

The Economic Espionage Act of 1996

Sorojini J. Biswas

The Economic Espionage Act (hereinafter "the EEA" or "the Act") was signed into law by President Clinton on October 11, 1996. The EEA makes the theft or misappropriation of trade secrets a criminal offense, and is the first federal law that purports to both broadly define and severely punish such misappropriation and theft. This paper will examine the business and legal environment in which this law developed, the provisions of the law, and some of the law's strengths and weaknesses.

Background of the EEA

Prior to the passage of the EEA, owners of trade secrets who suspected theft or misappropriation had very few legal options available at the federal level. The few, outdated federal laws that did touch upon trade secret theft were neither broad enough to reach the kinds of trade secret thefts being perpetrated, nor muscular enough to severely punish the perpetrators of the crimes. One law, entitled the "Trade Secrets Act," was a product of the 1948 codification and revision of the Federal Criminal Code brought about by the Act of June 25, 1948. This statute was limited to the prosecution of federal employees who wrongfully disclosed confidential information and trade secrets of a person, corporation or other organization that became known to such employees during the course of employment. The punishment associated with a violation of this law was a fine of \$1000, or imprisonment of a year, and termination of employment. Convictions under this act are extremely rare, with only two published opinions being known to this author.

Federal prosecutors seeking to prosecute non-governmental employees for trade secret theft were forced to rely on the Interstate Transportation of Stolen Property Act (ITSP), or the Mail Fraud and Wire Fraud Acts. The ITSP was enacted by Congress in 1934 to prevent criminals from evading prosecution by fleeing across state lines with stolen property. Prosecution under this act requires the government to prove that "goods, wares or merchandise" were transported in interstate or foreign commerce, and that the defendant knew that they were "stolen, converted or taken by fraud." However, trade secret prosecutions under this law are difficult, in that the theft of purely intellectual property may not constitute "goods, wares, or merchandise" in the eyes of some federal courts. The federal mail and wire statutes have similarly failed to provide sufficient protection of owners of trade secrets.

The dearth of federal provisions useful in prosecuting trade secret theft has meant that the laws of the individual states were traditionally responsible for punishing trade secret misappropriations and compensating injured parties. Over 40 individual states have passed some form of trade secret protection legislation, mostly adaptations of the Uniform Trade Secrets Act (UTSA). Despite the name, however, there has been considerable variation in how trade secret law has developed in the various states. Additionally, the civil remedies provided by these laws are often inadequate in compensating a business for the theft of its secrets. In debating the merits of the EEA, Congress observed that many companies forgo civil suits either because the defendant is "judgment proof," or the company does not have the financial resources to bring a civil action, or the investigative resources to pursue trade secret theft. Criminal trade secret laws exist in twenty-four states. However, local jurisdictions often lack the means and resources to effectively investigate and prosecute alleged violations of the law. Several of the laws punish violations only at the level of a misdemeanor, and as such are rarely used by state prosecutors. Finally, state trade secret laws obviously cannot provide for the punishment of illegal actions by foreign governments or their instrumentalities.

The legislative history of the EEA makes clear that one reason for the passage of the Act was a desire to fill the gap left by the patchwork of the combined existing federal and state laws, and to create a national schema to protect US economic information. The

necessity of a more far-reaching law intended to cover the theft of trade secrets was emphasized by one report (provided by the White House Office of Science and Technology) that estimated business espionage costs to U.S. companies to be on the order of \$100 billion a year in lost sales, and a survey of 74 U.S. corporations (conducted by the National Counterintelligence Center and the U.S. Department of State) that reported more than 400 incidents of suspected foreign targeting against their businesses in 1995. Testifying in early 1996 for passage of the EEA, FBI Director Louis Freeh said the Bureau's investigations of economic espionage cases had doubled in the previous year from 400 to 800, and that 23 countries had been involved. According to Freeh, foreign governments are actively targeting U.S. industry and the U.S. government to steal "critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage."

It was this climate of perceived increased vulnerability that ultimately led to the passage of the EEA. In an early incarnation, the Act applied only to thefts of trade secrets that were intended to benefit a "foreign government, foreign instrumentality or foreign agent." Concerns that such a law may violate a number of international trade treaties caused the bill to be rewritten to include both foreign and domestic theft of trade secrets. The provisions of the EEA that were finally approved by Congress are set forth and discussed more fully below.

Provisions of the EEA

Under the EEA, a trade secret is defined as " 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 general known to, and not being readily

ascertainable through proper means by the public." (emphasis added)

Although this definition generally follows the definition of "trade secret" set forth in the UTSA, there are important differences. Most significantly, the EEA definition of trade secret is much more expansive than the UTSA definition. Moreover, the EEA definition encompasses information in any form, "whether tangible or intangible," and whether **or how** stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing. It seems clear from the language of this definition that the EEA specifically covers that information that is stored only to the extent that an individual has memorized it – that is, information in a person's head. This broadened definition has serious implications for businesses that hire from competitors, which will be discussed more fully in the oral presentation.

