mandatory.[150] 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 ,"[151] forfeiture of such instruments is discretionary rather than mandatory.[152] The proceeds and instruments in question are forfeited to the United States, rather than to the victim of the crime.[153] However, the Congressional Record suggests that victims may be able to seek restitution from the United States out of the forfeited proceeds.[154]

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.[155] 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."[156] Where the assets seized include the misappropriated trade secret itself--for example, where the secret is embodied in a product--the victim of the trade secret theft has a potential problem. Under section 1834, the government is granted title to the product embodying the victim's trade secret, and indeed has a mandate to auction that product to the highest bidder.[157] This is hardly consistent with the victim's interest in keeping the information secret. The victim's best recourse in such circumstances is to proceed under section 853(n) of the drug forfeiture statute, which specifies a procedure whereby the victim can petition the court to return all forfeited property in which the victim claims an ***203** interest.[158] Alternatively, the victim could seek to have the infringing goods destroyed, as is done with drugs. Either of these two options seems more probable than public sale. 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, where the products do not directly incorporate a stolen trade secret, but are instead indirectly derived from misappropriated knowledge. This situation is likely

to arise in cases involving "negative know-how." 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."[159] This strongly suggests that such derivative products are subject to seizure and sale, despite the intervening contribution of the 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.[160] 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 secret actions.[161] However, the government can use its injunctive power during the initial stages of prosecution to maintain the status quo or prevent public disclosure of a victim's secret. On balance, the deterrent effect of a pending criminal action is such that preliminary injunctive relief will rarely be necessary: no reasonable lawyer would advise her client to continue to engage in conduct that 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 injunctive relief under existing state trade secrets laws.[162] For the majority of cases, however, section 1836 adds little--besides federal court jurisdiction--to what can already be accomplished using state law.

*204 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.[163] The territorial reach of the statute is extremely broad. It applies not only to acts conducted entirely within the United States, but also to foreign schemes, provided any "act in furtherance of the offense was committed in the United States."[164] This is consistent with the goal of reaching foreign espionage, much of which occurs outside the United States. However, section 1837 also hypothetically sweeps within its scope acts which are primarily foreign in nature. For example, if the government of Algeria acquired the secrets of a Tunisian company through espionage, the misappropriation would violate the EEA, and could be prosecuted in the United States, if a single act in furtherance of the scheme occurred in the United States. Furthermore, under section 1837(1) of 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.[165] 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, one 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 the clear signal that Congress ostensibly intended. There are also several problems with the EEA. Some of these problems--such as the lack of an explicit provision 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 broad provisions can be ameliorated to some extent by the exercise of prosecutorial discretion within the Justice Department; we discuss such prosecutorial issues below. On the other hand, the loopholes in the statute cannot be removed so easily. ***205** However, the fact that state civil and criminal sanctions continue in force[166] may help to solve existing problems.

IV. Strategies

Unlike other forms of intellectual property, trade secrets require a great deal of self-help 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, owners of secret information, and those who handle information belonging to others) consider 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 differ greatly 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 Attorneys' offices are very busy and handle a wide variety of cases, which often involve defendants who are accused of committing heinous crimes.[167] Additionally, scarce resources have forced many United States Attorneys' offices to set monetary thresholds in white collar crime cases, including those involving intellectual property. Such thresholds may be keyed to the amount of the defendant's financial gain or the amount of the victim's financial loss. Furthermore, the higher standard of proof in criminal cases may mean that, while a victim might have a very strong civil case, the matter may still be unsuitable for criminal prosecution and therefore 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.

*206 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 to adequately 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 the charge. By contrast, the burden of proof in civil cases is "preponderance of the evidence," which means that the jury, or the judge, must decide which party's version of the facts is more likely to be correct. Many victims and their lawyers who are 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 become even more difficult in a trade secret case that involves complex technology not easily understood by the jury, or in one that implicates philosophical concerns about an individual's right to move to a new job.

b) Discovery and the Protection of Trade Secrets

Discovery in criminal cases is also different than in civil cases. Because of the public nature of criminal trials, additional details about the trade secret (which would otherwise be kept from the public in civil litigation) might be disclosed in a criminal case. However, there are effective means of managing and limiting this risk. Two types of disclosure are generally at issue in EEA cases: (1) disclosure to the defendant and his lawyers; and (2) disclosure to the general public. Referral to federal law enforcement of a matter involving the theft of a trade secret does not necessarily mean that the details of the trade secret will be disclosed to the public. During the time that the matter is being investigated by a federal agency and is being presented to a grand jury by a United States Attorneys' office, the trade secret will not be disclosed to anyone because of constitutional and statutory protections, as well as the nature of the federal criminal justice system. 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 many trade secrets have a short "shelf-life," by the time of trial 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.[168] The principal function of a federal grand jury, therefore, is to decide whether to approve or "return," an indictment proposed by a federal prosecutor ***207** charging federal felony violations. 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 the "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."[169]

In deciding whether to approve indictments, the grand jury may also perform an investigative function, for which its powers are broad.[170] It can compel the testimony of witnesses and the production of documentary and other physical evidence, subject to very few limitations.[171] 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."[172] While there are several exceptions to this rule,[173] from a practical standpoint, no details of the trade ***208** secret will be disclosed to the public during the investigative stage. Once the grand jury has returned the indictment, the victim should be aware that the protections afforded by Rule 6(e) are lifted and there is some risk that additional information may be disclosed due to the federal discovery rules in criminal cases.

Rule 16 of the Federal Rules of Criminal Procedure requires federal prosecutors to provide the defense with: (1) all relevant 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 criminal 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.[174] There is also a continuing duty upon the prosecuting attorney for the government to exercise due diligence in disclosing additional information within these categories that may become known to him at any time before or during trial.[175] Furthermore, the government has a duty to disclose exculpatory evidence material to findings of guilt or innocence, or the amount of punishment.[176] Finally, under the "Jencks Act," the government must produce statements of all trial witnesses.[177] 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, similar disclosures would probably also be required in civil cases.

In drafting the EEA, Congress was concerned about additional trade secret disclosures during criminal prosecutions. 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 ***209** Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws."[178] Accordingly, the victim should continue to work with federal prosecutors after the indictment has been returned to seek an entry of orders that will preserve the status of the information as a trade secret and avoid unnecessary disclosure of the information.[179] Moreover, 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 the court their name, employment history, and other relevant information.[180]

Additionally, courts can limit the disclosure of information to the public even during the proceedings without necessarily violating the defendant's right to a public trial under the Sixth Amendment. Although the right to a public criminal trial is protected by the Sixth Amendment, the right is not absolute and may be limited in appropriate circumstances.[181] At least one circuit court has recognized a district court's power to restrict access to that portion of the proceeding which would reveal trade secrets. In *Stamicarbon N.V. v. American Cyanamid Co.*,[182] on appeal of a criminal contempt conviction, the Second Circuit held that a district court may limit access to portions of the proceedings if the court determines that: (1) a party would be 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."[183]

Victims should make sure that prosecutors seek to prohibit the public disclosure of the trade secret during trial. This can be achieved by requesting that the court deny public access during the testimony of expert witnesses who are called upon to describe the details of the trade secret. Of course, a court order limiting ***210** public access to an expert witness's testimony should include a similar limit on access to trial transcripts.

2. Factors That Enter Into the Decision Whether to Prosecute

As noted above, limited resources have forced many United States Attorneys' offices to set guidelines on what type of cases will be investigated and prosecuted. Such guidelines may also reflect the philosophy of the current United States Prosecuting Attorney in a particular district. However, this does not mean that United States Attorneys' offices are completely rigid in their application of these guidelines. Failure to meet certain criteria does not necessarily mean that the United States Attorneys' 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.

In almost all other types of criminal matters, a United States Attorneys' Office usually makes the final determination on whether to investigate and prosecute a case. However, before a United States Attorneys' Office can seek to return an indictment alleging a violation of section 1833, it first must obtain the approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for the Criminal Division.[184] It is not clear how this approval authority will be exercised or what type ***211** of regulations will be issued, but it is expected that the local prosecution 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 was clearly a trade secret; (b) whether the information was technical or scientific in nature; (c) evidence of criminal conduct and intent; (d) evidence of the information's monetary value; (e) the availability of other remedies; and (f) whether the misappropriation was promptly reported. An analysis and understanding of these factors should be helpful to victims considering whether to refer a matter to a United States Attorneys' office and should maximize the chances for a successful referral.

a) Trade Secret

The issue of whether certain 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, namely that the information was not generally available to the public. Federal prosecutors will need access to objective and independently verifiable evidence showing that the information was truly secret. This evidence should also explain why the information 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 a technical journal or other similar publication. Because of the nature of trade secrets, the victim will generally be the best 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 the 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 trade secret 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 ***212** to protect the information.[185] 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."[186] The government does not need to prove that a specific jurisdictional amount was lost. However, in order to satisfy the informal monetary threshold set by many United States Attorneys' 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 significant expense in research and development.

b) Type of information

The EEA protects all information, regardless of type, that meets the statutory definition of a "trade secret."[187] The most obvious sort of trade secret is represented by research, formulas and other scientific information. Business information, such as sales forecasts, market studies, risk analysis, training materials, employee records, customer lists, and budgets, are less likely to be investigated because in most cases this sort of data is not obviously valuable enough to reach the threshold amount required by many United States Attorneys' offices. Moreover, it is often difficult to meet the standards of proof for business information. For example, it is very difficult for the government to prove beyond a reasonable doubt that a customer list was either not known to a competitor of the victim or was not legally obtainable. Furthermore, most business information depreciates in value so quickly that prosecution is not worth pursuing. Finally, business information is inherently more difficult to qualify through independent experts because it is more speculative in value, making 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.[188] The EEA even covers situations where the lawful ***213** owner retains the original copy of the trade secret and is not deprived of its use.[189] However, to overcome the potential problems of prosecuting a defendant's "mental recollections" or of rebutting a defense that "great minds think alike," it is essential to establish tangible evidence of theft.

