The Economic Espionage Act of 1996

Dennis J. Kelly, Esq.
Paul R. Mastrocola, Esq.

I. INTRODUCTION

Your company makes a product that has cornered a large segment of the retail market for products of the same genre. The company's unique process and product formula and specifications comprise trade secrets at common law, and the company assiduously maintains their secrecy. The company also zealously guards the confidentiality of its customer lists. Because the trade secrets give the company a competitive edge, they become the fish that competitors cast for, mostly by legal means, but sometimes by illegal means. And where there are fishers, there are likely to be innovators making better lures to help the trade secret fishers land the big one.

In November 1996, a self-appointed innovator who happened to be a supervisor at Pittsburgh Plate Glass ("PPG") marketed such a lure to the CEO of Corning Glass, PPG's major competitor. For the appropriate price, the supervisor surreptitiously offered to sell PPG trade secrets such as product formulas and specifications and customer lists to Corning. The CEO decided he would do his fishing by other means and promptly tipped off his counterpart at PPG, who notified the FBI, which promptly conducted an undercover sting operation netting the PPG supervisor and his brother -- fish of a different kettle, so to speak. Both perpetrators were prosecuted and convicted of federal crimes. The PPG supervisor was sentenced to fifteen months incarceration, followed by three years probation, and his brother was given home confinement, community service, and five years probation.

The crime charged was violation of the federal Economic Espionage Act of 1996 (the "EEA"), found at 18 United States Code §§1831-1839 (effective October 11, 1996). The PPG case became the very first prosecution under the EEA. The total number of EEA cases brought to date is estimated to number only in the twenties. Of the nineteen EEA cases for which information is available, thirteen cases resulted in guilty pleas or convictions after trial, five cases are pending, and one case was dismissed. Most EEA defendants have been individuals, although a few corporations have also been named as defendants. While the floodgates were expected

to open with enactment of this broad purpose statute, the anticipated deluge of cases has not occurred, at least to date.

Inevitably, this state of affairs will change. Floods often begin as a trickle. The EEA will more often become the government's choice as an enforcement tool in trade secret theft, and the pace of the EEA prosecutions will eventually increase. In the past, cases like the PPG conspiracy more commonly would play out as private disputes handled in civil actions between the parties. Now with the passage of the EEA, federal prosecutors may bring direct charges of criminal trade secret theft for the first time under a statute specially designed and enacted to punish and deter the commission of this precise crime. Either the Internal Security Section or the Computer Crime and Intellectual Property Section of the Criminal Division, Department of Justice must approve and supervise prosecutions under the EEA by any U.S. Attorney's Office in the United States.[1] The Federal Bureau of Investigation has jurisdiction to investigate EEA crimes and has assigned such investigations to its espionage squads in field offices across the country.[2]

The EEA 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 in the wake of the cold war. Prior to the EEA, prosecutors had limited tools to prosecute thefts of trade secrets and there were state statutes in only a few states and a weak assortment of federal statutes less than apt for the prosecution of trade secret theft, *i.e.*, wire and mail fraud statutes (18 U.S.C. §§1341 and 1343) and the Interstate Transportation of Stolen Property Act (18 U.S.C. §2314). The EEA creates a single comprehensive federal scheme enabling federal law enforcement to target its vast resources specifically against thefts of proprietary information by foreign governments and unscrupulous business competitors.

II. THE ACT

The EEA declares it a federal crime to obtain trade secrets wrongfully if done either (1) with the intention or knowledge that the offense would benefit a foreign government, foreign instrumentality, or foreign agent,[3] or

---

1. 28 CFR §0.64-5 (1999).

2. The resources committed to investigation of an EEA case of trade secret theft can be quite substantial. An investigation often involves securing multiple search warrants, detailed review of large volumes of documents, and many witness interviews, all complicated by layers of corporate beaurocracy.

3. 18 U.S.C. §1831.