The heart of the EEA consists of two sections, Sections 1831 and 1832, which punish an individual or organization that **knowingly**

(1) steals, or without authorization appropriates, takes, carries

away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret, or

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization

Sections 1831 and 1832 also make illegal the attempt to commit one of the acts prohibited by paragraphs (1) to (3), or a conspiracy to commit such an act.

Sections 1831 and 1832 differ in the scope of defendants they reach. Section 1831 is specific in punishing someone who **intends or knows** that the violation of the Act will benefit any foreign government, foreign instrumentality, or foreign agent, as those terms are defined by Section 1839 of the Act. In contrast, Section 1832 targets trade secret theft more generally, without regard as to whether it benefits a foreign instrumentality. Specifically, Section 1832 seeks to punish those who commit one of the prohibited acts with the intent to convert a trade secret, which trade secret is related to or

included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret.

The sections also differ slightly with regard to what constitutes a trade secret. Under Section 1831, the theft of an intangible idea will not escape prosecution and/or punishment simply because it has not been commercially exploited. Under Section 1832, however, a trade secret is defined as being "related to or included in a product that is produced for or placed in interstate or foreign commerce." It would seem that under this definitions, the theft of a commercially unexploited trade secret would not be covered by the EEA.

Individuals and organizations convicted of violating Sections 1831 and 1832 are subject to severe penalties. Persons convicted of violating Section 1831 may be fined up to \$500,000 or imprisoned up to 15 years, or both, while any organization that commits any offense prohibited by Section 1831 may be fined up to \$10,000,000. A person convicted of violating Section 1832 faces a fine of up to \$500,000 or a prison sentence of up to 10 years, or both, while any organization that commits any offense described in Section 1832 may be fined up to \$5,000,000.

Section 1834 provides for the criminal forfeiture of property obtained or used in the process of violating Sections 1831 or 1832. The section provides for criminal forfeiture to the United States of any property constituting or derived from the process of violation of the act, and the forfeiture of any property used or intended to be used in the furtherance or committance of the act. This section may allow, for example, prosecutors and enforcers to dismantle internet espionage schemes and seek criminal forfeiture of all computers and devices used to commit the offenses prohibited by the Act.

Section 1835 relates to orders to preserve the confidentiality of trade secrets during the prosecution of an alleged offense under the Act. This section provides that in any prosecution or proceeding under the Act, a federal court shall "enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets." Additionally, should a court declare that information regarded as a trade secret must be revealed, the government will be allowed an immediate appeal of the decision. This confidentiality clause was included because Congress expressed concerns about the efforts taken by courts to protect the confidentiality of trade secrets, and, in part, so that legitimate owners of trade secrets would not be discouraged from using the

EEA.

The EEA applies not only to illegal acts conducted entirely within the United States, but also applies to foreign offenses, provided that any act in the furtherance of the offense was committed in the United States. As one might expect, a significant amount of foreign economic espionage occurs outside of the United States. Under Section 1837 of the Act, a foreign corporation that sells a product within the United States that embodies a stolen trade secret can be prosecuted in the United States if the misappropriation occurred here. This provision applies regardless of where the product is manufactured. The EEA also reaches completely foreign acts of economic espionage provided that the defendant is either a United States citizen, a permanent resident alien of the United States, or a United States corporation.

Strengths and Weaknesses of the EEA

The Economic Espionage Act creates federal trade secret rights. Although there is no private cause of action for trade secret misappropriation under the statute, the criminal penalties imposed for trade secret theft are generally more severe than criminal violations of other intellectual property rights.

For trade secret owners, the EEA provides the prospect of greatly improved protection with regard to trade secrets. The broadened definition of trade secret extends to such non-technical materials such as business plans and customer lists. Aggrieved companies will not be limited by the limited resources of local prosecutors, but instead may, through the federal prosecutor, have the resources of the FBI and the Department of Justice at their disposal. For example, the statute authorizes the attorney general, deputy attorney general or assistant attorney general in the Criminal Division of the Justice Department to apply for a federal court order authorizing or approving the interception of wire or oral communications by the FBI or other federal agencies having responsibility for the investigation of the offense. The attorney general is also authorized to commence civil actions to obtain injunctive relief to protect the trade secret owner from any violations or further violations of the Act.

The EEA is not without its critics, and business wishing to rely on the provisions of the Act in the future are well advised to be aware of potential weaknesses of the Act.