Tangible evidence of theft may also be necessary to overcome a reverse engineering defense. The EEA does not expressly prohibit or permit reverse engineering. Thus, the legality of the defendant's activity hinges solely on whether or not that activity falls within the specific proscription of the EEA. In most instances, this can only be proven through tangible evidence of misappropriation. Without such evidence, the defendant may be able to successfully claim that the details of the trade secret were lawfully obtained through reverse engineering. Alternatively, the defendant may succeed in arguing that the information was developed independently.

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 may be able to establish misappropriation by showing that the defendant had access to the victim's trade secret and that the defendant was attempting to sell a product that is ostensibly based on that trade secret. However, without tangible evidence of theft, it is unlikely that the federal government will prosecute the case.

This does not mean that a victim should hesitate in reporting 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 theft, especially if the search warrant is executed shortly after the misappropriation. 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."[190] Thus, to assist the United States Attorneys' office in obtaining a search warrant, the victim must be able to describe very specifically both the information that was stolen and the tangible objects that might contain the information. The victim will also have to identify the location where the information would likely be found.

In cases where the victim believes that the trade secret was obtained by computer intrusion or was transferred over a computer network, the victim should ***214** carefully maintain all computer audit logs[191] to document the defendant's criminal activities. However, before monitoring 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.[192]

Besides establishing the act of misappropriation, ideally the evidence 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 discussed above, the EEA does not require the government to prove the exact monetary value of the trade secret for its criminal sanctions to apply.[193] However, many if not most United States Attorneys' 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. This minimum varies from office to office, but in some large districts the loss to the victim must exceed $100,000.[194] Since there is often no legitimate market for trade secrets, establishing economic loss is difficult, and meeting the monetary guidelines of some United States Attorneys' offices can be particularly arduous. However, the difficulty in establishing "economic value" should not deter the victim from presenting its case to the United States Attorney.

In some circumstances, the value of the trade secret can be established by showing the price that the trade secret would have brought on the open market. Civil cases are generally more helpful determining the initial value, but the issue has come up in

the criminal context as well. For example, in *United States v. Bottone*,[195] the court held that the value of stolen chemical formulae could be based on what ***215** European drug manufacturers were willing to pay for the information.[196] Similarly, in *United States v. Greenwald*,[197] the Sixth Circuit held that the value of the misappropriated trade secret could be established from: (1) the "viable, albeit limited" market among chemical companies for the type of formulae misappropriated; (2) from licensing agreements; or (3) from sales of the chemical formulae that were misappropriated.[198] Thus, in cases where the victim has sold or licensed the information embodied in the trade secret, it should supply this information to the U.S. Attorney for use during the evaluation process.

In situations 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, and production. To maximize the chances of a successful referral, the victim should be as specific as possible in assessing the dollar value of the loss and should avoid making generalized, unsubstantiated claims that the trade secret was its "crown jewels," or that the victim will go out of business if the defendant is not prosecuted. While such claims may 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 Attorneys' offices are reluctant to pursue matters criminally if the victim has civil remedies available, because the government does not want to take sides in business disputes. Therefore, the victim should be able to explain why civil remedies are inadequate. The legislative history of the Act makes clear that in the past, many companies did not bring civil suits because the defendants were judgment-proof, or the victims did not have the financial resources to investigate the theft and file a civil lawsuit.[199] Therefore, the presence of these factors is important to note when making a criminal referral. Similarly, the absence of a state criminal trade secret law or a jurisdictional obstacle to effective relief may make federal prosecution more compelling.

f) Prompt Reporting of the Theft

Victims should report trade secret theft to federal law enforcement as soon as possible for a variety of reasons. First, if trade secret theft is not promptly reported, the thief might claim that the information was discovered through "reverse ***216** engineering" or "parallel development" in the intervening time. Second, as time passes it becomes less likely that tangible evidence of the theft will remain.

Nevertheless, in most cases the victim should first conduct its own internal investigation. This will allow the victim time to make an informed decision regarding the prospects for a successful referral, and will also allow the victim an opportunity to decide how the case should be presented. Furthermore, this preliminary investigation will also assist the U.S. Attorneys' office in evaluating the matter by providing it with the 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, the victim should be mindful that the Fourth Amendment generally does not protect against searches by private individuals,[200] unless a particular individual is acting as a government agent.[201] Whether a private individual is acting on behalf of the government depends on two factors: (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.[202] Thus, once a victim has reported the theft to law enforcement, the victim should exercise great caution in investigating the theft any further to minimize the possibility of a Fourth Amendment challenge at trial.

B. The Owner's/Victim's 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 the outset is the most cost-effective way of enforcing trade secrets. Certainly, it is much less expensive than litigation. Second, the EEA tracks the UTSA in requiring, as a condition of protection, that the owner of the information have "taken reasonable measures to keep such information secret."[203] 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 by refusing to intervene in cases where the victim's negligence contributed to the loss.

***217** Fortunately for the victim, the standard of "reasonable efforts" is flexible. Guiding principles seem to boil down to simple cost-benefit analyses.[204] Within a very wide band of discretion, the trade secret owner must have considered 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 are certainly not perfect either; hence, some mistakes are permitted.[205] In the end, the trier of fact will have to decide whether the owner's conduct was excusable.

Despite the apparent vagueness of this standard, some guidelines have emerged through the case law. For example, although the trade secret owner must act reasonably, "heroic" measures are not necessary.[206] The most frequently cited decision in support of this proposition is *E.I. DuPont deNemours & Co. v. Christopher*,[207] in which the defendant acquired secrets about DuPont's process technology by aerial photography of a plant under construction.[208] Other cases have noted that avoiding excessive expenditures on physical security is consistent with the goal of encouraging investment in trade secret research.[209] In essence, it is the victim's conduct in attempting to protect the secret that matters. Mere subjective intent that information be considered and treated as secret may be relevant, but does not by itself satisfy the "reasonable efforts" standard.[210]

***218** 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 such agreements, particularly with regard to employer/employee contracts. However, as with other tools and methods of enforcing confidentiality, nondisclosure agreements are not subject to "hard and fast" rules. In some cases, evidence of a valid nondisclosure agreement may be sufficient, along with very little else, to support a conclusion of "reasonable efforts".[211] In other cases, the trade secret owner may be able to satisfy the standard of care even though no written agreements were obtained from any employees.[212] As a matter of practice, though, employee nondisclosure agreements are a useful part of any information protection program because they enhance protectability in litigation, and they provide notice to the employees that trade secrets are considered 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 with vendors, contractors, and customers at virtually all levels of the enterprise.

2. A policy for *document protection*, retention, and destruction, including provisions for marking confidential documents.[213]

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."[214]

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

***219** 6. *Education*. Training and awareness are, without a doubt, the most cost-effective aspects of any protection program. The keys to successful training are: (1) continuity, rather than an initial "splash" that is not followed up; and (2) accountability in order to manage the function.

2. Whether To Make A Criminal Referral

a) Advantages

A trade secret owner who discovers (or strongly suspects) a theft must make a threshold choice of whether to seek a civil or ciminal remedy. The most obvious advantage to criminal prosecution over civil prosecution is cost. In the criminal context, the government pays for all the investigation and litigation costs, which the victim would otherwise have to pay investators and lawyers to perform. These costs can run into the tens or hundreds of thousands of dollars, and are a serious impediment

to those seeking remedies through civil proceedings. In addition, criminal cases can reach trial faster, reflecting the requirements of the Speedy Trial Act, as well as constitutional imperatives. Perhaps more importantly, 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 gain a reputation as a vigilant protector of its rights, thereby reducing the chance that others will trifle with those rights, and generally enhancing the value of its intellectual property portfolio.

b) Disadvantages

Criminal prosecution is not always the obvious choice, though. The most significant negative factor is the victim's loss of control over the process, including settlement. The authorities act in the interest of the government and the people they represent, 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 has otherwise compromised the claim.

A second major disadvantage in the case of concurrent proceedings is the impact of the criminal case on any civil proceedings. Because defendants are entitled to invoke the Fifth Amendment's protection against self-incrimination, a civil lawsuit can be effectively stayed as the result of a criminal filing. Recovery of damages will likely be delayed and possibly impaired.

However, victims who are considering criminal referral of a case may still want to consider a simultaneous filing in civil court, with an immediate request for injunctive relief. This will provide valuable protection during the time it takes to sort out procedural conflicts, should they arise. Alternatively, a victim might work ***220** with the prosecuting attorney in seeking a protective injunction through a collateral civil proceeding brought by the government.[215]

3. Federal Versus State Referral

Some states have laws specifically directed at trade secret theft.[216] Moreover, some jurisdictions have committed specific resources to the establishment of special prosecution units with experience in the field of technology crime. However, states are jurisdictionally limited in the crimes they can investigate and prosecute. Furthermore, it is difficult to match the resources of the FBI and the Department of Justice for the investigation and prosecution of most matters.[217] 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. Attorneys' office. Keep in mind, however, that some cases may not be accepted for prosecution by the U.S. Attorney's office, while local district attornies might be willing to take on such cases. 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.[218]

4. How to Make a Referral

We have examined above the general guidelines for assessing cases under the EEA. That information should be considered, along with the following practical tips, when preparing to present a matter to the prosecutor:

• Be realistic; don't oversell the case. The prosecutor will be judging credibility in addition to the legal requirements. A failed case can produce negative consequences, including retaliatory civil litigation by the accused. In general, prosecutors are less concerned about business information than technological and scientific information, so the presentation should reflect this fact.