(2) with the intention to injure the lawful owner of the trade secret for the economic benefit of another.[4] Benefit to a foreign government need not be economic; it can be strategic or reputational.[5] The proscribed illicit means used to obtain the trade secrets, as expressed in the statute, all involve either stealing some form of appropriation without authorization, or fraud, artifice, or deception. The government must prove some such aspect as an essential element of the offense. "Trade secret" is defined to include "all forms or types of financial, business, scientific, technical, economic, or engineering information."[6] For information to be considered a trade secret under the EEA, the statute requires that the owner of the trade secret has taken reasonable measures to keep the material secret. It also requires that the information derive independent economic value from not being generally known to, and not being readily ascertainable through proper means, by the public.[7] This new criminal statute covers conduct occurring within the United States, as well as conduct occurring entirely outside the United States if it is perpetrated by a U.S. citizen or resident alien or by an "organization" organized under the laws of the United States or any of its states.[8]

Violations under both the foreign governmental sponsored and the general industrial espionage sections of the EEA are treated as serious crimes. In the former cases, the statute prescribes maximum statutory penalties of fifteen years imprisonment or a $500,000 fine, or both, for an individual and a $10 million fine for an organization. In the latter cases not involving conduct designed to benefit a foreign government, the EEA provides for a term of up to ten years in prison and $250,000 in fines for individuals, or both, and fines of up to $5 million for corporations or other organizational defendants. As with most federal crimes resulting in pecuniary gain to the perpetrator or loss to the victim, the court is empowered to impose an alternative fine under 18 U.S.C. §3571(d). Thus, the fine can be set at the greater of twice the value of the loss to the trade secret owner or twice the gain to the infringer. The legislative history of the EEA indicates that such alternative fines should be imposed in cases of significant injury.[9] For ex-

---

4. 18 U.S.C. §1832.

5. No prosecutions have yet been filed under the "foreign state sponsorship" section of the EEA, although foreign corporations have been named as defendants in two cases under the "industrial espionage" section.

6. 18 U.S.C. §1839(3).

7. 18 U.S.C. §1839(3)(B).

8. 18 U.S.C. §1837.

9. Pooley, et al., "Understanding the Economic Espionage Act of 1996," TEX. INTELL. PROP. L.J., Vol. 5, No. 2, 177, 201 (1997).

ample, the legislature recognized that organizations could be fined more than $5 million in cases where the loss suffered by the trade secret owner was particularly high. Under the EEA the court also can order forfeiture of the proceeds of the crime, as well as the property used to commit the offense.[10] Furthermore, the Government may seek injunctive relief against activity that violates the EEA.[11]

Potential criminal penalties for EEA violations are certainly substantial, but sentences for EEA crimes are not in the same stratosphere as sentences for classic espionage offenses, despite the invocation of the term "Espionage" in the title of the EEA. Rather, EEA cases are sentenced as cases involving the theft of property. The Federal Sentencing Guidelines (hereinafter the "Guidelines") use a point system, based on designated factors or characteristics of the crime committed, to determine through use of a conversion matrix the sentence that should be imposed. Pursuant to the Guidelines, espionage and related offenses are sentenced extremely harshly. The base offense level under the Guidelines for espionage cases is 37 (assuming the case does not involve top secret information).[12] Thus, even if the individual espionage defendant had no prior criminal history, the sentence of imprisonment he risked would be in the range of 210 to 262 months. In EEA cases, however, the applicable area of the Guidelines is the "Larceny, Embezzlement, and other Forms of Theft" section.[13] The base offense level under the theft section is 4 and the level is increased according to the dollar amount of the loss from the theft. This guideline results in sentences dramatically lower than in traditional espionage cases. Indeed, even assuming a loss value of more than $80,000,000, which is the highest loss category specified in the theft guideline, the total offense level would only be 24, as compared to the minimum espionage offense level of 37.[14] Thus, the sentencing guidelines for economic espionage carry a

---

10. 18 U.S.C. §1834.

11. 18 U.S.C. §1836.

