The Economic Espionage Act of 1996: an Overview

George "Toby" Dilworth
Assistant United States Attorney
Computer and Telecommunications Coordinator
District of Maine

In January 1998, Caryn Camp was unhappy with her job at IDEXX Laboratories, a world-leading manufacturer of veterinary diagnostics products based in Maine. She started searching the internet for another job, and sent an email with her resume to a company called Wyoming DNAVaccine ("WDV"). Steven Martin, WDV's chief scientific officer, responded enthusiastically. Martin and Camp began corresponding regularly by email. Much of the early correspondence related to mundane topics about their lives in Maine and the west coast. However, as the correspondence progressed, Martin began emailing questions about IDEXX's manufacturing methods, customer base, and pricing schedule. Camp emailed her answers back to Martin. After Camp expressed reservations about sending information to Martin and WDV, a potential competitor to IDEXX, Martin emailed her claiming that he did "not want to know anything confidential about IDEXX." He said he only wanted public information.

After a brief hiatus, Martin resumed his questions regarding IDEXX's procedures. He inquired about IDEXX's flourescent-based tests, as well as its customer base. If Camp did not know the answers to Martin's questions, she researched them. She emailed him information about ongoing negotiations between IDEXX and a possible acquisition target, and shipped him copies of customer lists, manufacturing documents, and laboratory reports. On July 24, she mailed him the last shipment -- a box filled with operating manuals, research and development data, and information about other competitors in the industry. She spent that evening doing her laundry and packing for an extended vacation to California, where she planned to attend a family reunion and meet Martin for the first time. She wrote Martin a message describing the materials she had sent him, predicting that he would "feel like a kid on Christmas day" when he saw the contents. However, because she was tired and it was late at night, she made a terrible mistake. As she prepared to send the message, she went to the address book on her computer and inadvertently clicked on the address for John Lawrence, IDEXX's global marketing director. Lawrence's name was directly above Martin's name in her address book. Camp immediately realized her error, and tried in vain to delete the message. She left for California the following morning, hoping that Lawrence would not read the message. Lawrence found Camp's email meant for Martin and IDEXX notified the U.S. Attorney's Office. In short order, the FBI executed search warrants at Camp's home in Maine, and then Martin's home and office in California.

So began *United States v. Camp and Martin*, CR 98-48-P-H (D.Me., Indictment filed Sept. 16 1988), one of the first cases brought under the Economic Espionage Act. Although the defendants were not well-funded and did not employ sophisticated espionage techniques, and IDEXX had taken substantial steps to protect its trade secrets, the defendants managed to make off with important proprietary information. They probably would have avoided detection except for Camp clicking on the wrong address in the early morning of July 25. Like other biotech companies, IDEXX had spent considerable resources developing these trade secrets. That a competitor could obtain them without incurring any costs posed substantial risks to IDEXX.

Over the past 40 years, extraordinary technological advances have improved lives and created economic growth. High speed communications systems, novel medical devices, and robotics are just a few examples. Most of these technological advances are based on trade secrets -- proprietary information which the owner keeps confidential.

Ironically, high tech advances have made it more difficult to protect those trade secrets. Vast amounts of information can be stored and transferred electronically without serious risk of detection. No longer does

a disgruntled employee have to carry boxes of confidential files past the guard at the front door, nor does a competitor have to bribe an insider to deliver proprietary information. An unhappy employee or opportunistic licensee can abscond with a company's most important trade secrets simply by downloading them onto a floppy disk and walking out the front door with the disk in his pocket, or he can remain in his office and e-mail the information to a ready buyer. A competitor can steal trade secrets by gaining unauthorized access to the company's computers without ever leaving his home or office.

By 1996, Congress recognized the serious economic risks created by the theft of trade secrets from American companies. A 1995 survey of 325 companies determined that nearly half of them had experienced a trade secret theft. S. Rep. No. 104-359 (1996). It was estimated that nearly $24 billion of corporate intellectual property was stolen every year. *United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998). The FBI suspected that more than twenty countries were actively trying to steal United States companies' trade secrets. Some warned that the end of the Cold War "sent government spies scurrying to the private sector to perform illicit work for businesses and corporations." *Id*. As the nation's workforce became more mobile, employees used their former employers' trade secrets for the benefit of their new employers, who had spent nothing to develop the information. Federal prosecutors often had difficulty fitting trade secret cases within the existing federal statutes. The National Stolen Property Act, 18 U.S.C. § 2314, did not apply to the theft of purely intellectual property. *See Dowling v. United States*, 473 U.S. 207, 216 (1985); *United States v. Brown*, 925 F.2d 1301, 1307-08 (10th Cir. 1991). Mail and wire fraud statutes did not always apply. The only federal statute explicitly targeting the theft of trade secrets was limited to government employees' unauthorized disclosure of trade secrets, and offenders were subject only to misdemeanor penalties. 18 U.S.C. § 1905. States lacked the resources to investigate these crimes, and faced substantial jurisdictional hurdles. While more than 40 states had enacted some form of the civil Uniform Trade Secrets Act (UTSA), there was no effective criminal response to the problem.

