THE ECONOMIC ESPIONAGE ACT OF 1996

By Spencer Simon

The development and production of proprietary economic information is an integral part of virtually every aspect of United States trade, commerce, and business and, hence, is essential to maintaining the health and competitiveness of critical segments of the United States economy. The theft, misappropriation, and wrongful receipt, transfer, and use of United States proprietary economic information, particularly by foreign governments and their agents and instrumentalities, but also by domestic malefactors, directly imperils the health and competitiveness of our economy.¹

The Economic Espionage Act of 1996 (EEA),² signed into law by President Bill Clinton on October 11, 1996, creates two new federal criminal offenses involving the theft of trade secrets. The EEA has two primary goals: (1) prevention of trade secret theft specifically by a foreign government agent or instrumentality or person acting on behalf of a foreign government, and (2) general protection from theft of trade secrets by anyone.³ The EEA gives the U.S. Department of Justice broad authority to prosecute trade secret theft occurring both domestically and abroad, as well as over the Internet.⁴ It applies to conduct occurring outside the United States if the offender is a U.S. citizen or corporation or if any act in furtherance of the offense was committed in the United States.

I. NEED FOR FEDERAL TRADE SECRET LEGISLATION

The EEA was passed to fill a large hole in trade secret law that had been enlarged by the emergence of new information technologies. Prior to passage of the EEA, most federal trade secret theft cases were prosecuted


under the Interstate Transportation of Stolen Property Act,\(^5\) which was not designed nor intended to apply to intellectual property. Because of the lack of a federal statute, various state laws, mostly based on some variation of the Uniform Trade Secrets Act,\(^6\) were utilized to fill the gap. However, these state laws were not adequate to combat the increasing problem of trade secret misappropriation.

The problem of foreign economic espionage has grown significantly since the end of the Cold War. Testifying before joint hearings by the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology, and Government Information for the EEA's passage in early 1996, Federal Bureau of Investigation Director Louis Freeh stated that the Bureau's investigations of economic espionage cases had doubled in the previous year from 400 to 800, and twenty-three countries had been involved.\(^7\) He claimed that 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."\(^8\) According to Freeh and other law enforcement officials, former military spies have been redeployed by foreign governments to the "commercial world, presumably ready to use their skills in other ways."\(^9\) The losses to U.S. industry from foreign economic espionage is estimated at nearly $100 billion per year.\(^10\)

A. Interstate Transportation of Stolen Property Act

The principal problem before the enactment of the EEA was that no federal statute directly addressed economic espionage or otherwise protected proprietary information in a systematic manner. Federal prosecutors principally relied upon the Interstate Transportation of Stolen Property Act (ITSP) to combat trade secret theft.\(^11\) The ITSP was passed in the 1930s in an effort to prevent criminals from moving stolen property across state lines in attempts to evade the jurisdiction of state and local law enforcement officials. It was not enacted to protect proprietary information

---

7. See Hearings, supra note 1.
8. See id.
in an increasingly digital world. The main problem with the use of the ITSP for prosecution of trade secret misappropriation is that the statute applies only to "goods, wares, or merchandise."\(^{12}\) Consequently, prosecutors found it ill-suited to deal with thefts involving intellectual property, which by its nature is generally not physically transported from place to place. Further, courts have been reluctant to extend the reach of the ITSP to intangible property.\(^{13}\) Following the Supreme Court's interpretation of the statutory language of the ITSP six years earlier,\(^{14}\) the Tenth Circuit stated that "the element of physical 'goods, wares, or merchandise' in §§2314 and 2315 is critical. The limitation which this places on the reach of the ITSP is imposed by statute itself, and must be observed."\(^{15}\)

**B. Wire Fraud and Mail Fraud Statutes**

Other federal laws commonly-used to combat trade secret misappropriation were the Wire Fraud and Mail Fraud statutes.\(^{16}\) These statutes have been somewhat more useful for prosecutors than the ITSP because they do not define "property" so narrowly.\(^{17}\) The laws have other limitations which detract from their use in trade secret prosecutions, such as the requirement that wire or mail transmission is used in the commission of the thefts.\(^{18}\) In addition, both statutes requires an intent to defraud as well as the use of either the mail or wire, radio, or television.\(^{19}\) This fraud element is another significant limitation because many trade secret thefts involve merely the copying of vital information and not a permanent loss of the information itself.

