

THE CRIMINALIZATION OF TRADE SECRET THEFT: THE ECONOMIC ESPIONAGE ACT OF 1996

Pamela B. Stuart

I.	BACKGROUND.....	374
II.	THE DIMENSIONS OF THE PROBLEM	375
III.	DOESN'T EVERYBODY DO IT?	376
IV.	THE ECONOMIC ESPIONAGE ACT OF 1996.....	377
	A. <i>Penalties for Criminal Violations</i>	377
	B. <i>Civil Remedies</i>	378
	C. <i>Extraterritorial Application of the EEA</i>	378
	D. <i>Economic Espionage and Trade Secret Theft Defined</i>	378
	E. <i>The EEA Does Not Preempt Other Laws</i>	381
	F. <i>Protecting the Trade Secret from Disclosure in Litigation</i>	382
	G. <i>Enforcement Actions To Date</i>	382
	1. <i>United States v. Worthington</i>	382
	2. <i>United States v. Kai-Lo Hsu</i>	382
	3. <i>United States v. Steven Louis Davis</i>	383
V.	CONCLUDING THOUGHTS	384

The collapse of the Soviet Union has resulted in far-reaching changes in the global environment. One of the immediate effects of the demise of what Ronald Reagan dubbed the Evil Empire was the need to

* Pamela B. Stuart is a Washington attorney who represents corporations and individuals in criminal and civil matters. She prosecuted fraud cases at the Federal Trade Commission (1973-79), served as an Assistant United States Attorney, and advised United States prosecutors while at the Office of International Affairs of the Department of Justice (1985-87). In 1987, Ms. Stuart entered private practice. She has directed international corporate investigations and asset searches. She has also represented individuals in complex white collar criminal, extradition, and prisoner transfer matters. She also handles commercial, medical malpractice, employment, and health care litigation. She is a proponent of the use of experienced former prosecutors to prepare cases for prosecution against corporations. Ms. Stuart appears frequently as a legal commentator on CNN's *Burden of Proof*. She has also appeared on *Cochran & Company* (Court T.V.), NBC's *Today*, *Rivera Live*, *Both Sides With Jesse Jackson*, and other television programs focusing on legal topics. Ms. Stuart is a member of the bars of the District of Columbia, Florida, Maryland, New York, and Virginia. She is a 1970 graduate of Mount Holyoke College and a 1973 graduate of the University of Michigan Law School.

find useful work for the army of FBI agents who formerly were assigned to counter-intelligence. Because they would no longer be sitting for hours in unmarked vehicles in full surveillance mode, those agents were available for reassignment. According to intelligence agencies, FBI agents were not the only ones looking for work. The reduction in East-West tensions enabled intelligence services in allied nations to devote greater resources to collecting sensitive United States economic information and technology.

While its full implications are not yet apparent, the passage of the Economic Espionage Act of 1996 might be viewed as the FBI agent full employment act. The government will now make use of sophisticated investigators hitherto employed at rooting out spies, waste, fraud, abuse, and other criminal activities in an effort to protect something else that is vital to our national security and prosperity — the nation's trade secrets. It is yet one more step in the progress of the effort to criminalize conduct that was formerly of interest only to commercial lawyers.

I. BACKGROUND

The Economic Espionage Act of 1996, 18 U.S.C. § 1831 *et seq.*, became effective on October 11, 1996. Its passage was prompted by concern over the efforts of foreign businesses and governments to conduct industrial espionage against United States businesses both at home and abroad. United States intelligence reports established that there was a continuing threat of economic espionage that was emanating mostly from such allies as France, Japan, and Israel. Oddly enough, the businesses most routinely at risk were those in the defense industry. Apparently the R&D costs involved in home-grown defense technology were too high for our foreign friends. Rather, they wanted cutting-edge weapon systems technology at a cut-rate price.

The Act also provided American businesses with the prospect of federal assistance in the effort to prevent competitors from stealing their intellectual property. While twenty six states had legislation on the books to prevent trade secret theft, the federal law provides protection for businesses in the states without appropriate legislation and provides another option for aggrieved businesses in the states where trade secret acts were already in place. The federal law does not preempt or displace other remedies.¹

1. 18 U.S.C. § 1838 (1996).