12. U.S. SENTENCING GUIDELINES MANUAL §2M3.1.

13. U.S. SENTENCING GUIDELINES MANUAL §2B1.1.

14. If the circumstances of a case involve the export or attempted export of trade secrets, and if the trade secret were deemed military information pursuant to the Arms Export Control Act, 22 U. S.C. §2778, or dual (civil/military) technology pursuant to the International Emergency Economic Powers Act (the "IEEPA"), 50 U.S. §1701 et seq., then the government probably would indict under these statutes because the defendant would be subject to the much more onerous sentences set forth in the espionage section of the Guidelines. When the Export Administration Act, 50 U.S.C. §2410, which was specifically enacted in 1969 to control export of dual use technology, lapsed on August 20, 1994, the Export Administration Regulations promulgated

maximum range of 51 to 63 months imprisonment for individual defendants with no prior criminal history, while the guideline for traditional espionage begins with a floor of 210 months imprisonment.

In practice, sentences for EEA defendants have ranged from a low of probation to a high of seventy-seven months imprisonment. Thus, EEA sentences can involve significant prison time, but generally do not approach the prison terms imposed upon defendants convicted of "traditional" espionage.

In cases where the convicted defendant is an organization, such as a corporation, a separate section of the Guidelines, USSG §8, applies. The organizational sentencing section of the Guidelines generally dictates sentences of fines, restitution, and probation.[15] The organizational sentencing section incorporates the same offense levels, representing the seriousness of the crime, for the same conduct as that for individual defendants. The fine assessed against the organization is determined by the offense level, which is dependent on the dollar amount of the loss from the theft, as previously discussed. Organizational fines begin at a low of $5,000 for offense level 6 or less, which encompasses for thefts of $2,000 or less in value.[16] Assuming once again a loss value in the highest specified offense category of more than $80,000,000, and a corresponding offense level of 24, an organization would receive a fine of $2,100,000.[17] By comparison, the minimum fine for an organization for an offense level of 37, if an EEA case were sentenced instead under the espionage section of the Guidelines, would be a staggering $57,500,000.[18]

In addition to payment of the fine, the government would be sure to seek an order of restitution against an organization in the amount of the loss, as it would for an individual defendant. The determination of restitution, however, can be fraught with difficulties. The calculation of a restitution amount inherently presents the problem of quantifying the lost market share of the victim company resulting from a trade secret theft and extrapolating lost profit from reduced market share. The economic complexities of the issue may render the restitution element speculative, and the court is unlikely to issue an order for restitution that cannot be proved.

At first glance, the breadth of the statute makes it conceivable that the criminal provisions of the EEA could easily be implicated whenever a key

---

by the Department of Commerce thereunder were extended by Executive Order 12924 and are now applied under the authority of IEEPA.

15. U.S. SENTENCING GUIDELINES MANUAL §8A1.1 et seq.

16. U.S. SENTENCING GUIDELINES MANUAL §§8C2.4(d); 2B1.1.

17. U.S. SENTENCING GUIDELINES MANUAL §§2B1.1; 8C2.4(d).

18. U.S. SENTENCING GUIDELINES MANUAL §§2M3.1; 8C2.4(d).

employee moves to another company. The term "trade secrets" includes tangible or intangible information, "whether or how stored, compiled or memorialized physically, electronically, graphically, photographically or in writing."[19] Such language would suggest that not only theft of information stored in electronic form but also information "stored" only in an individual's memory can be the basis for prosecution under the statute.[20] In the EEA's legislative history, however, Congress attempts to make it clear that the statute is not designed to prosecute innovators or corporate employees who seek to take advantage of the skills and knowledge they have developed working for a company that has trade secrets.

> The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed. It is the intent of Congress, however, to make criminal the act of employees who leave their employment and use their knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer.[21]

While these words are clear in their distinction, the line in practice could become quite blurred. Thus, companies seeking to hire persons who were exposed to proprietary information encompassed in the broad EEA definition of trade secrets must be keenly aware of the risks of prosecution and criminal forfeiture if the trade secrets are used to benefit the new employer. Principles of vicarious liability essentially preclude a corporation's defense that it was unaware of its new employee's criminal conduct. Under federal law, corporations generally are criminally liable for the wrongful acts of their employees or agents.

