Touro Law Review

Volume 15 | Number 1 Article 6

1998

# Transforming Trade Secret Theft Violations into Federal Crimes: The Economic Espionage Act

Lorin L. Reisner

# TRANSFORMING TRADE SECRET THEFT VIOLATIONS INTO FEDERAL CRIMES: THE ECONOMIC ESPIONAGE ACT

*Lorin L. Reisner*[*]

## INTRODUCTION

The law of intellectual property is becoming increasingly criminalized. Violations of the copyright law are punishable as federal criminal offenses.[1] Trafficking in goods or services using counterfeit trademarks also violates federal criminal law.[2] No law, however, has more potential to transform a broad category of intellectual property violations traditionally carrying civil liability into federal felonies than the Economic Espionage Act of 1996 (the "EEA"),[3] which creates federal criminal liability for the theft of trade secrets.

---

* Lorin L. Reisner is a partner at Debevoise & Plimpton in New York and a former Assistant United States Attorney in the Southern District of New York. R. Townsend Davis, Jr., a Debevoise & Plimpton associate, assisted in the preparation of this article.

[1] *See* 18 U.S.C. § 2319 (1998); *see also* 17 U.S.C. § 506 (1998). Section 506 provides in pertinent part: "Any person who infringes a copyright willfully and for purposes of commercial advantage or private financial gain shall be punished as provided in section 2319 of title 18." *Id.* Congress recently enacted the "No Electronic Theft Act," which expanded the scope of criminal liability for copyright infringement and increased the maximum fines and terms of imprisonment. No Electronic Theft Act, Pub. L. 105-147, 111 Stat. 2678 (1997).

[2] 18 U.S.C. § 2320 (1998). This section provides in pertinent part:

> Whoever intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services shall, if an individual, be fined not more than $2,000,000 or imprisoned not more than 10 years, or both, and, if a person other than an individual, be fined, not more than $5,000,000. In case of an offense by a person under this section that occurs after that person is convicted of another offense under this section, the person convicted, if an individual, shall be fined not more than $5,000,000 or imprisoned not more than 20 years, or both, and if other than an individual, shall be fined not more than $15,000,000.

*Id.*

## I. THE EEA

Before the EEA was enacted, federal law had little impact on trade secrets matters.[4] Owners of trade secrets relied primarily on state law and the traditional civil remedies of damages and injunctive relief to protect their proprietary information.

In February 1996, FBI Director Louis Freeh asked Congress for greater authority to combat economic espionage against U.S. companies.[5] This request was based on a concern that American companies had suffered billions of dollars in lost revenues, lost jobs and reduced market share as a result of trade secret theft. As the Senate Report supporting the legislation observed: "Today, a piece of information can be as valuable as a factory is to a business. The theft of that information can do more harm than if an arsonist torched that factory."[6] The EEA was enacted in October 1996.[7]

The EEA has two principal sections: one prohibiting the theft of trade secrets with intent to benefit a foreign government[8] and

---

[3] 18 U.S.C. §§ 1831-1839 (1996).

[4] *See generally* Gerald Mossinghoff, *The Economic Espionage Act: A New Federal Regime of Trade Secret Protection*, 79 PAT. & TRADEMARK OFF. SOC'Y 191 (1997) (discussing economic espionage and the creation of federal legislation to more effectively regulate and prevent the theft of trade secrets).

[5] *See* Mossinghoff, *supra* note 4, at 192. Two significant hearings were held to consider the necessity for additional Federal legislation to prevent trade secrets theft resulting from economic espionage. *Id.* Director Freeh was the lead witness in the hearings. *Id.*

[6] S. REP. 104-359, 1996 WL 497065 at *7.

[7] *See* 18 U.S.C. § 1831 *et seq.*

[8] 18 U.S.C. § 1831 (1996). This section provides in pertinent part:

> 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;

another prohibiting trade secrets theft more generally.[9] Under 18 U.S.C. Section 1832, a crime is committed by any person who

> with intent to convert a trade secret . . . 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.[10]

A "trade secret" is defined broadly as information that (1) the owner has taken "reasonable measures" to keep secret and (2) derives "independent economic value" from "not being generally known to" and not being "readily ascertainable

---

> (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 subdivision (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

*Id.*

[9] *See* 18 U.S.C. § 1832 (1996).