II. THE DIMENSIONS OF THE PROBLEM

A 1994 Report to Congress on Foreign Acquisition of and Espionage Activities Against United States Critical Technology Companies reported that the intelligence organization of one ally ran an espionage operation that paid a United States government employee to obtain United States classified military intelligence documents. Citizens of that ally were found to be stealing sensitive United States technology used in manufacturing artillery gun tubes within the United States. Other agents of that ally stole design plans for a classified reconnaissance system from a United States company and gave them to a defense contractor in their home country. A company based in the territory of the ally was suspected of surreptitiously monitoring a Defense Department telecommunications system in order to obtain classified information for the intelligence organization of its government. Citizens of that country were investigated for passing advanced aerospace design technology to unauthorized scientists and researchers.

According to the 1994 report, another country that did not maintain its own intelligence service relied on private companies to do that kind of work. Those firms operate abroad and collect data for their own purposes, but also gather classified documents and corporate proprietary information for the use of their government. For example, electronics firms from that nation directed their data gathering efforts at United States firms in order to increase the market share of companies in that country in the semiconductor industry. With friends like that, who needs enemies?

The magnitude of the problem is substantial. The White House Office of Science and Technology estimated that business espionage cost United States companies \$100 billion annually in lost sales.² The most likely targets are companies involved in one or more of the technologies named on its National Critical Technologies List (NCTL). These include sophisticated manufacturing technology, materials, information, and telecommunications. Also included are biotechnology, aeronautics, surface transportation, energy, and environmental technologies. Loss of proprietary information related to these products would be likely to undermine the United States strategic industrial position according to the FBI.

According to the National Counterintelligence Center and the State Department, seventy-four corporations reported more than 400 incidents of suspected foreign intelligence incursions against their business last year.

2. Ed Jopeck and Ken Sawka, *Foreign Espionage: Is your Business at Risk?* (visited Oct. 30, 1997) <<http://www.execpc.com/~mhalign/indict.html>> .

Slightly more than half of these incidents involved technologies on the NCTL. So, much of American commercial activity is potentially at risk.

III. DOESN'T EVERYBODY DO IT?

The CIA has repeatedly denied that the Agency will engage in corporate spy work.³ However, apparently if the information turns up, the Agency will pass it along to interested parties. The CIA is reportedly providing the government with information about Japanese auto technology that may be of support to President Clinton's effort, in cooperation with Ford, General Motors, and Chrysler, to produce a more fuel-efficient car through the Partnership for a New Generation of Vehicles. While much of the data on the current state of auto technology abroad may be gathered from publicly available sources, some of it is gathered clandestinely and is classified. Battery technology in Japan is of particular interest according to Matt Dzieciunch, a project engineer at the government-Big Three cooperative effort known as the United States Advanced Batteries Consortium.⁴

For the most part, American companies do not need the government's help to spy on their competitors. The vast majority of business and competitive information may be obtained legally and ethically from newspaper articles, trade publications, SEC filings, specialized databases, and from materials readily available at trade shows. Sensitive or restricted data include financial information, manufacturing processes, customer lists, and other information not normally shared with those outside a business.

The CIA has long monitored data on such world economic issues as oil production, crops, world trade, foreign government economic policies, and technology. After the Clinton Administration formed the National Economic Council in January 1993, the CIA's role in economic intelligence grew in support of enhancing United States competitiveness in the world. By forming a cooperative among the Big Three auto makers, the government facilitated the sharing of information gathered through foreign industrial spying. When Stansfield Turner was Director of Central Intelligence, the agency would brief United States corporations about its findings of the acquisition plans of foreign governments through seminars at the Commerce Department. Information sharing has been practiced with private defense contractors under a number of administrations. Laws designed to permit American companies to gain access to the work product

3. Robert Dreyfuss, *Company Spies, Mother Jones Mo Jo Wire* (visited Oct. 30, 1997) <<http://www.mojones.com/motherjones/MJ94/dreyfuss.html>>.

4. *Id.*

of United States government laboratories and to avail themselves of cooperative ventures without fear of the antitrust regulators also facilitated United States government assistance to the military-industrial complex.⁵

IV. THE ECONOMIC ESPIONAGE ACT OF 1996

The Act treats those who steal on behalf of a foreign government or knowing that the offense will benefit a foreign government, foreign instrumentality, or foreign agent differently from those who merely appropriate trade secrets or business information for domestic use. It also punishes organizations who engage in the prohibited skullduggery more harshly than individuals.