The EEA is a criminal statute; thus the burden of proof is on the government and each element of every offense must be established beyond a reasonable doubt. This may prove to be a difficult burden to shoulder, especially in satisfying the proof of the requisite intent (i.e., the intent to injure the owner of the trade secret, or the knowing theft of a trade secret). The existence of the criminal remedy may also complicate civil litigation involving trade secret misappropriation. Witnesses in the civil action may refuse to answer questions by asserting their Fifth Amendment right against self-incrimination.

A criminal prosecution for trade secret violation also emphasizes the tension between preserving the confidentiality of trade secrets, and the public nature of U.S. legal proceedings. Companies may not report suspected trade secret theft if they fear that their secrets may be brought into the public. To reduce this chance, and as explained above, the EEA has a provision that states that a court must enter the appropriate orders or take whatever action is necessary to preserve the confidentiality of the trade secret. (e.g., drafting protective orders limiting access to documents and conducting hearings *in camera*, or allowing certain parts of the record to be sealed).

It is not clear whether the Act will actually increase the number of trade secret thefts reported to the authorities. In the past, many companies were reluctant to report known acts of business espionage, fearing that the report would affect stock prices and customer confidence. In a survey published in July 1995 by the National Counterintelligence Center, 42% of the respondents said they never reported suspected incidents of economic espionage to the Governments, although 74 of 173 companies that responded reported a

total of 446 incidents of suspected economic espionage.

Finally, while provisions of the EEA purport to extend its jurisdictional reach offshore, these provisions are not likely to be effective in dealing with countries that do not have an extradition treaties with the United States.

A recent survey indicates that the EEA has been used to prosecute alleged industrial spies a mere four times. In spite of the apparently infrequent enforcement of the new law to date, the FBI has been briefing companies across the country on the provisions of the Act, while the United States Department of Justice has been writing regulations to govern which cases will be undertaken and presented. In light of this activity, it appears that prosecutions under the EEA will increase in the future. In the meantime, it behooves owners of trade secrets to become familiar with the provisions of the Economic Espionage Act, in order to both more fully understand the new legal tools available to them for protecting their trade secrets, and to bring their own businesses into compliance with the provisions of the EEA, thus preventing the unintended violation of those provisions.

SUPPLEMENT A

Economic Espionage Act of 1996

Section 1: Short Title

"This Act may be cited as the "Economic Espionage Act of 1996."

Title I : Protection of Trade Secrets

Sec. 101. Protection of Trade Secrets

(a) In General.-Title 18, United States Code, is amended by inserting after chapter 89 the following:

Sec.

1831. Economic espionage.

1832. Theft of trade secrets.

1833. Exceptions to prohibitions.

1834. Criminal forfeiture.

1835. Orders to preserve confidentiality.

1836. Civil proceedings to enjoin violations.

1837. Conduct outside the United States.

1838. Construction with other laws.

1839. Definitions.

Chapter 90- Protection of Trade Secrets

Section 1831. Economic espionage

(a) In General - Whoever, intending or knowing that the offense will

benefit any foreign government, foreign instrumentality, or foreign agent,

knowingly -

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret,

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization,

(4) attempts to commit any offense described in any of paragraphs (1) through (3), or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than \$500,000 or imprisoned not more than 15 years, or both.

(b) Organizations - Any organization that commits any offense described in subsection (a) shall be fined not more than \$ 10, 000, 000.

Section 1832. Theft of trade secrets.

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly -

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches,. draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs

(1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than \$5,000,000.

Section 1833. Exceptions to prohibitions.

This chapter does not prohibit -

- (1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or
- (2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

Section 1834. Criminal forfeiture.

(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States -

(1) any property constituting or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) any of the person's or organization's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, 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.

(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S. C. 8 5 3), except for subsections (d) and 0) of such section, which shall not apply to forfeitures under this section.

Section 1835. Orders to preserve confidentiality

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

Section 1836. Civil proceedings to enjoin violations

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

Section 1837. Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof-, or

(2) an act in furtherance of the offense was committed in the United States.

Section 1838. Construction with other laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employees under section 552 of title 5 (commonly know as the Freedom of Information Act).

Section 1839. Definitions

As used in this chapter,

(1) the term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government:

(2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government:

(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 general known to, and not being readily

ascertainable through proper means by the public, and

(4) the term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to or license in, the trade secret is reposed."

(b) Clerical Amendment. The table of chapters at the beginning part I of

title 18, United States Code, is amended by inserting after the item relating to chapter 89 the

following:

"90. Protection of trade secrets 1831"

(c) Reports. - Not later than 2 years and 4 years after the date of the

enactment of this Congress of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S. C. 10601).

Sec. 102 Wire and Electronic Communications Interception and Interception of Oral Communications.

Section 2516(l)(c) of title 18, United States Code, is amended by inserting "chapter 90 (relating to protection of trade secrets)," after "chapter 37 (relating to espionage),".

[\[Back to Top\]](#)