• Clearly define what was taken. This may be difficult to do, in part because proof of the theft is usually circumstantial, and trade secrets are difficult to describe with particularity. However, it is important that the prosecutor be ***221** informed to the greatest extent possible so that he can determine whether the information is distinguishable from that which is publicly available. Consider offering "inside experts" to explain the technical details in layman's terms.

• 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 accused's conduct threatens the public interest.

• Show how the victim took reasonable steps to protect the misappropriated information.

• Present facts that reflect the intent of the accused: e.g., that the theft was done deliberately; or that the accused knew the information was valuable.

• If a parallel civil case is contemplated, be clear about what must be done in that context, and assure the prosecutor of the victim's commitment to the criminal process and its limitations.

C. The Defense Perspective

The presence of "illegal" data within a business environment is analogous to a viral infection. Undetected and unchecked, the data can become part of a company's product or process. Because the EEA applies to the mere unauthorized possession of information, possibilities for infection are extensive. Opportunities for infection start with each employee, especially new hires who often bring with them personal collections of disks, files, and documents, or those who just know a lot about the competitors where they used to work. This situation is usually innocent, since the information typically stays at home or is used by the employee for format rather than content. However, when pressed to complete a project, some otherwise honest employees 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 other personnel with less tenure and loyalty. Temporary workers, employees "on loan" from other companies, 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 different competitors. Even the most honest and cautious consultant faces a challenge of separating and protecting large amounts of closely related trade information.

In today's massively-wired business network, information flows daily among affiliates, partners, customers, and suppliers all over the world. Using tools like the Internet, organizations have come to depend upon instant access to relevant data. ***222** With so many ports opened to the outside, unauthorized information can easily enter (and exit) 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 to control the process of assuming, tracking, and enforcing confidentiality obligations to 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 a company's training program. Perhaps most importantly, a company must examine its business relationships to determine the procedures and behaviors of those who may create vicarious liability under the EEA.

The central feature of any strategy for avoiding criminal liability is the "compliance plan." Compliance plans are a helpful means of preventing misappropriated 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 the knowing theft of trade secrets. Moreover, under the Federal Sentencing Guidelines, courts applying the EEA must take compliance plans into account in assessing punishments.[219]

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 the implementation of a compliance plan. However, some businesses are more exposed than others, and the following checklist should be considered in determining the relative need for such guidelines.

(1) High Competitive Visibility

A high visibility company in a very competitive market has a greater chance that its competitors will care about perceived

violations than a lower visibility company in a less competitive market. Success in highly competitive markets breeds envy, making one a target for those who view prosecution as a means of levelling the playing field.

(2) 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 ***223** customers lists to resolution in civil courts. The more a company uses valuable technical information, the more likely it is to be involved (either as victim or accused) in trade secret theft litigation.

(3) 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 generally less cautious about who is hired and how well they are screened and trained to avoid incoming data infection.

(4) 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. Companies that rely on these sorts of resources, especially in the sensitive areas of research and development, are especially vulnerable to trade secret theft problems.

(5) Extensive Outsourcing, Joint Ventures, and Other "Collaborative" or "Virtual" Businesses

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 whom should be in possession of particular 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 might not be completely effective.

(6) 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 this history, and the increased penalties that apply to cases involving foreign entities (many of which are under indirect control of foreign governments), compliance plans are especially necessary for businesses with foreign facilities, subsidiaries, affiliates, or venture partners.

*224 b) Objectives of a Compliance Plan

(1) 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.

(2) Prevent Loss

Although a plan's primary objective is to prevent sensitive information from entering a particular facility, a by-product of

such a plan should be the retention of a company's own valuable information. Good compliance plans will generally raise the level of awareness within the organization regarding the importance of intellectual assets. Increased care when handling 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 is an extremely cost-effective way to protect investment in research and other secrets.

(3) Increase Chance of Early Discovery and Reporting

Information loss is inherently difficult to detect, since 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 may have received trade secrets through, for example, a new hire. By creating a program to sensitize the organization as to how data can be compromised, violations are more likely to be spotted sooner. In addition, 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.

(4) Protection Against Exposure to Criminal Liability

Companies do not go to jail, but their officers do, and fines can be substantial. Just the expense, diversion, and embarrassment of defending criminal charges are significant enough to justify measures to prevent involvement in this sort of nightmare. A compliance plan is not a guarantee against indictment, but a good plan properly implemented makes it far more likely that the authorities will view the company sympathetically and decide not to prosecute, or, at the very least, that the authorities will concentrate exclusively on the culpable individuals. The EEA requires a *knowing* theft,[220] and compliance procedures can effectively isolate those who have the requisite knowledge and intent.

***225 (5) 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 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.[221] In effect, the guidelines are a scorecard to measure an organization's culpability. Various criteria such as the value of the property stolen, management knowledge, speed of reporting, and cooperation are all assigned point levels.[222] Bad conduct/circumstances will increase the points, and good conduct will decrease them. The point total then becomes the primary determinant of fines and jail time.[223] The corporate guidelines also stress the importance of implementing "compliance plans." A good compliance plan can reduce points at sentencing, but it can also help to convince the federal prosecutor that the company found to possess trade secrets has in fact been victimized by an errant employee.[224]

(6) 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 are 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 is almost always found. As a result, relationships are preserved, and the expense and diversion of emotional litigation is avoided. In other words, the institutionalization of ethics pays off.

c) Elements of a Compliance Plan

(1) Custom Design

Compliance plans should 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: (1) the size of the company (the larger the

company, the more formal the plan); (2) the risks inherent in the business (e.g., a specialty fabricator would be at higher risk because it handles a lot of customers' secret ***226** information); (3) past history of either security problems or trade secret theft; and (4) any applicable industry or government standards related to information security.[225]

(2) Standard of Conduct

The company must "establish compliance standards and procedures to be followed by its employees and other agents."[226] These standards should be specific because employees and agents cannot be guided effectively by general principles. Wherever there are peculiar risks to the operation or environment of the enterprise, those should be singled out and direction given on how to avoid 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: namely, who should be notified and what sort of investigation should be conducted. Finally, the disciplinary consequences of noncompliance must be spelled out.

(3) 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 involved in defining and enforcing the plan.[227] 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.

(4) 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 (e.g., employees, contractors, consultants, vendors, affiliates, etc.) as an important part of the corporate ethic.[228] This effort focuses initially on the screening and initiation of new employees; however, the effort must be ongoing because of employee turnover and other changing circumstances. Keep in mind that education is inexpensive in relation to the cost and difficulty of solving problems after they occur. To the extent that the plan is meant to ward off potential indictments, it will count for little if it has not been promoted.

*227 (5) Monitoring

There are two basic aspects to monitoring. First, one must address the company's operations, monitoring behavior sufficiently so that violations are likely to be discovered and reported within the organization.[229] Records should be maintained to demonstrate that the company took all reasonable steps (within the 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 needed.[230]

(6) Implementation

In considering the sufficiency of a compliance plan, the authorities will first look to the plan itself; ultimately, however, it is the company's own effort at implementation 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 (at least partially) in terms of such responsibilities.

(7) Discipline

The company's records must show that violations are the subject of appropriate discipline.[231] This includes failures to detect and report offenses, 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 should be determined by the specific facts of the case.[232] 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.

(8) Reporting

Law enforcement depends heavily on self-policing. This means that an effective compliance plan should require individuals to report violations (and suspected violations) to responsible management.[233] It also means that, following an investigation to confirm the existence of a probable violation, company management ***228** should be encouraged not only to notify the owner of the stolen secret, but also to contact the authorities in apporpriate cases.

2. Defense of an EEA Prosecution

a) Importance of Criminal Procedure

Those who have become targets of a criminal investigation must recognize the 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 the need for specialized advice in dealing with the arcana of criminal procedure.

b) Joint Defense and Indemnification Agreements

In cases arising under the EEA there may be several people or entities targeted by the criminal investigation who will ultimately be indicted. These targets can consist of the company, its employees, its affiliates, and its business partners. All of these potential targets share an interest in defending against 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 that preserves the attorney-client privilege and work product protections.[234] In addition, individuals and entities may have rights of indemnity (e.g., 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 appropriately.

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 at 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 probably be less interested in investing prosecutorial resources if the matter has already been resolved to the victim's satisfaction..

Where a company (before being sued) discovers that one of its employees has compromised trade secrets belonging to someone else, the best strategy, following ***229** 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 sometimes avert both civil and criminal procedures.

V. Conclusion

The EEA has raised the stakes in the business of protecting trade secrets. Federal criminal prosecution is a powerful weapon, and one that should not be 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 how it is likely to be applied are critically important, both for victims and potential defendants.

Footnotes

[a1] Principal, Fish & Richardson P.C., Menlo Park, California.

[aa1] Assistant Professor, University of Texas School of Law; of counsel, Fish & Richardson P.C., Austin, Texas.

[aaa1] Attorney, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice.

The opinions expressed in this paper are those of the authors and do not reflect the positions of the Department of Justice, the University of Texas, Fish & Richardson, or its clients.

[1] 142 CONG. REC. H12137-01 (daily ed. Sept. 28, 1996) (statement of Rep. Lofgren).

[2] United States v. Brown, 925 F.2d 1301, 1307-09, 17 U.S.P.Q.2d (BNA) 1929, 1933-34 (10th Cir. 1991).

[3] *See* Douglas Pasternak & Gordon Witkin, *The Lure of the Steal: America's Allies Are Grabbing U.S. Technology, Washington is Worried*, U.S. NEWS & WORLD REP., Mar. 4, 1996.

[4] Pub. L. No. 104-294, §§ 1831-1839, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839).