Recognizing that intellectual property will play an increasingly important role in the national economy, and the ease with which it can be stolen and converted, Congress enacted the Economic Espionage Act of 1996 (the EEA), Pub. L. No. 104-294, 110 Stat. 3488. Congress intended the EEA to prohibit every type of trade secret theft, "from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics." H.R. Rep. No. 104-788 (1996).

The EEA does not restrict competition or lawful innovation. According to the First Circuit, the EEA "was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It *was*, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere." *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000) (emphasis in original). Under the EEA, federal prosecutors have the means to help protect proprietary economic information. When he signed the bill, President Clinton predicted that the EEA "will protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secrets theft and deter and punish those who would intrude into, damage or steal from computer networks." President William J. Clinton, Presidential Statement on the Signing of the Economic Espionage Act of 1996 (Oct. 11, 1996) *available at* 1996 WL 584924.

I. Two Distinct Parts

The EEA contains two distinct provisions. One addresses economic espionage directed by foreign governments or government-controlled entities. 18 U.S.C. § 1831. The other prohibits the commercial theft of trade secrets carried out for economic or commercial advantage, whether the perpetrator is foreign or domestic. 18 U.S.C. § 1832. While Congress apparently believed that foreign agents posed the greatest risk to American businesses and imposed more severe penalties against them, all of the prosecutions brought to date under the EEA have utilized section 1832. Because federal prosecutors have charged section 1832 more frequently, this article will address it first.

A. Section 1832: Theft of Trade Secrets for Economic or Commercial Advantage

Under section 1832, the Government must prove beyond a reasonable doubt that: (1) the defendant stole, or without the owner's authorization obtained, sent, destroyed, or conveyed information; (2) the defendant knew or believed that the information was a trade secret; (3) the information was in fact a trade secret; (4) the defendant intended to convert the trade secret to the economic benefit of somebody other than the owner; (5) the defendant knew or intended that the owner of the trade secret would be injured; and (6) the trade secret was related to, or was included in, a product that was produced or placed in interstate or foreign commerce. It is also illegal to attempt to steal a trade secret, or to receive, purchase, destroy, or possess a trade secret which the defendant knew was stolen. 18 U.S.C. §§1832(a)(2) - (4).

Unlike most other types of property, a trade secret may be stolen without ever leaving the custody or control of its owner. Congress recognized this fact, and prohibited copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying trade secrets. 18 U.S.C. § 1832(a)(2). The defendant must have acted "without authorization" from the owner. Accordingly, an employee or licensee who has authorization to possess a trade secret during the regular course of employment violates the EEA if he or she transfers it without the owner's permission. *See* 142 Cong. Rec. S12,212 (daily ed. Oct. 2, 1996) ("authorization is the permission, approval, consent or sanction of the owner" to transfer a trade secret).

1. Knowledge: The government does not have to prove the defendant definitely knew the information was a trade secret. "For a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is proprietary." 142 Cong. Rec. S12,213 (daily ed. Oct. 2, 1996). Evidence that a defendant knew the owner marked the documents "confidential" or "proprietary," restricted access to the information, and required personnel to sign non-disclosure agreements is solid proof of this element. *Martin*, 228 F.3d at 12. A person who takes a trade secret because of ignorance, mistake, or accident, or who reasonably believes that the information is not proprietary, is not liable under the EEA.

2. Definition of a Trade Secret: The definition of a trade secret is broader under the EEA than under state civil statutes and the Uniform Trade Secrets Act, and includes both tangible property and intangible information. *Martin*, 228 F.3d at 11. It protects:

all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if --

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, or not being readily ascertainable through proper means by, the public.

18 U.S.C. § 1839(3). The EEA "protects a wider variety of technological and intangible information than current civil laws," although "it is clear that Congress did not intend . . . to prohibit lawful competition such as the use of general skills or parallel development of a similar product." *Hsu*, 155 F.3d at 196-97. Moreover, while the civil definition requires that the trade secret is not known by business people or competitors, the EEA's definition requires only that the information not be known or ascertainable by the general public. *Id*.