**C. State Laws**

State laws, on the other hand, were expressly designed to combat trade secret misappropriation. The principal state trade secrets model is found in section 757 of the Restatement of Torts, entitled Misappropriation of Trade Secrets. According to the Restatement, a trade secret "may consist of any formula, pattern, device, or compilation of information which is

---

13. See the results in Dowling, 473 U.S. at 207; Brown, 925 F.2d. at 1301.
15. Brown, 925 F.2d at 1309.
17. "Property" is left undefined and without descriptive limitations such as the ITSP's "physical goods, wares, or merchandise" in these statutes. Id. §§ 1341 & 1343; see also United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978). In this case, the defendant was charged with fraud by wire. The court found that the computer system involved did constitute property.
19. See id.
used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."

Today, most states have some form of trade secret protections, and most states have enacted some form of the Uniform Trade Secrets Act (UTSA). The intent in proposing the UTSA was to codify existing common law standards and to provide a uniform approach to trade secret misappropriation among the states, providing for both civil and criminal penalties. The UTSA narrows the definition of a trade secret through the inclusion of two additional standards that must be met. A trade secret is defined as:

information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The UTSA did not produce uniformity. As one commentator observed, the "trade secret protection granted in each state is far from uniform relative to the other states. This often leads to the result that the ability to recover for theft of a trade secret becomes a choice of law or a contract interpretation question." This issue becomes more acute when the theft involves a foreign person, entity, or nation. States have neither the jurisdictional authority nor resources to prosecute violations international in scope.

20. RESTATEMENT OF TORTS § 757, cmt. b (1939). "It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers." Id.


23. See id. at 196.


25. Mossinghoff, supra note 21, at 196.
II. LEGISLATIVE HISTORY

Two major hearings were held to consider the need for federal legislation to prevent the theft of trade secrets as a result of economic espionage. The first, held on February 28, 1996, was a joint hearing before the Senate Select Committee on Intelligence and the Senate Judiciary Subcommittee on Terrorism, Technology, and Government Information.26 The second hearing was held before the Subcommittee on Crime of the House Judiciary Committee on May 9, 1996.27 The lead witness in both hearings was FBI Director Louis J. Freeh. A number of industry leaders, primarily representing Silicon Valley and aerospace companies, supported Director Freeh’s contention that federal legislation was necessary to combat the growing scourge of economic espionage by both domestic and, especially, foreign agents and entities.28

The hearings documented the two major underpinnings of the legislation. First, foreign governments, through a variety of means, are actively involved in stealing critical technologies, data, and information from U.S. companies or the U.S. Government for the economic benefit of their own industrial sectors.29 Second, federal laws then on the books—including the ITSP and the Mail Fraud and Wire Fraud statutes—were of limited use in prosecuting acts of economic espionage.30

Additionally, state laws protecting trade secrets were determined to be inadequate. As the Senate Judiciary Committee concluded:

What State law there is protects proprietary economic information only haphazardly. The majority of States have some form of civil remedy for the theft of such information - either adopting some version of the Uniform Trade Secrets Act, acknowledging a tort for the misappropriation of the information, or enforcing various contractual arrangements dealing with trade secrets. These civil remedies, however, often are insufficient. Many companies choose to forgo civil suits because the thief is essentially judgment proof ... or too difficult to pursue .... In addition, companies often do not have the resources or the time to bring suit. They also frequently do not have the investigative re-

29. See id. It is interesting to note that the U.S. itself has been accused of active involvement in economic espionage activities abroad, most notably in France. See Peter Schweizer, The Growth of Economic Espionage: America is Target Number One, FOREIGN AFF., Jan. 11, 1996, at 10.
sources to pursue a case. Even if a company does bring suit, the civil penalties often are absorbed by the offender as a cost of doing business and the stolen information retained for continued use. Only a few States have any form of criminal law dealing with the theft of this type of information. Most such laws are only misdemeanors, and they are rarely used by State prosecutors.