[5] 18 U.S.C. § 1905 (1994). It provides, *inter alia*, for misdemeanor criminal sanctions for the unauthorized disclosure of government information, including trade secrets, by a government employee. In the only reported decision under this statute, the court in *United States v. Wallington*, 889 F.2d 573 (5th Cir. 1989), upheld the defendant's conviction for running background checks on several people whom a friend of the defendant suspected of drug dealing. However, because this section provides for misdemeanor sanctions, is rarely used for prosecution purposes, and is limited in scope, it is of *de minimis* importance in this area.

[6] 18 U.S.C. §§ 2314, 2315 (1994). *See, e.g.*, United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990) (interstate transfer of an intangible computer text file); United States v. Bottone, 365 F.2d 389 (2d Cir. 1966) (interstate transfer of photographs of secret drug manufacturing processes); United States v. Seagraves, 265 F.2d 876 (3d Cir. 1959) (interstate transfer of geophysical maps); United States v. Greenwald, 479 F.2d 320 (6th Cir. 1973) (interstate transfer of a chemical formula); and United States v. Belmont, 715 F.2d 459, 222 U.S.P.Q. (BNA) 463 (9th Cir. 1983) (interstate sales of videotape cassettes of copyrighted motion pictures that had been copied "off the air"); *but cf.* United States v. Brown, 925 F.2d 1301, 17 U.S.P.Q.2d (BNA) 1929 (10th Cir. 1991) (holding that a computer program does not meet the "goods, wares, or merchandise" language of § 2314) (citing Dowling v. United States, 473 U.S. 207, 226 U.S.P.Q. (BNA) 529 (1985)).

[7] 18 U.S.C. § 1343 (1994). *See, e.g.*, Carpenter v. United States, 484 U.S. 19 (1987) (confidential business information); United States v. Cherif, 943 F.2d 692 (7th Cir. 1991) (confidential banking information); United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978) (stolen computer source code); and United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990) (network configuration information stolen intrastate, but transferred interstate after theft).

[8] 18 U.S.C. § 1341 (1994). *See, e.g.*, United States v. Cherif, 943 F.2d 692 (7th Cir. 1991).

[9] *See* MELVIN F. JAGER, TRADE SECRETS LAW, App.L-1 through App.L-44 (Clark Boardman Callaghan 1996) (state criminal trade secrets statutes collected); *see also* Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921 (1989).

[10] 18 U.S.C.A. § 2314 (1996).

[11] The National Motor Vehicle Theft Act (Dreyer Act), 41 Stat. 324, was enacted in 1919 and covered only stolen "motor vehicles." It is currently codified at 18 U.S.C. § 2312 (1994). "Congress acted to fill an identical enforcement gap when in 1934 it 'exten[ed] the provision of the [Dreyer Act] to other stolen property' by means of the National Stolen Property Act [of 1934]." United States v. Dowling, 473 U.S. 207, 219-20, 226 U.S.P.Q. (BNA) 529, 534 (1985) (citing S. REP. NO. 538, at 1 (1934); H.R. CONF. REP. NO. 1599, at 1, 3 (1934)).

[12] 925 F.2d 1301, 17 U.S.P.Q.2d (BNA) 1929 (10th Cir. 1991).

[13] *Id.* at 1309, 17 U.S.P.Q.2d at 1934 (restricting the interpretation of 18 U.S.C. §§ 2314, 2315).

[14] *Id.* at 1308-09, 17 U.S.P.Q.2d at 1934.

[15] *Id.* at 1303, 17 U.S.P.Q.2d at 1929-30

[16] 473 U.S. 207, 226 U.S.P.Q. (BNA) 529 (1985).

[17] *Brown*, 925 F.2d at 1303, 17 U.S.P.Q.2d at 1930.

[18] *Id.*

[19] *Id.* at 1306-07, 17 U.S.P.Q.2d at 1933 (quoting the district court record).

[20] *Id.* at 1307, 17 U.S.P.Q.2d at 1933.

[21] *Dowling*, at 209, 226 U.S.P.Q. at 530.

[22] *Id.* at 216-18, 226 U.S.P.Q. at 533-34.

[23] *Id.* at 217, 226 U.S.P.Q. at 533.

[24] *Id.* at 216, 226 U.S.P.Q. at 533.

[25] *Brown*, 925 F.2d at 1307, 17 U.S.P.Q.2d at 1933.

[26] *Id.* 1308, 17 U.S.P.Q.2d at 1934.

[27] 739 F. Supp. 414 (N.D. Ill. 1990).

[28] *Brown*, 925 F.2d at 1308, 17 U.S.P.Q.2d at 1934.

[29] *Riggs*, 739 F. Supp. at 416.

[30] *Id.* at 417. Enhanced 911 is a universal service for handling emergency calls in municipalities and surrounding unincorporated areas.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *See* 18 U.S.C. § 1030(a)(6), *Riggs*, 739 F. Supp. at 417-18.

[36] *Id.* at 420.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.* at 421.

[41] *Id.*

[42] *Id.* at 422.

[43] *Id.* at 418.

[44] *Id.* at 421-22

[45] *See Dowling*, 473 U.S. at 227, 226 U.S.P.Q. at 537.

[46] *Brown*, 925 F.2d at 1307-08 n.14 (citing United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988)). Furthermore, in two different cases arising out of the same factual circumstances, the Third Circuit affirmed convictions arising under section 2314, where the defendants were involved in the theft and interstate sale of geophysical maps from Gulf Oil. *See* United States v. Seagraves, 265 F.2d 876 (3d Cir. 1959); United States v. Lester, 282 F.2d 750 (3d Cir. 1960). The defendants argued that in many instances the original maps were not transported; rather, only copies made with the victim's copying equipment and supplies were actually transported via interstate commerce. *Lester*, 282 F.2d at 755. In fact, many of the original maps were never removed from the premises of Gulf Oil. Thus, according to the defendants, no "goods, wares, or merchandise" were stolen by the defendants and transported in interstate commerce. *Id.* at 755. The *Lester* court rejected this argument and focused instead on the value of the

maps, which was almost wholly derived from the intangible information contained therein. *Id.* at 754-55. Similarly, the *Seagraves* court stated that the "[t]he term 'goods, wares, or merchandise' is a general and comprehensive designation of such personal property or chattels as are ordinarily a subject of commerce." *Seagraves*, 265 F.2d at 880 (citing BLACK'S LAW DICTIONARY 823 (4th. ed. 1951)). Since there was evidence that a market for the copies of the maps existed, the maps *and* their copies could be considered "goods, wares, or merchandise" within the meaning of section 2314. *Id.*, at 880. Thus, unlike *Brown*, the defendants in these cases misappropriated both the intangible and tangible components of the plaintiff's trade secret, which happened to be embodied within the same object, namely, the copies of the stolen maps. *See also* Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967) (upholding defendant's state court conviction for theft of computer programs worth $5 million that the defendant copied using his employer's copying machine and paper). *But see* United States v. Bottone, 365 F.2d 389 (2d Cir. 1966) (holding that the interstate transfer of copies of secret drug manufacturing processes violates section 2314.); United States v. Gallo, 599 F. Supp. 241, 245, 226 U.S.P.Q. (BNA) 148, 150 (W.D.N.Y. 1984) ("The law of this circuit is that intangible rights can be the basis of prosecution under 18 U.S.C. § 2314."); United States v. Gilboe, 684 F.2d 235 (2d Cir. 1982) (holding that the electronic transfer of funds fraudulently obtained is a violation of § 2314); United States v. Steerwell Leisure Corp., 598 F. Supp. 171, 174, 224 U.S.P.Q. (BNA) 1059, 1060 (W.D.N.Y. 1984) ("Judge Friendly's opinion for the Second Circuit in *United States v. Bottone* ... stated in no uncertain terms that intangible rights, embodied in tangible objects which are not themselves stolen, can be the basis of a prosecution under 18 U.S.C. § 2314.") (citations omitted); United States v. Sam Goody, Inc., 506 F. Supp. 380, 390-91, 210 U.S.P.Q. (BNA) 318, 326-27 (E.D.N.Y. 1980) (holding that an intangible aggregation of sounds embodied on a tangible medium is a good, ware, or merchandise within the purview of § 2314).

47 18 U.S.C. § 1341 provides in pertinent part:
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises ... for the purpose of executing such scheme or artifice or attempting to do so, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Post Service, ... or takes or receives therefrom any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than five years, or both.
18 U.S.C. § 1343 provides in pertinent part:
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than five years, or both.

48 See, e.g., Abbott v. United States, 239 F.2d 310 (5th Cir. 1956).

49 589 F.2d 152 (4th Cir. 1978).

50 *Id.* at 154.

51 *Id.* at 160.

52 *Id.*

53 *Id.*

54 Those states are: Alabama, Arkansas, California, Colorado, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Missouri, New Hampshire, New Jersey, New Mexico, New York, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, and Wisconsin. *See* JAGER, App.L, *supra* note 9.

55 S. REP. NO. 104-359 at 10-11 (1996).

56 H.R. 3723, 104 Cong. (1996).

[57] Pub. L. No. 104-294, §§ 1831-1839, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831-1839).

[58] H.R. 3723, 104 Cong. (1996).

[59] H.R. REP. NO. 104-788 (1996).

[60] 142 Cong. Rec. H12137-01.

[61] 142 Cong. Rec. S12201-03.

[62] Economic Espionage Act, *supra* note 57.

[63] 18 U.S.C. § 1839(3).

[64] UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A 438 (1996) (hereinafter cited as UTSA). The UTSA has been adopted in 40 states and the District of Columbia. For a complete list of jurisdictions adopting the Act, see RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 statutory note at 437-38 (1995). Some jurisdictions, including California, have modified this definition, however. *See, e.g.*, CAL. CIV. CODE § 3426.1 (West 1997) (deleting the "readily ascertainable" language from the definition of a trade secret).