[10] *See* 18 U.S.C. § 1832(a) (1996).

through proper means by the public."[11] Trade secrets can include any type of financial, business, scientific, technical, economic or engineering information that satisfies these two requirements.[12] A violation of Section 1832 carries a maximum term of imprisonment of ten years and fines in excess of $250,000 for an individual[13] and $5 million for an organization.[14] The EEA also contains a provision for forfeiture of all property used to commit or derived from the proceeds of an offense.[15]

---

[11] 18 U.S.C. § 1839(3) (1996). This section provides in pertinent part:

> The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, programs 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 derived independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

*Id.* *See also* BLACK'S LAW DICTIONARY 1339 (6th ed. 1990). (Trade secret defined as a "formula, pattern, device or compilations of information which is used in one's business and which gives one opportunity to obtain advantage over competitors who do not know or use it.").

[12] *See* 18 U.S.C. § 1839(3) (1996).

[13] *See* 18 U.S.C. § 1832(a) (1996). This section provides in pertinent part:

> 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 . . . shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

*Id.*

[14] *See* 18 U.S.C. § 1832(b) (1996). This section provides that "[a]ny organization that commits any offense described in section (b), shall be fined not more than $5,000,000." *Id.*

[15] *See* 18 U.S.C. § 1834(a) (1996). This section provides in pertinent part:

## II. PROSECUTIONS UNDER THE EEA

There have been six publicly-reported prosecutions under the EEA.[16]

### A. *The Worthing Case*[17]

In the first reported EEA prosecution, Patrick Worthing, an employee of fiberglass research company PPG Industries, Inc., was charged with attempting to sell secret information relating to PPG's customers and auto-parts manufacturing process to Owens-Corning, a PPG rival.[18] In particular, the Government alleged that Worthing propositioned Owens-Corning's CEO under an assumed name in a letter that stated: "Would it be of any profit to Owens-Corning to have the inside track on PPG?"[19] The Owens-Corning executive provided the letter to PPG, which then contacted the FBI.[20] During an FBI undercover investigation that followed, Worthing requested cash payments in exchange for confidential information.[21] He later admitted to stealing documents, blueprints,

---

> 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 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.

*Id.*

[16] *See infra* notes 18-61 and accompanying text.

[17] United States v. Worthing, No. 97-9 (W.D. Pa., Dec. 9, 1996) (crim. indictment).

[18] *Id.*

[19] *See* Affidavit of Bruce T. Rupert in Support of Criminal Compl., United States v. Worthing, No. 96-2844M (W.D. Pa., Dec. 9, 1996).

[20] *Id.*

[21] *Id.*

photographs, and product samples from PPG.[22] Worthing pled guilty and was sentenced to a term of imprisonment of 15 months.[23]

B. *The Gillette Case*[24]

In September 1997, a grand jury in the Middle District of Tennessee indicted another "insider" with access to technical knowledge, Steven L. Davis.[25] Davis was an engineer employed by Wright Industries, Inc., a contractor engaged by Gillette to develop production equipment for a new shaving design.[26] He was alleged to have downloaded 600 "megs" of secret data and drawings from the Gillette project onto his laptop computer.[27] Davis then distributed the information to Gillette competitors by fax and electronic mail.[28] Davis was charged with copying and attempting to steal, copy or possess trade secrets in violation of the EEA.[29] In January 1998, he pled guilty to EEA violations and is currently awaiting sentencing.

---

[22] *Id.*

[23] United States v. Worthing, No. 97-9-1 (W.D. Pa., June 5, 1997). Worthing's brother also pled guilty to conspiracy to violate the EEA and received five years probation. United States v. Worthing, Crim. No. 97-9-2 (W.D. Pa., April 18, 1997).

[24] United States v. Davis, No. 3:97-00124 (M.D. Tenn., Sept. 24, 1997) (crim. indictment).