Merely stealing a trade secret though is not enough for a conviction under the EEA. For sure, the defendant must "knowingly" commit one of the acts of misappropriation enumerated in the statute. In addition he, she, or it must steal with the intent to benefit a foreign government, instrumentality or agent or "with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof."[22] With one exception, this intent requirement appears to preclude prosecution of persons acting out of spite or for some other noncommercial purpose. The exception relates to foreign governmental espionage where the EEA permits prosecution of

---

19. 18 U.S.C. §1839(3).

20. Pooley, *supra*, n. 2 at 189.

21. H.R. Rep. No. 104-788 at p. 4026. *reprinted in* 1971 U.S.C.C.A.N. 1017, 1020.

22. 18 U.S.C. §1832.

one who steals trade secrets knowing but not intending that the offense will benefit a foreign government or agent. Further, under the general industrial espionage section,[23] the EEA requires that the defendant intend or know that the offense would injure the owner of the trade secret. In contrast to the EEA, there is no requirement in civil trade secrets law that an infringer be aware of the trade secrecy of the information, or intend or know of the potential economic loss to the trade secret owner. Therefore, the knowledge and intent provisions of the EEA, in practice, should greatly limit application of the EEA statute in "doubtful cases," *i.e.*, those where the defendant transfers information seemingly without knowledge that his actions are wrong. Consistent with general federal criminal law, it is unlikely, however, that the courts will interpret the EEA to require knowledge by the defendant that he or she was violating a specific federal statute.

In the legislative history, Congress attempted to make clear that "parallel development" and "reverse engineering" are not EEA crimes.

> It is important to note that a person who develops a trade secret is not given an absolute monopoly on the information or data that comprises a trade secret. . . . Other companies can and must have the ability to determine the elements of a trade secret through their own inventiveness, creativity, and hard work. . . . 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. For example, if a person can drink Coca-Cola and, because he happens to have highly refined taste buds, can figure out what the formula is, then this legislation cannot be used against him. Likewise, if a person can look at a product and, by using their own general skills and expertise, dissect the necessary attributes of the product, then that person should be free from any threat of prosecution.[24]

The reality, however, is that while reverse engineering is not expressly prohibited under the EEA, neither is it expressly permitted. Furthermore, a literal application of the statute could encompass many traditional acts of reverse engineering. Under the EEA, a person who without authorization of the owner "copies," "downloads," or "replicates" a trade secret can be prosecuted under EEA if the intent and knowledge elements of the offense can be proved. Reverse engineering of computer software by decompila-

---

23. *Id.*

24. Joint Statement of Senators Spector and Kohl, October 2, 1996, Congressional Record at S.12212-13.

tion almost always involves making a prohibited "copy" of the program.[25]

One commentary goes so far as to contend that reverse engineering of mechanical devices and computer hardware "may well involve prohibited 'sketching, drawing, or photocopying' of the trade secret contained in the publicly sold device" and thus would violate the EEA.[26] Although theoretically possible under the statute, absent a licensing or confidential relationship between buyer and seller, such a result would criminalize behavior generally permitted under civil trade secret law.

A federal prosecutor ordinarily would not be inclined to prosecute such a case, both on policy grounds and because of the lack of jury appeal in such a case. Moreover, two features of the EEA itself would seem to limit prosecutions based on reverse engineering of products obtained in the public market: (1) the requirement that the information be stolen or taken without authorization, and (2) the definitional requirement that the owner of a trade secret take reasonable measures to keep the subject information secret. If trade secret information of products sold in the open market can be revealed by reverse engineering, the owner might be deemed not to have taken reasonable measures to keep the information secret. In any event, clarification of this murky area of the statute will have to await legislative amendment or the evolution of more prosecutions under the statute and the rendering of judicial opinions interpreting its meaning and scope.