[65] 18 U.S.C. §§ 1831, 1832.

[66] 18 U.S.C. § 1839(3).

[67] *See Legislation Addressing Trade Secret Theft, Computer Break-ins Passed by Congress*, 1 ELEC. INFO. POL'Y & L. RPT. 599 (Oct. 4, 1996) (hereinafter *Legislation Passed*) (indicating that the change from "proprietary economic information" to "trade secrets" was added only in the final version of the bill, after conference committee).

[68] Section 1(4) of the UTSA provides:
(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
UTSA § 1(4), 14 U.L.A. 438 (1996).

[69] *See Legislation Passed, supra* note 67, at 599 (indicating that the terms "data," "tools," "mechanisms," "compounds," and "commercial strategies" were removed from an earlier version of the Senate bill).

[70] *See, e.g.*, Religious Tech. Center v. Lerma, 908 F. Supp. 1362, 1368-69, 37 U.S.P.Q.2d (BNA) 1258, 1262-63 (E.D. Va. 1995) (religious scriptures); Thermodyne Food Service Prods., Inc. v. McDonald's Corp., 940 F. Supp. 1300, 40 U.S.P.Q.2d (BNA) 1801 (N.D. Ill. 1996) (interrelationship of publicly known elements); Allen v. Johar, Inc., 823 S.W.2d 824, 21 U.S.P.Q.2d (BNA) 1854 (Ark. 1992) (customer lists); ABBA Rubber Co. v. Seaquist, 286 Cal. Rptr. 518 (Cal. Ct. App. 1991) (customer lists); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39, cmt. d (1995).

[71] CAL. PENAL CODE § 499c(9) (West 1988).

[72] *Id.* Revised § 499c(9), which applies to business as well as technical information, took effect Jan. 1, 1997.

[73] For example, one class of "insider trading" cases involves individuals outside the corporate structure (such as printers or runners working for those engaged in corporate control transactions) who take information and trade on it. *See, e.g.*, Carpenter v. United States, 484 U.S. 19, 5 U.S.P.Q.2d (BNA) 1059 (1987); Chiarella v. United States, 445 U.S. 222 (1980); Securities & Exchange Comm'n v. Materia, 745 F.2d 197 (2d Cir. 1984). One might treat these cases as involving secret business information "converted" by the defendants.

[74] Economic Espionage Act § 1839(3).

[75] *See, e.g.*, Allen v. Johar, Inc., 823 S.W.2d 824, 21 U.S.P.Q.2d (BNA) 1854 (Ark. 1992); Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d 209, 35 U.S.P.Q.2d (BNA) 1134 (Ill. Ct. App. 1995). Both of these cases dealt with the punishment of defendants who memorized customer lists. *See also* PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 35 U.S.P.Q.2d (BNA) 1010 (7th Cir. 1995) (precluding a former employee from accepting competing employment even absent proof of trade secrets theft, due to the "inevitable disclosure" of secrets).

[76] *See, e.g.*, 142 CONG. REC. S12212 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl) ("Trade secrets are carefully defined so that the general knowledge and experience that a person gains from working at a job is not covered."); H.R. REP. NO. 104-788 (1996). Indeed, an entire section of the Senate Debate is entitled "General Knowledge Not Covered by Definition of Trade Secrets." 142 CONG. REC. S12212 - S12213.

[77] 18 U.S.C. § 1839(3)(A).

[78] 18 U.S.C. § 1839(4).

[79] Indirect support for this proposition is found in § 1832(a), which speaks of misappropriation that "will injure *any owner* of that trade secret," suggesting that a single secret may have multiple owners under the EEA. 18 U.S.C. § 1832(a) (emphasis added). On the other hand, the same provision also requires that the secret be converted "to the economic benefit of anyone other than *the owner* thereof." *Id.* (emphasis added). Thus the EEA is somewhat inconsistent in its treatment of the ownership issue.

[80] *See, e.g.*, Ferroline Corp. v. General Aniline & Film Corp., 207 F.2d 912, 99 U.S.P.Q. (BNA) 444 (7th Cir. 1953) (holding that the issuance of patent destroys trade secrecy); Religious Tech. Center v. Lerma, 908 F. Supp. 1362, 1368, 37 U.S.P.Q.2d (BNA) 1258, 1263 (E.D. Va. 1995) (holding that the publication on the Internet destroys trade secrecy); Vacco Indus. v. Van den Berg, 6 Cal. Rptr. 2d 602, 611 (Cal. Ct. App. 1992) (holding that the sale of product, which fully discloses the secret, destroys trade secrecy).

[81] *See* Rockwell Graphics Systems, Inc. v. DEV Indus., 925 F.2d 174, 17 U.S.P.Q.2d (BNA) 1780 (7th Cir. 1991); ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 56-59 (1997) (offering justifications for the "reasonable precautions" requirement).

[82] *See, e.g.*, Rockwell Graphic Systems Inc. v. DEV Indus., 925 F.2d 174, 179-80, 17 U.S.P.Q.2d (BNA) 1780, 1784-85 (7th Cir. 1991).

[83] UTSA § 1(4)(I), 14 U.L.A. 438 (1996).

[84] 18 U.S.C. § 1839(3)(B).

[85] *Cf.* James H. Pooley, *The Uniform Trade Secrets Act: California Civil Code* § 3426, 1 SANTA CLARA COMP. & HIGH TECH. L.J. 193, 197 (1985) (discussing the California civil statute, which contains both the "public" and "other persons" language).

[86] *Cf.* Thermodyne Food Serv. Prods. v. McDonald's Corp., 940 F. Supp. 1300, 1304-05, 40 U.S.P.Q.2d (BNA) 1801 (N.D. Ill. 1996) (rejecting claim that newly asserted trade secret unfairly surprised the defendant).

[87] California is one such state. *See* CAL. CODE CIV. PROC. § 2019(d) (West Supp. 1997).

[88] *Thermodyne*, 940 F. Supp. at 1305 (amended complaint); Vacco v. Van den Berg, 6 Cal.Rptr.2d 602, 612 n.16 (1991).

[89] 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (statement of Peter Schweizer) (emphasis added).

[90] 18 U.S.C. §§ 1831(a), 1832(a). These sections also punish attempts and conspiracies to do any of the acts listed above. 18 U.S.C. at §§ 1831(a)(4)-(5), 1832(a)(4)-(5).

[91] By way of contrast, the UTSA defines misappropriation as either "acquisition of a trade secret ... by improper means" or "disclosure or use of a trade secret ... acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use." UTSA at § 1(2)(i),(ii)(B)(II), 14 U.L.A. 438 (1996).

[92] UTSA § 1(2)(I), 14 U.L.A. 438 (1996); *see also* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 166 U.S.P.Q. (BNA) 421 (5th Cir. 1970).

[93] *See Christopher*, 431 F.2d at 1017, 166 U.S.P.Q. at 425 ("We therefore need not proclaim a catalogue of commercial improprieties. Clearly, however, one of its commandments does say 'thou shall not appropriate a trade secret through deviousness under circumstances in which countervailing defenses are not reasonably available."'); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995); RESTATEMENT OF TORTS § 757, cmt. f (1939).

[94] 18 U.S.C. §§ 1831(a)(1), 1832(a)(1).

[95] 142 CONG. REC. S12212 (daily ed. Oct. 2, 1996) (statement of Peter Schweizer) ("Other companies can and must have the ability to determine the elements of a trade secret through their own inventiveness, creativity and hard work. ... [P]arallel development of a trade secret cannot and should not constitute a violation of this statute.").

[96] 18 U.S.C. §§ 1831(a)(2), 1832 (a)(2).

[97] UTSA § 1(2)(ii)(B), 14 U.L.A. 438 (1996)..

[98] *See* H.R. Rep. 104-788 ("The concept of control also includes the mere possession of the information, regardless of the manner by which the non-owner gained possession of the information.").

[99] Legal protection for trade secrets is premised on two theories that are only partly complementary. The first is utilitarian. Under this view, protecting against the theft of proprietary information encourages investments in such information. This is sometimes associated with the view that trade secrets are a form of property. The second theory emphasizes deterrence of wrongful acts, and is therefore sometimes described as a tort theory. Under this theory, the aim of trade secret law is to punish and prevent illicit behavior and to uphold reasonable standards of commercial behavior. *Cf.* KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW (1988) (arguing that cases involving legal secrets--including trade secrets cases--are better explained in terms of universally accepted principles rather than in terms of law and economics). Although under the tort theory, trade secret protection is not explicitly concerned with encouraging investment, it is plain that one

consequence of deterring wrongful behavior would be to encourage investments in trade secrets. Hence, despite their conceptual differences, the tort and property approaches to trade secrets may well push in the same direction.

The Supreme Court adopted the property rights view of trade secrets law in *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1001-04 (1984). In that case, the Court faced the question of whether a federal law that required Monsanto to publicly disclose its trade secrets was a "taking of private property," for which the Fifth Amendment required compensation. The Court found that trade secrets were "property," reasoning in part that "[t]rade secrets have many of the characteristics of more tangible forms of property. A trade secret is assignable. A trade secret can from the *res* of a trust, and it passes to a trustee in bankruptcy." *Id.* at 1002-04. Treatment of trade secrets as property rights vested in the trade secret "owner" is consistent with a view of trade secrets law as providing an additional incentive to innovate, beyond those provided in patent law. The Supreme Court has offered some support for this view in other cases, such as *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481-85, 181 U.S.P.Q. (BNA) 673, 678-80 (1974).