[25] *Id.*

[26] *Id.* Through faxes and electronic mail, along with the use of pseudonyms, Davis allegedly transmitted the new shaving system to Gillette competitors such as Warner Lambert Company, BIC and American Safety Razor company. *Id. See also* A. Primer, Protecting Your Client Under the Espionage Act, 80 J. PAT. & TRADEMARK OFF. SOCIETY 360, 365 (1998).

[27] United States v. Davis, No. 3:97-00124 (M.D. Tenn., Sept. 24, 1997) (crim. Indictment).

[28] *Id.*

[29] *Id.*

C. *The "Four Pillars" Case*[30]

Two EEA prosecutions have involved alleged efforts by foreign companies to extract trade secrets from "insiders" employed by U.S. companies. The defendant in an Ohio case, Ten Hong "Victor" Lee, was an employee of Avery Dennison Corporation -- a large adhesive products manufacturer -- who provided manufacturing and research information about Avery's business to Four Pillars, a Taiwanese company, in exchange for cash payments over a seven-year period.[31] Lee worked for Avery as a scientist and had access to a broad range of information at Avery's technical facility in Concord, Ohio.[32] After FBI surveillance captured Lee on closed-circuit TV rummaging a colleague's files containing confidential documents, Lee was arrested.[33] He subsequently pled guilty and admitted to having provided Four Pillars with secret adhesives formulae and testing data valued at between $50 and $60 million.[34]

After his arrest, Lee cooperated with the government and arranged a meeting with the chairman of Four Pillars, Pin Yeng Yang, and his daughter, also an employee of Four Pillars.[35] Shortly after this meeting, the Yangs and Four Pillars were charged with attempting to steal trade secrets in violation of the EEA.[36] The defendants are awaiting trial.

---

[30] United States v. Yang, Crim. No. 97-288 (N.D. Ohio, Sept. 4, 1997) (crim. compl.).

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.* Federal prosecutors estimated a cost of fifty million dollars to develop the subject information. *Id.* Following the indictment, Avery Dennison filed an action under RICO, and froze defendants' assets. *Id.* The Yangs have since been under electronic monitoring in Cleveland. *Id.*

[36] *Id.* *See also* Dean Starkman, *Secret and Lies: The Dual Career of a Corporate Spy*, WALL ST. J., Oct. 23, 1997, at B1.

D. *The Taxol Case*[37]

In the Eastern District of Pennsylvania, a two-year FBI undercover operation resulted in the arrest last year of two employees of a Taiwanese company alleged to have offered cash payments in exchange for the secret formula for the anti-cancer drug Taxol, which had sales of $941 million in 1997 and is allegedly one of Bristol-Myers's most closely-guarded secrets.[38] After Kai-Lo Hsu and Jessica H. Chou of the Yueng Foong Paper Company expressed interest to an undercover FBI agent in obtaining the Taxol formula, a meeting was arranged between the defendants and a fictitious "corrupt scientist" at Bristol-Myers to discuss cash payments to the scientist.[39] The meeting took place at a Philadelphia hotel, where the agent was accompanied by an actual Bristol-Myers employee.[40] During the meeting, the defendants discussed their interest in acquiring technology that would advance their research efforts.[41] They were subsequently arrested and charged with attempt and conspiracy to receive trade secrets in violation of the EEA.[42]

The pretrial phase of the *Hsu* case demonstrates the classic tension in trade secrets litigation between preserving the secrecy of allegedly stolen trade secrets during litigation and the rules of pretrial discovery.[43] This tension is heightened in criminal cases, where defendants have a right to discover materials under both Rule 16 of the Federal Rules of Criminal Procedure and as a matter of constitutional law.

---

[37] United States v. Hsu, crim. 97-323 (E.D. Pa. 1997) (crim. compl.); (July 10, 1997) (crim. indictment). *See also* Francis A. McMorris, *Corporate-Spy Case Rebounds on Bristol,* WALL ST. J., Feb. 2, 1998, at B5.

[38] *See* United States v. Hsu. Crim. 97-323 (E.D. Pa. 1997) (crim. compl.); (July 10, 1998) (crim. indictment).