An important issue at any trade secret trial is the owner's effort to maintain the secrecy of the information. A non-exhaustive list of the relevant factors includes whether the owner:

kept and enforced clear policies about the confidential information;

trained its employees, consultants, and licensees regarding the proprietary information;

required employees, consultants, and licensees to sign confidentiality and nondisclosure agreements;

limited physical access to areas where the trade secrets were kept;

restricted the number of copies of certain documents;

kept hard copies of the documents on colored paper so they were difficult to photocopy;

encrypted trade secrets kept in electronic form; and

restricted access to certain electronic files and data on a "need to know" basis.

The owner's security measures do not have to be absolute, but must be reasonable under the circumstances. 18 U.S.C. § 1839(3)(A). In addition, the information cannot be readily ascertainable through observation or reverse engineering.

Information disclosed to licensees, vendors, or third parties for limited purposes may still be a trade secret. *Rockwell Graphic Systems v. DEV Industries*, 925 F.2d 174, 177 (7th Cir. 1991). Non-disclosure agreements can protect companies and retain the information's trade secret status. Information can lose its status through legal filings and the issuance of a patent. However, refinements and enhancements of the technology set out in a patent may qualify as trade secrets if they are not reasonably ascertainable from the published patent. *United States v. Hsu*, 185 F.R.D. 192, 201 (E.D.Pa. 1999). The EEA's definition of a trade secret is not unconstitutionally vague, although a district court has expressed concerns about determining what is "generally known" and "reasonably ascertainable." *United States v. Hsu*, 40 F. Supp. 2d 623, 630 (E.D.Pa. 1999). According to the opinion,

what is 'generally known' and 'reasonably ascertainable' about ideas, concepts, and technology is constantly evolving in the modern age. With the proliferation of the media of communication on technological subjects, and (still) in so many languages, what is 'generally known' or 'reasonably ascertainable' to the public at any given time is necessarily never sure.

Id. The district court questioned whether information on the Internet or discussed at scientific conferences is readily ascertainable or generally known. *Id.*

The trade secret can be "minimally novel," but some element must be unknown to the public. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974). Not every part of the information needs to qualify as a trade secret, and a trade secret may include a combination of elements which are generally known to the public. "[A] trade secret can include a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the claimant a competitive advantage which is protected from misappropriation." *Rivendell Forest Products v. Georgia Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994).

3. Independent Economic Value: The trade secret must derive "independent economic value . . . from not being generally known to . . . the public." 18 U.S.C. § 1839(3)(B). There is no minimum jurisdictional amount, however.

4. Economic Benefit to a Third Party: The government must prove that the theft was intended for the economic benefit of a person other than the rightful owner. A person who steals a trade secret but does

not intend anyone to gain financially from the theft does not violate section 1832. This element is not included in section 1831. In section 1831, the benefit may be non- economic.

5. Intent to Injure the Owner: The government is not required to prove malice or evil intent, but only that the defendant knew or intended that the offense would injure the owner. *Hsu*, 155 F.3d at 196. Proof of a defendant's plan to use the information to create a more successful competitor against the trade secret owner satisfies this element. *Martin*, 228 F.3d at 12.

6. Interstate or Foreign Commerce: The government must prove that the trade secret was "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832. This term is not unconstitutionally vague. *Hsu*, 40 F. Supp. 2d at 627. The element should not be difficult to determine for products already in the marketplace. However, the element may be more problematic where the trade secrets relate to products in the development stage.

7. Customer lists: A customer list may be a trade secret under the EEA's definition. In *Martin*, the First Circuit stated that a customer list "had the potential to fall within the § 1839 definition of trade secret." *Martin*, 228 F.3d at 12 n.8. There, the evidence showed that the owner had devoted considerable resources generating and updating the lists, which included all of the relevant details about the customers in a defined and narrow market. However, customer lists are not trade secrets where they can be compiled by general marketing efforts, or where the base of customers is neither fixed nor small. *Nalco Chemical Co. v. Hydro Technologies*, 984 F.2d 801, 804 (7th Cir. 1993); *Standard Register Co. v. Cleaver*, 30 F. Supp. 2d 1084, 1095 (N.D. Ind. 1998).