A powerful alternate explanation for much of trade secrets law is what might be described as a "duty-based" theory, or what the Supreme Court has called "the maintenance of standards of commercial ethics." *Id.* at 481, 181 U.S.P.Q. at 678. The Supreme Court first expressed this view in a famous early decision, in which it upheld an order limiting access to trade secret information in litigation:

The word property as applied to trademarks and trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. Whether the plaintiffs have any valuable secret or not the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied but the confidence cannot be. Therefore the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs, or one of them.

E.I. du Pont De Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917).

Closely related to *Masland*'s theory of "breach of confidence" is the contract basis for trade secret law. While not always applicable, many trade secret cases arise out of a "duty" explicitly stated in a contract, such as a technology license or an employment agreement. The tort-based theory of breach of duty merges in those cases with a standard common-law style action for breach of contract.

100 Destroying a secret might mean "destroying its value by publishing it to the world," in which case civil law does provide a remedy. In the alternative, it might mean the physical destruction of valuable information, which is not covered by the UTSA.

101 871 F. Supp. 535, 541-42, 33 U.S.P.Q.2d (BNA) 1978, 1983 (D. Mass. 1994) (holding that the criminal copyright statute did not apply to an electronic bulletin board owner who posted infringing computer software without receiving any financial benefit).

102 Thus, the assumption in certain business circles that the EEA "should make it easier to prosecute hackers," Richard Behar, Amy Kover & Melanie Warner, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 59, may be unwarranted.

103 *See* 142 CONG. REC. S12212 (Oct. 2, 1996) (Manager's Statement).

104 *Cf.*, Mason v. Jack Daniel Distillery, 518 So. 2d 130 (Ala. Civ. App. 1987) (rejecting a claim that the defendant reverse-engineered an alcoholic beverage by tasting it).

105 Sega Enter. Ltd. v. Accolade, Inc., 977 F.2d 1510, 25 U.S.P.Q.2d (BNA) 1561 (9th Cir. 1992). *See, e.g.*, Andrew Johnson-Laird, *Reverse Engineering of Software: Separating Legal Mythology From Actual Technology*, 5 SOFTWARE L.J. 331 (1992) (describing software reverse engineering); Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 COLUM. L. REV. 2308, 2392 n.333 (1994) (indicating that decompilation is difficult and time-consuming). A separate form of software reverse engineering, called "black-box analysis," does not involve the creation of a copy of the computer program. However, for many applications it is significantly less effective than decompilation. *Id.* at 2317-18 n.23.

106 142 CONG. REC. S12212-13 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl) (emphasis added).

107 *Id.* at S12213. *Cf. Mason*, 518 So. 2d at 133.

108 On the legality of reverse engineering in copyright law, *compare* DSC Communications Corp. v. DGI Tech., Inc., 81 F.3d 597, 601, 38 U.S.P.Q.2d (BNA) 1699, 1703 (5th Cir. 1996), *and* Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1539-40 n.18, 38

U.S.P.Q.2d (BNA) 1225, 1229-30 n.18 (11th Cir. 1996), *and* Lotus Dev. Corp. v. Borland Int'l, 49 F.3d 807, 819-22, 34 U.S.P.Q.2d (BNA) 1014, 1024-26 (1st Cir. 1995) (Boudin, J., concurring), *and* Atari Games Corp. v. Nintendo of America, 975 F.2d 832, 843-44, 24 U.S.P.Q.2d (BNA) 1015, 1024 (Fed. Cir. 1992), *and* Sega Enter. Ltd. v. Accolade, 977 F.2d 1510, 1527-28, 24 U.S.P.Q.2d (BNA) 1561, 1574 (9th Cir. 1992), *and* Vault Corp. v. Quaid, 847 F.2d 255, 270, 7 U.S.P.Q.2d (BNA) 1281, 1295 (5th Cir. 1988), *and* Mitel, Inc. v. Iqtel, Inc., 896 F. Supp. 1050, 36 U.S.P.Q.2d (BNA) 1703 (D. Colo. 1995) (all endorsing a right to reverse engineer in some circumstances), *with* Apple Computer v. Franklin Computer, 714 F.2d 1240, 1253, 219 U.S.P.Q. (BNA) 113, 124 (3d Cir. 1983), *and* Digital Communications Assoc. v. Softklone Distrib. Corp., 659 F. Supp. 449, 2 U.S.P.Q.2d (BNA) 1385 (N.D. Ga. 1987) (both cases rejecting the right to reverse engineer). The weight of more recent authority clearly supports a reverse engineering right.

In trade secret law, the right to reverse engineer is even better established. *See, e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 181 U.S.P.Q. (BNA) 673 (1974); Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160, 9 U.S.P.Q. (BNA) 1847, 1856 (1989); Chicago Lock Co. v. Fanberg, 676 F.2d 400, 216 U.S.P.Q. (BNA) 289 (9th Cir. 1982); UTSA § 1, cmt., 14 U.L.A. 438 (1996); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995); RESTATEMENT OF TORTS § 757 cmt. f (1939).

Finally, other intellectual property statutes sometimes include a similar right. *See* Semiconductor Chip Protection Act of 1984, 17 U.S.C. §§ 901-907; Brooktree Corp. v. Advanced Micro Devices, Inc., 977 F.2d 1555, 24 U.S.P.Q.2d (BNA) 1401 (Fed. Cir. 1992).

109 *See supra* note 108 (citing courts); *see also* JONATHAN BAND & MASANOBU KATOH, INTERFACES ON TRIAL (1995); Julie Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs* 68 S. CAL. L. REV. 1091 (1995); Lawrence D. Graham & Richard O. Zerbe Jr., *Economically Efficient Treatment of Computer Software: Reverse Engineering, Protection, and Disclosure*, 22 RUTGERS COMPUTER & TECH. L. J. 61 (1996); Dennis S. Karjala, *Copyright Protection of Computer Documents, Reverse Engineering, and Professor Miller*, 19 U. DAYTON L. REV. 975, 1016-18 (1994); David A. Rice, *Sega and Beyond: A Beacon for Fair Use Analysis ... At Least as Far as It Goes*, 19 U. DAYTON L. REV. 1131, 1168 (1994).

110 Kewanee Oil Corp. v. Bicron Corp., 416 U.S. 470, 489-90, 181 U.S.P.Q. (BNA) 673, 681 (1974) (indicating that the patent and trade secret law can coexist because "trade secret law provides far weaker protection in many respects than the patent law.... [T]rade secret law does not forbid the discovery of the trade secret by fair and honest means, e.g., independent creation and reverse engineering...."); Bonito Boats v. Thunder Craft Boats, 489 U.S. 141, 160, 9 U.S.P.Q.2d (BNA) 1847, 1856 (1989) (rejecting a state statute because it "prohibit[ed] the entire public from engaging in a form of reverse engineering of a product in the public domain. This is clearly one of the rights vested in the federal patent holder, but has never been a part of state protection under the law of unfair competition or trade secrets.").

111 Indeed, it is not entirely clear how courts would resolve such a conflict in purposes between two federal intellectual property statues. *Cf.* Vornado Air Circulation Systems, Inc. v. Duracraft Corp., 58 F.3d 1498, 1500, 35 U.S.P.Q.2d (BNA) 1332, 1333 (10th Cir. 1995) (noting that federal trademark law could not protect a product configuration that was the subject of an expired patent, because of the potential for conflict between the policies behind the two statutes).

112 142 CONG. REC. S12212 (daily ed. Oct. 2, 1996) (Manager's Statement).

113 142 CONG. REC. S12212 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl).

114 Indeed, informal conversations with those involved in the passage of the EEA indicate that it was not the intent of the drafters to make reverse engineering a crime. Relying on this apparent intent, some have taken the position that the Act does not apply to reverse engineering at all, despite its wording. *See, e.g.*, Jonathan Band & William Leschensky, *New U.S. Law Hits at Foreign Theft of Trade Secrets*, IP WORLDWIDE, Jan./Feb. 1997, at 17 ("The definition of trade secret also does not cover reverse engineering.").

115 18 U.S.C. § 1832(a)(3)-(a)(5).

116 18 U.S.C. § 1832(a)(3).

[117] UTSA § 1(2)(ii)(c), 14 U.L.A. 438 (1996).

[118] 18 U.S.C. § 1831(a).

[119] *See* 142 CONG. REC. S12208 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

[120] 18 U.S.C. § 1839(1).

[121] *See* 142 CONG. REC. H12137-01 (daily ed. Sept. 28, 1996) (statement of Rep. McCollum) ("The term 'foreign instrumentality' is defined in the legislation to mean a foreign corporation or company only when a foreign government substantially owns, controls, sponsors, commands, manages, or dominates that corporation or company. Thus, when this is not the case, a foreign corporation or company should not be prosecuted under the section dealing with economic espionage ...."); 142 CONG. REC. S12212 (daily ed. Oct. 2, 1996) (Manager's Statement) ("Enforcement agencies ... should not apply section 1831 to foreign corporations when there is no evidence of foreign government sponsored or coordinated intelligence activity.... Although the term 'substantially' is not specifically defined, it is a relative term that connotes less than total or complete ownership, control, sponsorship, command, management or domination.... [T]he pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.").

[122] 19 U.S.C. § 1337 (1980). Because § 1337 requires only that a domestic industry exist and that a defendant be importing patented goods, it has been used as a weapon not only by domestic companies against foreign ones, but also by foreign companies against domestic ones. For example, recent ITC proceedings between Texas Instruments and Samsung involved *both* sides filing complaints against the other, since both companies had some facilities in the United States and others abroad.

[123] 18 U.S.C. § 1831(a).

[124] 18 U.S.C. § 1832(a).

[125] *See* 142 CONG. REC. H12137-01 (daily ed. Sept. 28, 1996) (statement of Rep. McCollum).