[39] *Id.* The "corrupt scientist" was a Bristol-Meyers employee who cooperated with the FBI. *Id.*

[40] *Id.*

[41] *Id.* The Bristol-Meyers scientist was asked several questions about Taxol's technology after viewing documents showing scientific data and technological processes. *Id.*

[42] *Id.* The indictment alleges that the documents were marked "Bristol-Meyers" and stamped "confidential." *Id.*

[43] *Id.*

At the outset of the *Hsu* case, the Government sought a protective order under the EEA[44] to limit the disclosure of Bristol-Myers documents, arguing that disclosure would reveal the very trade secrets that formed the basis of the prosecution. Prosecutors proposed an *in camera* review during which the court could redact documents containing confidential trade secrets.[45] The defendants proposed an alternative order that would require production of the information, but limit the disclosure of material designated by the Government as "confidential" only to individuals requiring access to the documents for defense purposes, such as defendants' attorneys, outside experts and prospective witnesses.[46]

The district court rejected the Government's application and adopted the order proposed by the defendants.[47] In reaching its conclusion, the court observed that denying defendants discovery of material deemed by the court to be "trade secrets" would "effectively be relieving the Government of the burden of proving one of the essential elements of its case: the existence of a trade secret."[48] The court emphasized that the determination of what constituted a "trade secret" was for the jury at trial and not the proper subject of a pretrial ruling by the court.[49] The court also suggested that denying the defendants the materials would violate

---

[44] *Id. See also* 18 U.S.C. § 1835 (1996). This section authorizes courts to issue orders as necessary to preserve the confidentiality of trade secrets and provides in pertinent part:

> 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.

*Id.*

[45] United States v. Hsu, 982 F. Supp. 1022, 1024 (E.D. Pa. 1997).

[46] *Id.* at 1023.

[47] *Id.* at 1029.

[48] *Id.* at 1024.

[49] *Id.*

their rights under the Confrontation Clause of the Sixth Amendment.[50]

On appeal, the Third Circuit reversed the district court's order.[51] The Court of Appeals observed that because the government charged the defendants only with an attempt and conspiracy to violate the EEA – and not with the completed offense of theft of trade secrets – the existence of a "trade secret" was not a required element of the charged offenses. In reaching this determination, the court held that "legal impossibility" is not a defense to attempted misappropriation of trade secrets or conspiracy to violate the EEA.[52] The court stated:

> [T]he government need not prove that an actual trade secret was used during an EEA investigation, because a defendant's culpability for a charge of attempt depends only on "the circumstances as he believes them to be," not as they really are. The government can satisfy its burden under § 1832(4) by proving beyond a reasonable doubt that the defendant sought to aquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such.[53]

The Court therefore concluded that the defendants had no constitutional or statutory right to view the unredacted portion of the Taxol documents. The case was remanded to the district court for an in camera review to assess whether the documents were properly redacted only to exclude confidential information and whether any of the redacted information was "material" to the defense.[54]

---

[50] *Id. See also* U.S. CONST. amend. VI. The Sixth Amendment provides in pertinent part: "In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and . . . to be confronted with the witnesses against him." *Id.*

[51] United States v. Hsu, 1998 WL 538221, 47 U.S.P.Q.2d 1784 (3d Cir. 1998).

[52] *Id.* at 8, 13.

[53] *Id.*

[54] *Id.* at 16.

E. *The Deloitte & Touche Case*[55]

Federal prosecutors in the Southern District of Texas charged Mayra Justine Trujillo-Cohen, a former employee of Deloitte & Touche (the accounting and management consulting firm) with violating the EEA by attempting to sell confidential Deloitte & Touche software programs.[56] Trujillo-Cohen was alleged to have downloaded the programs onto her personal laptop computer while employed by Deloitte & Touche and later to have engaged in negotiations to sell the software package to a company in New York for $7 million.[57] The indictment charges her with two counts of violating the EEA.[58]

F. *The Pei Case*[59]

In the District of New Jersey, an FBI investigation resulted in the arrest of Huang Doa Pei who is alleged to have attempted to steal trade secrets from his former employer, Roche Diagnostics ("Roche").[60] The criminal complaint alleges that Pei approached a Roche scientist to obtain confidential information about Roche's Hepatitis C diagnostic monitoring kit ("HCV Kit"). Pei allegedly intended to develop and market a HCV Kit for sale in China.[61] During recorded conversations, Pei allegedly stated that he intended to translate confidential Roche documents into Chinese, cut off relevant names and bring the documents to China.