III. U.S. V. HSU

One of the few reported EEA cases is United States v. Kai-Lo Hsu.[27] The Hsu prosecution arose out of a two-year "sting" operation in which an undercover FBI agent offered to sell to the defendants the formulae and processes for the manufacture of an anti-cancer drug, Taxol, produced by Bristol-Myers Squibb Company (Bristol-Myers). Information relating to the production of Taxol was regarded by Bristol Myers as a highly valuable trade secret. Specifically, the defendants were charged under the EEA with the inchoate offenses of attempted theft of and conspiracy to steal trade secrets relating to the drug. In discovery, the Hsu defendants sought the production of information and documents relevant to the existence of the trade secret. The defendants claimed to need the documents to establish the defense of legal impossibility, arguing that they could not be convicted of attempting to steal trade secrets if the documents did not actually con-

25. Pooley, *supra* n. 2, at 195.

26. *Id.*

27. 155 F. 3d 189 (3rd Cir. 1998).

tain trade secrets.[28] The government opposed disclosure on the basis that the defendants had no need for documents containing proof of the actual trade secrets, because they had been charged only with attempt and conspiracy to steal trade secrets, rather than with the actual theft of trade secrets. Undoubtedly, the government was loath to disclose highly confidential and valuable trade secret information to the very defendants who were alleged to have attempted to steal it.

Ultimately, the Third Circuit Court of Appeals held that the defendants could not assert the legal defense of impossibility because the possibility of achieving the goal of the attempt or conspiracy was irrelevant to the offense.[29] In the case of inchoate crimes, the government does not have to prove that the information the defendants sought was an actual trade secret. The government can satisfy its burden by proving beyond a reasonable doubt simply that the defendants sought to acquire information that he, she, or it believed to be a trade secret, regardless of whether it qualified as a trade secret pursuant to the EEA.[30]

It may not be comforting to know that one can be convicted of an economic espionage crime, *i.e.*, conspiracy or an attempt, when the information targeted is not in fact a trade secret. The Hsu case, however, merely reflects the general application of the doctrine that proof of inchoate crimes does not require proof that the attempt or conspiracy could actually succeed. On the other hand, the Court of Appeals in Hsu clearly intimated that, if the crime charged is actual theft of a trade secret, the government and the victim company likely would be compelled to disclose information relating to the trade secret because the absence of a trade secret precludes conviction for the substantive offense of economic espionage and the defendant must be alerted and given the opportunity to argue it.

The requirement to prove the trade secret element in EEA cases raises the specter of "graymail," which occurs when defendants seek the production of sensitive information and then threaten to disclose the information publicly in an attempt to force the government to dismiss the charges because it does not want to risk disclosure. "Graymail" defenses usually occur in cases involving national security and classified information. The Classified Information Procedures Act[31] (CIPA) established the procedures for disclosure of classified information in federal prosecutions. The CIPA, however, usually applies in cases of traditional espionage involving military secrets and national security. In EEA cases, the "graymail" dilemma is

---

28. *See Id.* at 193.

29. *See Id.* at 203.

30. *See Id.* at 203 *(emphasis added)*; 18 U.S.C. §1832.

31. 18 USC App. 3 §16; P.L. 96-456, Oct. 15, 1980, 94 Stat. 2025 (18 App. 3).

not limited to the foreign state sponsorship section, but also can arise in industrial espionage cases. In fact, in the Hsu prosecution, the government tried to attribute the "graymail" motive to the defense, contending that the defendants' attempt to gain disclosure of the trade secret information was a ruse to force the Government to elect to drop the prosecution.[32] In any event, the requirement to prove the existence of a trade secret under the EEA and the attendant possibility of "graymail" raises a serious issue concerning the feasibility and efficacy of EEA prosecutions. If a victim company ultimately is going to be forced to disclose its trade secrets, it may be disinclined to refer a trade secret theft to the government or to cooperate with the prosecution if the government initiates an EEA case by means of other sources. Of course, restrictions imposed by the court on the use and disclosure of the trade secret information by the defendants may mitigate this problem somewhat, but certainly not to the extent a defendant actually goes to trial. Whether the required disclosure of the trade secret information in prosecutions of choate offenses sounds the death knell for such EEA prosecutions must await further experience with the EEA.