[126] 18 U.S.C. § 1832(a).

[127] *Id.* 1832(a). The Congressional Record suggests at one point that the government need only show "that the accused knew *or had reason to know* that a trade secret had been stolen or appropriated without authorization." 142 CONG. REC. S12212 (daily ed. Oct. 2, 1996) (Manager's Statement) (emphasis added); *see also* 142 CONG. REC. H12137-01 (daily ed. Sept. 28, 1996) (statement of Rep. McCollum) (using the term "knew or should have known"). These statements cannot be reconciled with the language of the statute, which provides that the defendant must "knowingly" misappropriate the trade secret. The inconsistency may result from the late amendment of the bill. In any event, the language of the statute must take precedence over even express statements in the legislative history.

[128] 18 U.S.C. § 1832(a).

[129] *Id.*

[130] *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995); UTSA § 1, 14 U.L.A. 438 (1996); *see also* Rohm & Haas Co. v. Adco Chem. Co., 689 F.2d 424, 215 U.S.P.Q. (BNA) 1081 (3d Cir. 1982) (rejecting the defense that a former employee did not know that the information he took to a competitor qualified as a trade secret).
Once again, the legislative history of the EEA is inconsistent with the statute on this point. *See* 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (citing Spring Steel v. Molloy, 400 Pa. 354, 363 (1960)) ("[A] defense should succeed if it is proven that the

defendant actually believed that the information was not proprietary *after taking reasonable steps to warrant such belief*.") (emphasis added). On the other hand, the Congressional Record also provides that "[f]or a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is in fact proprietary." *Id.* This latter statement is consistent with the use of the word "knowingly" in the EEA, but is inconsistent with the first statement. *Cf.* 142 CONG. REC. H12137-01 (daily ed. Sept. 28, 1996) (statement of Rep. McCollum) (indicating that the revised version of bill "will increase the proof of state of mind required").

131 *See, e.g.*, RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) (requiring that a defendant know or have reason to know of the *secrecy* of an item, but not about potential economic loss).

132 *See, e.g.*, CAL PENAL CODE § 499c. For a general survey of state criminal statutes, *see* Lederman, *supra* note 9, at 921.

133 While the House Report speaks of a desire to protect "innocent innovators," it is not clear that this motivated the inclusion of the knowledge and intent requirements. H.R. REP. NO. 104-788 at 7 (1996). Someone who is truly an "innocent innovator"--that is, a competitor who independently develops a similar idea--is not liable under the EEA because he has not engaged in any of the prohibited acts listed in sections 1831 or 1832. The intent requirement seems instead to protect what might be called "innocent infringers"--those who engage in misappropriation because, for example, they were not aware that the information they took was a secret.

134 18 U.S.C. § 1832(a).

135 Generally speaking, "negative know-how" refers to valuable information about "blind alleys" or other methods that have been determined *not* to achieve the desired result.

136 Because section 1 of the UTSA speaks of information that "derives independent economic value, *actual or potential*," from its secrecy, it seems evident that the information does not have to be used by the trade secret owner to qualify for protection. *See* Pooley, *supra* note 85, at 197 ("The Uniform Act settles the issue of 'negative information' by giving it trade secret status."). By contrast, the Restatement of Torts protects information "used ... in one's business," and arguably does not apply to information that is not directly and affirmatively used by the trade secret owner. *See* RESTATEMENT OF TORTS § 757 (1939).

137 753 F.2d 1244, 225 U.S.P.Q. (BNA) 441 (3d Cir. 1985).

138 *Id.* at 1262, 225 U.S.P.Q. at 452-453. This seemingly odd result was reached because the employees had not disclosed the secret to their employer, and the employer could not therefore be said to be the "owner" of the secret. The EEA would cut even more broadly, though, preventing owners from enforcing rights under the EEA until the secret was not only known, but actually incorporated in a product. 18 U.S.C. § 1832(a).

139 By contrast, there seems to be no easy way to get around the "products" language when applying the EEA to the misappropriation of service-related trade secrets.

140 18 U.S.C. § 1832(a).

141 18 U.S.C. § 1832(b).

142 *See* 18 U.S.C. § 3571(b)(3).

143 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) ("We, therefore, fully expect that courts will take full advantage of the provision in 18 U.S.C. § 3571(d) allowing for fines of up to twice the gain or loss resulting from the theft of trade secrets and that courts will opt for the larger of the fines available under 18 U.S.C. § 3571(d) or the fines provisions of this statute.").

[144] *Id.* At least one court has held that § 3571(d) can be relied upon in setting fines where Congress did not intend to cap the fine at a lower figure. United States v. Pyatt, 725 F. Supp. 885 (E.D. Va. 1989).

[145] 18 U.S.C. § 1831(a).

[146] 18 U.S.C. § 1831(b).

[147] 18 U.S.C. § 1831(a).

[148] 18 U.S.C. § 1834(a)(1).

[149] *Id.*

[150] The EEA explicitly provides that a court "shall order" forfeiture in addition to any other sentence imposed. 18 U.S.C. § 1834(a).

[151] 18 U.S.C. § 1834(a)(2).

[152] *Id.* (providing for forfeiture of instruments "if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.").

[153] 18 U.S.C. § 1834(a).

[154] 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (statement of Sen. Nickles).

[155] *See* 21 U.S.C. § 853 (1994). The exception is found in § 853(d), establishing the presumption that *all* of a defendant's property is attributable to drug proceeds. This "wholesale" approach is not carried over to trade secret defendants, though.

[156] 21 U.S.C. § 853(h).

[157] 18 U.S.C. § 1834.

[158] 21 U.S.C. § 853(n). *See also* 142 CONG. REC. S12213 (daily ed. Oct. 2, 1996) (statement of Sen. Nickles) (suggesting that the government should look favorably on victim requests for restitution from forfeited proceeds).

[159] 18 U.S.C. § 1834(a)(1) (emphasis added).

[160] 18 U.S.C. § 1836(a).

[161] *See infra* Part IV.B.l.

[162] *See infra* notes 164, 165 and accompanying text (discussing the geographic reach of the EEA).

[163] 18 U.S.C. § 1837.

[164] 18 U.S.C. § 1837(2).

[165] 18 U.S.C. § 1837(1).

[166] 18 U.S.C. § 1838 provides that the EEA does not preempt state civil or criminal trade secret statutes. Thus, in some cases, a single act of misappropriation may be subject to the jurisdiction of both state and federal prosecutors, which will require those prosecutors to use care in coordinating their actions.

[167] There are ninety-three United States Attorneys' offices in the United States and they are charged with the primary responsibility of enforcing the federal criminal laws.

[168] The Fifth Amendment to the United States Constitution provides:
No person shall be held to answer for a capital, or otherwise infamous crime, unless on presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of war or public danger.

[169] FED. R. CRIM. P. 6(f).

[170] In routine cases, the grand jury's role is only accusatory, not investigative. Federal investigative agencies in such cases usually gather all the evidence, which the prosecutor then presents to the grand jury for review together with a proposed indictment. The grand jury then decides whether probable cause exists to support the prosecutor's proposed charges. In practice, federal grand juries do not draft their own proposed indictments.

[171] *See* Branzburg v. Hayes, 408 U.S. 665, 688 (1972) (stating that because the grand jury's "task is to inquire into the existence of possible criminal conduct and to return only well-founded indictments, its investigative powers are necessarily broad.") *See also* United States v. Dionisio, 410 U.S. 1, 15 (1973).

[172] FED. R. CRIM. P. 6(e) provides, in part:
A grand juror, an interpreter, a stenographer, an operator of a recording device, a typist who transcribes recorded testimony, an attorney for the government, or any person to whom disclosure is made under paragraph 3(A)(ii) of this subdivision shall not disclose matters occurring before the grand jury, except as otherwise provided for in these rules.
Grand jury secrecy serves several distinct interests, primarily: (1) to encourage witnesses to come forward and testify freely and honestly; (2) to minimize the risks that prospective defendants will flee or use corrupt means to thwart investigations; (3) to safeguard the grand jurors themselves and the proceedings from extraneous pressures and influences; and (4) to protect accused persons who are ultimately exonerated from unfavorable publicity. See Douglas Oil Co. v. Petrol Stops Northwest, 441 U.S. 211, 219 (1979); United States v. Proctor & Gamble Co., 356 U.S. 677, 681-82, n.6 (1958); Executive Sec. Corp. v. Doe, 702 F.2d 406, 409 (2d Cir. 1983); United States v. Rose, 215 F.2d 617, 628-29 (3d Cir. 1954); United States v. Fishbach and Moore, Inc., 776 F.2d 839, 843 (9th Cir. 1985); United States v. Eisenberg, 711 F.2d 959, 961 (11th Cir. 1983).

[173] FED. R. CRIM. P. 6(e) does not cover all information developed during the course of a grand jury investigation, but only information that would reveal the strategy or direction of the investigation, the nature of the evidence produced before the grand jury, the views expressed by members of the grand jury, or anything else that actually occurred before the grand jury. Thus, Rule 6(e) does not apply to material obtained or created independently of the grand jury as long as the disclosure of such material does not reveal what transpired before or at the direction of the grand jury. Rule 6(e) also does not apply to information that, under certain circumstances, has become a matter of public record.
U.S. Department of Justice, Criminal Division, Federal Grand Jury Practice 157 (1993).

[174] FED. R. CRIM. P. 16(a).

[175] FED. R. CRIM. P. 16(c).

[176] *See generally* Brady v. Maryland, 373 U.S. 83 (1963).

[177] This requirement is set forth in 18 U.S.C. § 3500(b):
After a witness called by the United States has testified on direct examination, the court shall, on motion of the defendant, order the United States to produce any statement (as hereinafter defined) of the witness in the possession of the United States which relates to the subject as to which the witness has testified.
In many districts, the government is required to provide to the defense copies of witness statements prior to the beginning of trial to give the defense adequate time to prepare for cross-examination.