Pei has since posted a $100,000.00 surety bond and is free on bail.

---

[55] United States v. Trujillo-Cohen, No. 97-251 (S.D. Tex., November 14, 1997) (crim. indictment).

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] United States v. Pei, No. 4090-01 (D.N.J. July 27, 1998) (crim. compl.).

[60] *Id.*

[61] *Id.*

## III. THE REUTERS/BLOOMBERG INVESTIGATION

The EEA may receive its most high-profile application in an investigation currently being conducted by federal prosecutors into whether an American subsidiary of Reuters Holdings P.L.C. stole trade secrets from its competitor, Bloomberg L.P. The investigation reportedly is focused on whether Reuters attempted to obtain the operating code used for a highly successful Bloomberg market data system for use in connection with a competing desktop product sold by Reuters. Although initial news reports suggested that Reuters may have participated in "electronic break-ins" of Bloomberg's computers,[62] more recent reports have suggested that a consultant hired by Reuters may have simply subscribed to the Bloomberg service and received information that was readily available to thousands of Bloomberg customers. The Reuters/Bloomberg matter may therefore raise novel questions concerning the scope of "reverse engineering" permitted by the EEA and the extent to which subscription agreements and other contractual restrictions imposed upon recipients of information may serve as the basis for a criminal prosecution under the EEA.

Although the EEA does not expressly address the issue of "reverse engineering," its legislative history suggests the law would not be violated "if a person can look at a product and, by using their own general skills and expertise, dissect the necessary attributes of the product."[63] Limitations on "reverse engineering" and disclosure of information also may be imposed by contractual restrictions on how recipients may use information.[64] Whether breaches of these types of contractual restrictions should rise to the level of criminal offenses, however, is not a settled issue.[65] A reasonable argument certainly can be made that the EEA was not intended to criminalize ordinary claims for breach of a subscription or license agreement. As one of the Bill's sponsors emphasized,

---

[62] *See, e.g.*, Kurt Eichenwald, *Reuters Unit Is Investigated Over Theft of a Rival's Data*, N.Y. TIMES, January 30, 1998, at A1 (discussing whether Reuters, a financial information and news giant, employed computer experts to pilfer confidential information from the computers of Bloomberg, a major rival).

[63] 142 CONG. REC. at S12212 (Managers' Statement).

[64] 142 CONG. REC. at S10886 (remarks of Sen. Kohl).

[65] *Id.*

the EEA was intended to reach only "flagrant and egregious cases of information theft."[66]

## IV. THE FUTURE OF THE EEA

Criminal prosecution under the EEA should proceed with caution. The statutory language gives prosecutors wide discretion to challenge a broad range of commercial activities, some of which either may be permitted under state trade secrets law or properly subject only to civil sanctions.[67] Attorney General Janet Reno recognized the potential danger of criminalizing the law of trade secrets by pledging to have all federal prosecutions under the EEA in its first five years specifically approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.[68]

Prosecutors are likely to continue to bring charges under the EEA in paradigm scenarios involving payments to a company "insider" in exchange for trade secrets, or breaking into a building or a secure computer system to obtain secret data -- the type of industrial espionage Congress clearly intended to curb. Cases lacking these elements -- such as those involving reverse engineering of widely distributed products or the interpretation of restrictive provisions of license or subscription agreements -- may be more appropriately resolved through civil litigation. A careful application of the EEA is necessary to strike the right balance between preventing the theft of secret information through acts of trespass, bribery, corruption or fraud, and permitting the reasonable study and use of available information to develop new and improved products without the threat of criminal sanctions.

---

[66] 142 CONG. REC. at S12212 (remarks of Sen. Kohl).

[67] *See* 18 U.S.C. § 1832(a) (1996).

[68] *See* Letter from Attorney General Janet Reno to Senator Orrin G. Hatch (October 1, 1996) (reprinted in 142 CONG. REC. at S12214).