A. Penalties for Criminal Violations

Those who steal trade secrets with the intent or knowledge that they are doing so for or will benefit the foreign entities or agents may be imprisoned up to fifteen years and fined not more than \$500,000. If an organization gets into the foreign intrigue business and steals trade secrets, it makes itself liable for a fine not to exceed ten million dollars.

Those who merely want to rob Apple to benefit Bill Gates will be imprisoned not more than ten years or fined not more than the schedule in 18 U.S.C. § 3571 (1987) permits or both. An organization that limits the influence of its thefts to United States territory may be fined not more than \$500,000.

Perhaps of more far-reaching significance, the Economic Espionage Act includes a provision that permits the forfeiture to the United States of:

any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of the violation; and any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of the offense⁶

The forfeiture provisions make such forfeiture an option within the discretion of the court, as part of the sentencing process, "taking into consideration the nature, scope, and proportionality of the use of the property in the offense."⁷ Thus, it is within the power of the court to order what in effect would be a corporate death sentence for a new company

5. *Id.*

6. 18 U.S.C. § 1834 (a)(1), (a)(2) (1996).

7. 18 U.S.C. § 1834 (a)(2) (1996).

established on the basis of purloined information in the possession of its founders.

B. Civil Remedies

Of course, in the business context, the conniving trade secret thief must be concerned about civil suits, which can result in injunctive relief to stop the production line, damages, seizure of unjust profits as well as attorneys fees. This has been the traditional means of stopping the unlawful conversion of trade secrets. Prior to the enactment of the Economic Espionage Act of 1996, twenty six states had anti-trade secret theft laws on the books. Common law theft and conversion statutes also applied.

The Economic Espionage Act of 1996 permits the Department of Justice to get involved on the civil side as well,⁸ and it provides that the Attorney General may obtain appropriate injunctive relief against any violation of the Act in federal district court.

C. Extraterritorial Application of the EEA

This power potentially may have far-reaching effects, as the law provides that it is applicable to conduct outside the United States if the offender is a United States citizen or permanent resident alien or an organization organized under the laws of the United States government or a state government or an act in furtherance of the offense was committed in the United States.⁹ Thus, if a multinational corporation incorporated in Delaware engages in trade secret theft in England or hires someone to do the evil deed abroad on its behalf after a meeting in the company's offices in New York to plan the theft, the offense may be punished in the United States.

Likewise, if an American investigator is hired by a foreign company to commit economic espionage abroad, he may be prosecuted in the United States (as well as in the country where the crime was committed, assuming that country prohibits trade secret theft).

D. Economic Espionage and Trade Secret Theft Defined

A *trade secret* is defined as:

all forms and types of financial, business, scientific, technical, economic, or engineering information, including

8. 18 U.S.C. § 1836 (1996).

9. 18 U.S.C. § 1837 (1996).

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—

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

the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.¹⁰

Thus, in order for the theft to be actionable under this law, the owner must have taken some measures that objectively would be reasonable under the circumstances to protect the confidentiality of the trade secret information at issue, and the government must demonstrate that the secret has some economic value as a result of its confidentiality. Thus, it behooves corporate America to add to the compliance programs established to mitigate any punishment imposed under the Federal Sentencing Guidelines for Organization a program of trade secret protection. Attorneys who practice in this field will have to figure out what is *reasonable* in terms of protection and will have to keep up with what the courts are saying on the subject. On the defensive side, the company caught in this sort of conduct may wish to minimize the protective efforts of its competitive adversary in order to demonstrate that what appeared to be a trade secret was really readily available and thus, not a trade secret.

The intent required in order to be guilty of criminal conduct under the act is different, depending upon whether the theft has foreign ramifications or not. For economic espionage to be actionable under 18 U.S.C. §1831(a) (the foreign economic espionage offense), the offending individual or entity must have taken the trade secret knowingly “intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent.”¹¹ For the domestic theft of trade secrets offense, 18 U.S.C. §1832(a), the offender must knowingly have

10. 18 U.S.C. § 1839 (3)(A), (3)(B) (1996).

11. 18 U.S.C. §1831(a) (1996).

intent to convert a trade secret, that is related to or included in a produce that is produced for or placed in interstate or foreign commerce, to the economic benefit or anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret.¹²

Thus, for a conviction of the domestic trade secret crime, the government must show not only the theft but also, in effect, that the theft would damage the owner and would economically benefit someone other than the owner. The government must also show that the theft occurred with respect to a product that is in interstate commerce.