[178] 18 U.S.C. § 1835. This section also provides a right of immediate appeal to preserve the secret.

[179] Federal courts have inherent powers to prevent abuse with respect to discovery and to grant injunctions. *See e.g.*, United States v. Criden, 648 F.2d 814 (3d Cir. 1981). Non-disclosure orders can be obtained in a criminal trade secret case. *See e.g.*, United States v. Riggs, 739 F.Supp. 414 (N.D.Ill. 1990).

[180] *See* Kenneth Rosenblatt, *Criminal Law and the Information Age: Protecting Trade Secrets from Disclosure in Criminal Cases*, 8 NO. 1 COMPUTER LAWYER 15, January 1991.

[181] Richmond News Papers, Inc. v. Virginia, 448 U.S. 555, 599-600 (1980) (Stewart, J. concurring); *see also* Gannett v. Depasquale, 443 U.S. 368, 422-23 (1979) (Marshall, J., concurring in part and dissenting in part) (tracing the history of the right to a public trial and citing cases where that right has been limited); State *ex rel.* LaCrosse Tribune v. Circuit Court, 340 N.W.2d 460, 466-67 (Wis. 1983) (citing State *ex rel.* Ampco Metal, Inc. v O'Neil, 78 N.W. 2d 921 (Wis. 1956)) (discussing inherent power of a court to limit the public nature of trials).

[182] 506 F.2d 532, 183 U.S.P.Q. (BNA) 321 (2nd Cir. 1974).

[183] *Id.* at 540, 183 U.S.P.Q. at 326.

[184] This requirement is not contained in the text of the Act, but is based on Attorney General Janet Reno's assurance to Congress contained in a letter sent prior to the Act's passage. The letter provides:
The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510
Dear Chairman Hatch:
Thank you for your support of the Economic Espionage Act of 1996 ("Act"). The need for this law cannot be understated as it will close significant gaps in federal laws, thereby protecting proprietary economic information and the health and competitiveness of the American economy.
The Department shares your concerns that the legislation be implemented in accordance with the intent of Congress and therefore will require, for a period of five years after implementation to the Act, that the United States may not file a charge under Chapter 90, or use a violation of Chapter 90 as a predicate offense under any other law, without the personal approval of the Attorney General for the Criminal Division (or the Acting Official in each of these positions if a position is filled by an Acting official). This requirement will be implemented by published regulation.
Violations of such regulations will be appropriately sanctionable. Any such violations will be reported by the Attorney General to the Senate and House Judiciary Committees.
Once again, thank you for your leadership in this critical area.

Sincerely,
Janet Reno

[185] For a detailed discussion of what activities constitute "reasonable measures" regarding the protection of a trade secret, see Kenneth S. Rosenblatt, High-Technology Crime, Investigating Cases Involving Computers 192-99 (1995).

[186] 18 U.S.C. § 1839(3)(B).

[187] 18 U.S.C. § 1839(3).

[188] *Id.* §§ 1831(a)(2), 1832(a)(2) (including one who "copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret....").

[189] *Id.* Although not explicitly stated in the EEA, this fact can be implied from the absence of a "deprivation of use" requirement in the statute.

[190] Illinois v. Gates, 462 U.S. 213, 238 (1983).

[191] A computer audit file contains a list of commands (keystrokes) that a user issues during a particular session while logged onto a computer.

[192] Pub. L. No. 90-351, 82 Stat. 212, June 19, 1968 and Pub. L. No. 100-690, 102 Stat. 4405, Nov. 18, 1988 as amended in 18 U.S.C. §§ 2510-2711. The Electronic Communications Privacy Act protects, *inter alia*, stored electronic communications and sets forth when and how the contents of such stored communications can be disclosed to law enforcement. 18 U.S.C. §§ 2701-2711. It also protects "real-time" wire and electronic communications. 18 U.S.C. §§ 2510-2522. The details of the Electronic Communications Privacy Act are beyond the scope of this article. *See generally* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994).

[193] 18 U.S.C. § 1839(3)(b) (stating that the information need only have some "independant economic value, actual or potential....").

[194] In cases with a smaller loss, not only is criminal prosecution under the EEA unlikely, but civil litigation may also be cost-preclusive.

[195] 365 F.2d 389 (2d Cir. 1966).

[196] *Id.* at 393 (refusing to overturn a fraud conviction due to a $5,000 minimum requirement when European drug manufacturers were willing to pay "six figures" for the fraudulently obtained papers).

[197] 479 F.2d 320 (6th Cir. 1973).

[198] *Id.* at 322.

[199] *See supra* Part I.E.

[200] *See, e.g.*, Walter v. United States, 447 U.S. 649 (1980).

[201] *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

[202] *See, e.g.*, United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994); United States v. Leffall, 82 F.3d 343 (10th Cir. 1996); United States v. Parker, 32 F.3d 395 (8th Cir. 1994).

[203] 18 U.S.C. §1839(3)(a).

[204] *See In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 884, 230 U.S.P.Q. (BNA) 94, 101 (7th Cir. 1986) (stating that "[i]n essence, this requires an assessment of the size and nature of [the plaintiff's] business, the cost to it of additional measures, and the degree to which such measures would decrease the risk of disclosure. What may be reasonable measures in one context may not necessarily be so in another."). *See also* 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.04, p. 1-132 (1996):
As a practical matter the care exercised tends to correspond to the economic value of the secret and its nature, some secrets being more readily protected with minimal effort than others with extensive care. Thus, failure to employ the fullest range of protective techniques will not terminate the secrecy provided that the techniques employed were, in and of themselves, reasonably prudent."
See also RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43, cmt. c (1995).

[205] *See, e.g.*, Syntex Ophthalmics, Inc v. Novicky, 214 U.S.P.Q. (BNA) 272, 277 (N.D. Ill 1982), *aff'd sub nom.* Syntex Ophthalmics, Inc. v. Tsuetaki, 701 F.2d 677, 219 U.S.P.Q. (BNA) 962 (7th Cir. 1983) (holding that "[a]lthough it may be true that Syntex did not always adhere to certain recommended precautions for confidentiality, such as stamping sensitive documents "confidential," and such documents were occasionally left unlocked within the Research and Development area, the court believes that, on the whole, Syntex took extensive precautions to protect the integrity of its secrets.").

[206] *See e.g.*, 142 Cong. Rec. S12213 (explaining that "[t]he definition of a trade secret includes the provision that an owner have taken reasonable measures under the circumstances to keep the information confidential.").

[207] 431 F.2d 1012, 1016, 166 U.S.P.Q. (BNA) 421, 424 (5th Cir. 1970), (declaring that "[p]erhaps ordinary fences and roofs must be built to shut out incursive eyes, but we need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available.... To require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy's trick.").

[208] *Id.* at 1013, 166 U.S.P.Q. at 422.

[209] *See, e.g.*, Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174, 180, 17 U.S.P.Q.2d (BNA) 1780, 1785 (7th Cir. 1991); *accord* MERGES ET AL., *supra* note 81 at 57-59.

[210] Arco Indus. Corp. v. Chemcast Corp., 633 F.2d 435, 443, 208 U.S.P.Q. (BNA) 190, 197 (6th Cir. 1980).

[211] *See, e.g.*, Surgidev Corp. v. Eye Tech., Inc., 828 F.2d 452, 455, 4 U.S.P.Q.2d (BNA) 1090, 1093-94 (8th Cir. 1987).

[212] *See, e.g., In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 884-85, 230 U.S.P.Q. (BNA) 94, 100-01 (7th Cir. 1986).

[213] The policy must not be too detailed to follow in practice. For example, using five tiers of relative confidentiality to designate documents and establishing intricate document security measures may look good on paper; however, if employees find this too burdensome and the program is honored in the breach, the program will have failed in its intended purpose.

[214] "Social engineering" refers to the practice of illegally obtaining computer passwords through social skills. For example, a computer hacker who has learned the name of the system administrator of a company's computer network (perhaps by going

through the company's trash at night), might call an employee and say that he needs the employee's password to run a test. Unwitting employees often divulege their passwords in such situations. The weakest link in any computer system is almost always the human one.

215 *See* 18 U.S.C. § 1837.

216 *See supra* note 54 (listing states).

217 In a recent California case, an entire county office of the district attorney was recused from prosecution of a trade secret theft case for having accepted funds from the alleged victim in order to defray the government's cost of investigation. People v. Eubanks, 14 Cal. 4th 580, 598 (Cal. 1996). The court held that this activity compromised the independence of the prosecutor, and rejected the argument that such private financial assistance was "a political necessity created by inadequate tax revenues." *Id.* at 597.

218 *See supra* note 184 (letter from Janet Reno).

219 *See infra* note 223 and accompanying text.

220 18 U.S.C. § 1832(a).

221 18 U.S.C.A. § 8A1.1 (1996).

222 18 U.S.C.A. § 8C2.5.

223 As of this writing, no offense levels have been set by the Federal Sentencing Commission with respect to the EEA. Until that happens, it is likely that the chapter on fraud (Chapter 2) will apply.

224 18 U.S.C.A. § 8C2.5(f).

225 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(i)-(iii).

226 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(1).

227 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(2).

228 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(4). This comment suggests that requiring participation in training programs and disseminating publications are effective ways of communicating a compliance plan to the organization.

229 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(5).

230 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(5).

231 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(6).

[232] *Id.*

[233] 18 U.S.C.A. § 8A1.2, comment (n.3)(k)(5).

[234] It is important to ascertain whether if there is a substantial risk of one defendant "turning" on another.