Federal criminal law is needed because of the international and interstate nature of this activity, because of the sophisticated techniques used to steal proprietary economic information, and because of the national implications of the theft. Moreover, a Federal criminal statute will provide a comprehensive approach to this problem—with clear extraterritoriality, criminal forfeiture, and import-export sanction provisions.31

III. DISCUSSION OF THE EEA

A. Economic Espionage

Section 1831 of the EEA, titled “Economic Espionage,” criminalizes acts done with the intent to benefit any foreign government, instrumentality, or agent. Culpability is determined with reference to section 1831(a):

(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

31. Id. at 12.
more of such persons do any act to effect the object of the con-
spiracy.\textsuperscript{32}

The EEA provides a list of examples of violative acts, but the legisla-
tive history states that these examples were not intended to be exhaustive. Rather the examples serve as illustrative guidelines.\textsuperscript{33}

\textbf{B. Theft of Trade Secrets}

Section 1832 of the EEA, titled “Theft of Trade Secrets,” pertains to
domestic acts and makes the same conduct described in section 1831 a
crime regardless of whether the theft is meant to benefit a foreign govern-
ment. Section 1832 differs from section 1831 by including stipulations
that the goal of the misappropriation is to harm the owner of the trade se-
et and to economically benefit someone other than the owner of the trade
secret.\textsuperscript{34}

\textbf{C. Definition of Trade Secrets}

The definition of trade secrets under the EEA is broader than that
contained in the UTSA because it includes the new technological methods
by which trade secrets can now be created and stored. A trade secret is
defined under the EEA to mean “all forms and types of financial, business,
scientific, technical, economic, or engineering information, including pat-
terns, 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 memori-
alized physically, electronically, graphically, photographically, or in writ-
ing ....”\textsuperscript{35} Like the UTSA, the EEA definition requires that the owner of
the information take undefined “reasonable measures” to keep the infor-
mation secret and that the information has independent economic value,
actual or potential, because it is not generally known to the public or read-
ily ascertainable through legal means.\textsuperscript{36} Under the EEA, “secret” means

\textsuperscript{33} See H.R. REP. No. 104-788, at 11-12 (1996).
\textsuperscript{34} Specifically, it requires “intent to convert a trade secret, that is related to or in-
cluded 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.” 18 U.S.C.A. § 1832.
\textsuperscript{35} Id. § 1839. Also note that “[t]hese general categories of information are included
... for illustrative purposes and should not be read to limit the definition of trade secret.”
\textsuperscript{36} While it is up to the court to determine in each case whether reasonable efforts
were made to protect the information, the legislative history states: “[t]he fact that the
owner did not exhaust every conceivable means by which the information could be kept
that "the information was not generally known to the public or to the business, scientific, or educational community in which the owner might seek to use the information." 37

D. Mens Rea Requirement

Both new crimes require specific states of mind. As stated above, section 1832, (which relates to domestic violations) contains two intent elements, both of which must be present for conduct to fall within the domestic prong of the statute. 38 The perpetrator must intend to convert a trade secret to the economic benefit of "anyone other than the owner" and also intend or know that the offense will injure the owner of the trade secret. 39 Section 1831, the foreign violations regulation, requires only that the perpetrator intend, know, or have reason to know that the trade secret theft will benefit a foreign government, instrumentality, or agent. Unlike section 1832, section 1831 contains no requirement that the offender intend or know that the theft will injure the owner of the trade secret. 40 Presumably, this was done to lower the bar in cases involving international economic espionage.

E. Penalties

The EEA's most noticeable and perhaps significant effect is to implement stiff fines and imprisonment for offenders. Violations of the EEA are treated as serious crimes.

Section 1831 violations exact significantly greater penalties than do section 1832 violations. This can be interpreted as a judgment by Congress that foreign economic espionage is a more severe transgression than wholly domestic trade secret thefts. 41 Section 1831 specifically imputes a maximum fine of $500,000 per convicted violation for individuals and, for corporations, a maximum fine of $10,000,000 per convicted violation. 42 Individual criminal liability under section 1831 is set at a maximum of fifteen years per violation. 43

Section 1832 fines, while lesser than their foreign espionage counterparts, are still significant. The maximum individual fine is not specifically

37. Id. at 13.
38. 18 U.S.C.A. § 1832.
39. Id.
41. See Pooley, supra note 9, at 202.
42. See id.
43. See id.
set, but it is implied that the maximum fine for felonies is applicable: $250,000 per violation. Corporate liability is set at a maximum of $5,000,000 per violation.

The legislative history indicates that these criminal fines should be set pursuant to the federal fines provision, where the fine should be set at the greater of twice the value of the loss to the trade secret owner or twice the gain to the perpetrator if this amount is greater then the fines provision of the EEA. Furthermore, the legislative history suggests that fines above the stated maximums could be imposed on corporations, "in cases where the loss to the trade secret owner was particularly high," by relying on the federal fines provision rather than the fines provided for in the EEA.