IV. COMPANY CONSIDERATIONS AND PROTECTION

The EEA provides a new tool to any company damaged by theft of its trade secret. The company cannot use this tool at will, however. Federal law enforcement authorities control its use and management, based on general federal prosecutorial standards and cost/benefit analyses in each case. The obvious advantages of federal prosecution to a victim company are that the government bears the cost of the investigation and litigation and does most of the hard work. The disadvantages are the high standard of proof required in criminal cases, *i.e.*, proof beyond a reasonable doubt, and the victim company's lack of control over the litigation and de facto submission to the whims of the Government. The Department of Justice and the U.S. Attorneys Offices, which prosecute EEA offenses, will exact commitment and cooperation from the victim company, but will never cede any control to it.

The victim company can always file a civil action seeking injunctive relief and damages against the infringer and thereby retain control of the litigation. Unfortunately in doing so, it takes on the potentially significant expense of such litigation as well.

On balance, many companies probably will find it preferable to obtain the benefit of the federal government leading the charge, with all its powers and resources, against the infringer. For smaller victim companies or

32. 982 F.Supp. at 1023.

failing companies, or even larger companies injured by judgment-proof defendants, referral for federal prosecution may be the only option. The choice to undertake criminal prosecution, however, is at the D.O.J.'s or the U.S. Attorney's discretion. The government's interests are more focused on general and specific deterrence, and less on recoupment of the victim company's loss, although restitution certainly is an expected part of a convicted infringer's sentence under federal law. Indeed the government might well consider a viable civil action by the victim company good reason not to prosecute the case, particularly in cases where the state of the incriminating evidence is less than compelling.

In any event, it is prudent for the trade secret owner to engage in self-help in order to guard against a potential theft of its trade secrets. Obviously, preventing theft in the first place is the most cost effective way to enforce trade secrets. All such efforts have the concomitant advantage of promoting protection for the victim company under the EEA. This is because, as stated previously, the EEA places the burden on the trade secret owner to take reasonable measures to protect the trade secret information from discovery.[33]

A. Trade Secret Protection Plan

Within a very wide band of discretion, a trade secret owner should consider the value of the secret, the nature of the threat to disclosure, and the cost of any particular security mechanism.[34] Physical security, in itself, is not necessarily fully effective to guard against the unanticipated methods of theft. The most effective way to demonstrate "reasonable efforts" in protecting trade secrets is to implement a comprehensive trade secret protection plan. While such a plan could have many elements, at a minimum, it should include the following: visitor and employee access controls; procedures for controlling access to computer networks; a policy for document protection; background checks on employees, vendors, and contractors; education and continuing training for employees; and nondisclosure agreements for employees, vendors, contractors, and customers.[35]

B. Compliance Program

For every victim company, there is an accused. Each company needs to protect itself from becoming a defendant under the EEA. The best way to

---

33. 18 U.S.C. §1839(3)(A).

34. Pooley, supra, at 217.

35. *See id.* at 218-19.

avoid such risk would be to have a sound corporate compliance program deterring misappropriation of competitors' trade secrets for the company's benefit. Compliance programs grew out of the federal Organizational Sentencing Guidelines adopted by Congress in 1991. The Guidelines provide for a reduction in offense level points, and hence a lesser fine, if a company has an effective compliance program in place designed to prevent, detect, and facilitate the reporting of the commission of the crime by the company, its employees and agents.[36] These Guidelines apply to EEA offenses committed by organizations. Compliance plans take on additional special significance because the existence and effectiveness of such a plan is a major factor considered by federal prosecutors whenever deciding whether they should prosecute a corporation for knowing theft of trade secrets. The existence of an effective compliance program can help a target company avoid prosecution for the acts of rogue employees.

C. Dual Objectives

The sweeping provisions of the EEA provide strong motivation for every company to bolster the protection of its trade secrets, so it can obtain the benefit of the EEA should it become a victim of a trade secret theft. The Act also provides good reason to each company to strengthen its corporate controls to minimize the possibility of ever becoming a defendant in an EEA prosecution. Both objectives should be pursued. In this way the company can keep its fishing hole of trade secrets unknown to its competitors and simultaneously avoid the warden's citation for poaching from a competitor's secret fishing hole.

---

36. U.S. SENTENCING GUIDELINES MANUAL §8C2.5(f).