8. Penalties: A person convicted under section 1832 can be imprisoned for up to ten years and fined $250,000, and an organization can be fined up to $5,000,000. 18 U.S.C. §§ 1832(a) and (b). The applicable guideline is USSG § 2B1.1. Calculating the loss is oftentimes difficult. In some cases, the value of the trade secret may be determined by what the defendant sought to pay for it, or by the cost of a legitimate licensing agreement. Value is far more difficult to determine when the information relates to a small part of a larger process, or the product to which the trade secret relates has not made it to the marketplace. The cost of the research and development for the information, and the "thieves market" theory are potential methods of determining the value.

Prosecutors should understand that the risk of divulging the trade secret may be greatest at the sentencing stage, as the nature of the trade secret is an important factor. Even under the Uniform Trade Secrets Act, courts have recognized that "the general law and the proper measure of damages in a trade secret case is far from uniform." *Telex Corp. v. IBM*, 510 F.2d 894, 930 (10th Cir. 1975).

B. Section 1831: Foreign Economic Espionage

Section 1831 was "designed to apply only when there is 'evidence of foreign government sponsored or coordinated intelligence activity.'" *Hsu*, 155 F.3d at 195 (quoting 142 Cong.Rec. S12,212 (daily ed. Oct. 2, 1996)). Under section 1831, the government must prove that: (1) the defendant stole, or without the owner's authorization obtained, destroyed, or conveyed information; (2) the defendant knew or believed that this information was a trade secret; (3) the information was a trade secret; and (4) the defendant intended or knew that the offense would benefit a foreign government, instrumentality, or agent. The term "foreign instrumentality" means "any agency, bureau, component, institution, association, or any legal, commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1). The legislative history reveals that, in this context, "substantial" means "material or significant, not technical or tenuous." 142 Cong.Rec. S12,212 (daily ed. Oct. 2, 1996).

We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns ten percent of a company

exempt it from scrutiny. Rather, the pertinent inquiry is whether the activities of the company are, from a practical and substantive viewpoint, foreign government directed.

Id. The term "benefit" is to be interpreted broadly, and is not limited to economic gains. H.R. Rep. No. 788, 104th Cong. (1996).

Unlike section 1832, section 1831 does not require the government to prove that a defendant intended to convert the trade secret to the economic benefit of another, that the defendant intended or knew that the offense would injure the owner, or that the trade secret was related to a product in interstate or foreign commerce. The other proof elements have been discussed previously.

1. Extraterritoriality: Both sections 1831 and 1832 may control acts committed outside the country. The EEA applies if the offender is a citizen or resident alien of the United States, or an organization organized under the laws of the United States or any state. 18 U.S.C. § 1837.

2. Penalties: Congress imposed a greater penalty on those who steal trade secrets on behalf of foreign agents. A person convicted of violating section 1831 is subject to a term of imprisonment of up to 15 years and a fine of $500,000. 18 U.S.C. § 1831(a). An organization convicted under section 1831 faces a fine of not more than $10,000,000. *Id.* at § 1831(b).

II. Conspiracies

The EEA prohibits conspiracies to steal trade secrets. In order to prevail, the government must prove: (1) that an agreement existed; (2) that it had an unlawful purpose; (3) that the defendant was a voluntary participant; (4) that the defendant possessed both the intent to agree and the intent to commit the substantive offense; and (5) that at least one co-conspirator took an affirmative step toward achieving the conspiracy's purpose. *Martin*, 228 F.3d at 11; *Hsu*, 155 F.3d at 202. It is irrelevant whether the defendant actually received a trade secret. *Martin*, 228 F.2d at 13. It is sufficient to prove that the conspirators agreed to convey information "that potentially fell under the definition of a trade secret in 18 U.S.C. § 1839." *Id*. Legal impossibility is not a defense to a conspiracy charge. *Hsu*, 155 F.3d at 203. Prosecutors should recognize the advantages of charging conspiracy wherever possible, as there are fewer elements to prove and there is a reduced risk the trade secrets will be disclosed during the litigation.