Individuals may face substantial terms of imprisonment in addition to criminal fines. Individual criminal liability under section 1831 is set at a maximum of fifteen years per violation. Section 1832 violators are subject to a maximum of ten years per violation.

In addition, section 1834 of the EEA requires a court to order forfeiture of any proceeds obtained directly or indirectly from the offense. Further, the EEA allows courts to order forfeiture of any property used or intended to be used in the commission of the offense. Such forfeitures are governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970, except for subsections (d) and (j) of that section. These forfeitures do not go toward compensating the actual victim of the trade secret misappropriation, although there is an indication in the legislative history that such victims may be able to petition the government for restitution based on the proceeds from the sale of forfeited property.

F. Confidentiality and Injunctive Relief

Section 1835 specifically provides for the protection of trade secrets during the prosecution of any offense under the EEA. This provision was

44. See id. at 201; see also 18 U.S.C.A. § 3571(b)(3) (The federal fines provision serves as a guideline to courts in the assessment of fines.).
46. See 142 CONG. REC. S12201-03, S12213 (1996) (referencing 18 U.S.C.A. § 3571(d)).
47. See Pooley, supra note 9, at 201; see also 18 U.S.C.A. § 3571(d).
48. See Pooley, supra note 9, at 201 (citing 142 CONG. REC. S12201-03, S12213 (1996)).
50. See id.
52. See 142 CONG. REC. S12201-03, S12213 (1996).
added to protect trade secret owners from further disclosure of the trade secret(s) at issue, beyond the actual violation itself, and possibly to encourage trade secret owners, who otherwise would be wary of further disclosure, to be forthcoming in the event of a misappropriation.\textsuperscript{53} Section 1835 further allows the Attorney General to instigate separate civil proceedings to enjoin continued trade secret violations during prosecution.\textsuperscript{54}

G. Territorial Jurisdiction

Section 1836 confers expansive jurisdiction on federal courts that is not limited to the territorial or maritime boundaries of the United States.\textsuperscript{55} The statute provides for exclusive federal jurisdiction and is intended to punish conduct occurring in the United States, or outside of the United States if the defendant is a U.S. citizen or permanent resident alien or an organization substantially owned or controlled by U.S. citizens or permanent resident aliens, or incorporated in the United States.\textsuperscript{56} Interestingly, the EEA also grants federal jurisdiction to acts primarily foreign in nature.\textsuperscript{57} If any single act in furtherance of an action or scheme to misappropriate trade secrets occurred in the United States, it would be actionable as an EEA violation.\textsuperscript{58} For example, a trade secret theft involving the electronic transfer or routing by any means of the secret merely through the U.S. on its way to another foreign locale would constitute a violation of the statute. Even more curious is the EEA’s extension to acts committed entirely in foreign countries, where the defendant is either a United States’ corporation or a citizen or permanent resident alien of the United States. These acts can lead to EEA violations even in the absence of any other connection between the misappropriation and the United States.\textsuperscript{59} Violations similar to the last two examples will probably be rare, as it is seems unlikely that the Department of Justice would pursue or have the resources to pursue such acts.

H. Preemption

Section 1837 explicitly states that the EEA should not be construed in any manner to preempt or displace any other remedies.\textsuperscript{60} This statute is

\textsuperscript{53} See Hearings, supra note 1.
\textsuperscript{54} See 18 U.S.C.A. § 1835.
\textsuperscript{55} See id. § 1836.
\textsuperscript{56} See id.
\textsuperscript{57} See id.
\textsuperscript{58} See id.
\textsuperscript{59} This would also mean that U.S. economic espionage agents abroad are liable under the EEA. See supra note 27.
\textsuperscript{60} See 18 U.S.C.A. § 1837.
not intended to preempt any claims based on state law or under any other federal law.

IV. LIMITATIONS OF THE EEA

The EEA does not protect trade secrets related to services (as opposed to goods), negative know-how, or reverse engineering. Furthermore, it does not address the needs of U.S. corporations operating abroad from trade secret theft. It also fails to adequately address the rights of victims for monetary loss sustained as a result of the theft and misappropriation of their trade secrets.

To qualify under section 1832, trade secrets must be “related to or included in a product that is produced for or placed in interstate or foreign commerce.” Because trade secrets explicitly must be embodied in a product in the stream of commerce, protection is limited if the trade secret relates to a rendering of services rather than a produced ware that contains or uses the secret. As noted by some commentators, “[t]his means that the EEA arguably does not cover either ‘negative know-how’ or information discovered but not [currently] used by a company.” It is interesting to note that both of these are protected under the UTSA. It should be questioned why these were purposefully left without protection in the EEA, as the drafters substantially borrowed from the UTSA in writing this statute.

Some commentators have also noted that sections 1831 and 1832(a)(2) (which are identical) “arguably prohibit[] many forms of heretofore lawful reverse-engineering activity.” The EEA could be used to prosecute reverse-engineering procedures that currently are legal. Such procedures are not mentioned in the statute at all. Reverse engineering often involves acts prohibited under subsection (a)(2) undertaken on publicly available merchandise. Formerly legal “reverse engineering ... may well involve [the now] prohibited ‘sketching, drawing, or photographing’ of the trade secret ....” Because the legislative history reveals that Congress did not intend to infringe on the legitimate interests of private businesses, compe-
tion, and commerce, the EEA should be amended to explicitly exempt reverse engineering from the scope of the statute.

Second, U.S. corporations with offices abroad are not protected under the EEA. If trade secrets are stolen from a U.S. company operating in a foreign country, the corporation has no legal protections if the theft is not perpetrated by a U.S. citizen, a permanent resident alien, or an organization incorporated in the U.S., and no part of the theft occurs within the U.S. If the EEA is to extend to acts entirely beyond territorial boundaries, there should be a provision protecting the interests of U.S. corporations operating abroad.

The last significant limitation of the EEA involves the lack of any civil remedies for victims of trade secret theft and misappropriation. All fines and forfeitures go to the government under the aforementioned Comprehensive Drug Abuse Prevention and Control Act of 1970. The only compensatory remedy for the injured party or parties under federal law is the possibility that such victims may be able to petition the government for restitution based on the proceeds from the sale of property forfeited under section 1834 of the EEA, as indicated in the legislative history. Barring this, the only recourse for trade misappropriation victims is filing an action under state civil law, which can be prohibitively expensive and often ineffective in substantially compensating the victim for real losses sustained. The EEA should be amended to correct this oversight. A federal law should specifically and adequately address the losses sustained by victims of trade secret theft in the same manner that the EEA protects the U.S. economy, in general, by imposing such stiff penalties for acts of foreign economic espionage.

V. CONCLUSION

The Economic Espionage Act of 1996 is a comprehensive device to combat trade secret misappropriation. It is particularly harsh toward perpetrators of foreign economic espionage, as evidenced by the significantly more severe penalties imposed. Another indication of the slant toward protection against foreign economic espionage is the near primary focus

68. See 142 CONG. REC. S12201-03, S12213 (1996).
69. See S. REP. NO. 104-359, at 12 (1996) (Senate Judiciary Committee’s conclusion on the effectiveness of state civil remedies).
on the foreign threat in discussions used to espouse passage of the statute.\textsuperscript{70}

There is much give and take in the statute, as it balances competing interests to preserve overall fairness. For example, while making convictions slightly more difficult and trade secret owners’ roles more burdensome by placing the victim’s secrecy maintenance conduct under scrutiny, the overall effect provides reasonable protection for potential defendants who utilize, rather than misappropriate, an alleged but not actual trade secret. Steps were taken in the drafting to avoid application to “innocent innovators or to individuals who seek to capitalize on the personal knowledge, skill, or abilities they may have developed.”\textsuperscript{71} The EEA does not criminalize the use of knowledge or skills developed while employed at another company or the use of generic business knowledge to compete with former employers. On the other hand, the EEA does criminalize “the acts 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.”\textsuperscript{72}

Overall, despite its limitations, the EEA should prove to be a substantial advance in the fight against industrial espionage. It has created a national standard governing trade secret misappropriation, supplementing the multitude of federal and state laws that were previously used to prosecute trade secret misappropriators with only mild results. In so doing, the EEA has filled a significant gap in the protection of trade secrets in the global information age.

\textsuperscript{70} See Hearings, supra note 1.
\textsuperscript{71} H.R. REP. No. 104-788, at 8 (1996).
\textsuperscript{72} Id. at 8.