III. Preserving Confidentiality of Trade Secrets During Litigation

Congress recognized the practical problem faced in all trade secret cases -- litigation to protect the trade secret could actually lead to the disclosure of the trade secret during the course of the trial. A defendant who has tried to obtain trade secrets by stealth and fraud might, after indictment, gain access to the same information through the federal discovery rules. Congress wanted to protect trade secrets during the litigation without infringing upon a defendant's rights, so it included a provision directing that a 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 requirement" of the applicable federal rules and laws. 18 U.S.C. § 1835. This confidentiality provision "represent[s] a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." *Hsu*, 155 F.3d at 197. The confidentiality provision was also intended to encourage victims to report thefts, as it provides some assurance that the trade secret will not be divulged during the litigation. *Id.*

The *Hsu* case is instructive. There, the indictment charged that the defendants contacted an FBI agent posing as a technological information broker and directed him to purchase information about an anti-cancer drug. *Hsu*, 155 F.3d at 192. The undercover agent announced that he had found a corrupt employee of the drug manufacturer, and arranged a meeting with the defendants. *Id*. At that meeting, the supposedly corrupt employee showed company documents which contained trade secrets and were marked "confidential." *Id.* at 192-93. As part of discovery, the defense requested a copy of the documents shown to the defendants during the meeting. *Id.* at 193. The trial court adopted the defendant's proposal

that the proprietary information would only be disclosed to select members of the defense team, and any documents filed with the court containing the information would remain under seal. *Id.* at 193. The trial court also encouraged the government to file an interlocutory appeal, as permitted under section 1835. *Id.* at 194. The Third Circuit reversed, holding that the defendant should not obtain access to the trade secrets because they were only charged with conspiring to violate the EEA. *Id.* at 199. The Circuit Court reasoned that because impossibility is not a defense to the conspiracy charge, whether the documents contained actual trade secrets and the nature of the trade secrets themselves were irrelevant. *Id.*

At a minimum, prosecutors should require the defendant, counsel, and any experts retained by the defendant to sign confidentiality agreements protecting all proprietary information. Federal prosecutors and law enforcement agencies do not need to sign protective orders with victims before accepting trade secret information, however. 18 U.S.C. § 1833.

The government may file an interlocutory appeal from an order authorizing or directing the disclosure of trade secrets. 18 U.S.C. § 1835. Since delaying the trial during an interlocutory appeal will usually help only the defendant, prosecutors should ensure that there are procedures in place to limit the chance that actual trade secrets will be discussed in open court. Prosecutors can more readily restrict disclosure when they charge a defendant only with conspiring or attempting to steal trade secrets, since the government does not have to prove that the information was actually a trade secret. *Hsu*, 155 F.3d at 203-04. In fact, in attempt and conspiracy cases, the government might not even offer in evidence any documents containing actual trade secrets. Department guidelines require the Deputy Attorney General's approval before a federal prosecutor can request that a courtroom be sealed. *See* 28 C.F.R. § 50.9; *U.S. Attorney's Manual* § 9-5.150.

IV. Forfeiture

The EEA provides that a court "shall" order the forfeiture of any proceeds or property derived from the violation, and may order the forfeiture of any property used to commit or facilitate the commission of the crime, "taking into consideration the nature, scope, and proportionality of the use of the property in the offense." 18 U.S.C. § 1834(a). With certain exceptions, the procedures set out in 21 U.S.C. § 853 govern the forfeiture proceedings.

V. Department of Justice Oversight

Responding to Congressional concerns that prosecutors might misapply the EEA, the Department of Justice agreed to require that all prosecutions under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. 28 C.F.R. § 0.64-5. This regulation, which remains in effect until October 11, 2001, applies to the filing of complaints, indictments, and informations, but not to search warrant applications. The Computer Crime and Intellectual Property Section ("CCIPS") coordinates requests for approval of cases under section 1832. In cases involving charges under section 1831, CCIPS consults with the Internal Security Section.

VI. Conclusion

It is hard to overstate the threat posed by the theft of proprietary information. The Computer Security Institute stated recently that "theft of proprietary information is perhaps the greatest threat to United States economic competitiveness in the global marketplace." The theft of trade secrets can affect any economic sector; high tech companies are not the only ones concerned about somebody stealing their trade secrets. *See Shurgard Storage Centers v. Safeguard Self Storage*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (in civil action, plaintiff alleged that defendant systematically hired key employees away for purpose of obtaining plaintiff's trade secrets). As the workforce becomes ever more mobile, and as other countries strive to compete by any means necessary, the threat will persist. The EEA provides prosecutors with an effective tool to combat this threat from whatever source -- a sophisticated foreign agency or an unhappy employee like Caryn Camp.

ABOUT THE AUTHOR

Toby Dilworth graduated from Yale University and Boston College Law School with honors. After serving as a law clerk for U.S. District Judge Gene Carter, he joined a private firm in Portland, Maine. He became an Assistant United States Attorney for the District of Maine in 1991. He now serves as the Computer and Telecommunications Coordinator in the Portland office. He is also an adjunct faculty member at the University of Maine Law School, where he teaches trial practice.