In this regard, the Fifth and Seventh Circuits have articulated a doctrine of *inevitable disclosure* of trade secrets in subsequent employment, which simplifies proof of what is a theft. Under this theory, a change of employment will result in a theft of a trade secret when the two employers involved are competitors; the new position taken by the departing employee is comparable to or would inevitably involve knowledge gained in the previous position; the new employer did not do enough to protect against disclosure of trade secrets, and there was some evidence of intent to disclose trade secrets.¹³ The First and Eighth Circuit have considered and rejected the doctrine.¹⁴

The law also will punish those who receive, buy, or possess the stolen trade secret information, knowing that it has been stolen or obtained without authorization.¹⁵ Attempts and conspiracies to commit trade secret theft are also offenses under the Act.¹⁶

It is unclear what the status of reverse engineering will be under this new statute. Silicon Valley entrepreneurs have made fortunes by moving from company to company and using their knowledge acquired on their previous job for the benefit of their new employers. A disgruntled former employer, when anticipating a suit, for example, for sex discrimination, might launch a pre-emptive strike by suing for theft of trade secrets under the Economic Espionage Act. Likewise, when a group of disgruntled auto mechanics leaves dealership A for more remunerative

12. 18 U.S.C. §1832(a) (1996).

13. See *Union Carbide Corp. v. UGI Corp.*, 731 F.2d 1186, 1192 (5th Cir. 1984); *PepsiCo Inc. v. Redmond*, 54 F.3d 1262, 1268 (7th Cir. 1995).

14. See *Campbell Soup Co. v. Giles*, 47 F.3d 467 (1st Cir. 1995) and *IBM Corp. v. Seagate Technology, Inc.*, 1991 U.S. Dist. Lexis 20406 (D. Minn. 1991), *remanded for a more specific statement of relief*, 962 F.2d 12 (8th Cir. 1992).

15. 18 U.S.C. § 1832 (a)(3) (1996).

16. 18 U.S.C. § 1832 (a)(4), (5) (1996).

work at dealership B and makes off with the list of loyal service customers, dealership B may end up vicariously liable if the new employees send out marketing letters to their old customers.

It is notable that this statute is broader in scope than most previous trade secret laws. By covering *business information*, the act covers data that may not be economically useful except by a competitor seeking financial information or expansion plans or other corporate intelligence. It also covers attempts to steal trade secrets and conspiracies to steal trade secrets.¹⁷

Perhaps because of the ambiguities of the statute and the situations to which it might be applied, Attorney General Janet Reno personally assured Senator Orrin Hatch prior to passage of the law that for five years following its effective date, any prosecution undertaken pursuant to the Act would have to be personally approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General in charge of the Criminal Division. Traditional standards of case selection are likely to be applied in determining whether to go forward with a particular prosecution. Thus, the Department is likely to look at the economic value of the damage to the victim from the theft, the clarity of the proof of criminal intent, the measures in place to protect the secrecy of the information purloined, and the availability of civil remedies to redress the harm short of prison, huge fines, and forfeiture.

E. The EEA Does Not Preempt Other Laws

The statute provides that it should not be construed as preempting or displacing any other civil or criminal remedies provided by any United States federal, state, commonwealth, possession, or territorial law for the misappropriation of trade secrets. It also does not affect the disclosure of information under the Freedom of Information Act.¹⁸

Thus, a corporate victim of trade secret theft may have an array of possible avenues of retaliation available to it. Attorneys must be careful, however, in selecting the remedies and considering a possible call to the FBI or the Department of Justice, not to run afoul of state bar ethical rules by improperly threatening criminal prosecution in order to gain advantage in an ongoing civil matter. It would be better to merely alert the FBI and let the government's investigation take its course without threatening the other side.

17. 18 U.S.C. § 1832(a)(4), (5) (1996).

18. 5 U.S.C. § 552 (1996).

F. Protecting the Trade Secret from Disclosure in Litigation

The statute anticipates that the proof of the offense may require the disclosure, in whole or in part, of the hitherto secret and valuable trade secret information. Corporate counsel should seek the benefit of 18 U.S.C. § 1835 and petition the court at the outset of the matter for an order to preserve the confidentiality of the trade secrets at issue. Should the court not understand the sensitivity of the issue and order its disclosure, the United States has the right to lodge an interlocutory appeal with the Court of Appeals to forestall such missteps.

G. Enforcement Actions To Date

1. United States v. Worthington¹⁹

Patrick Worthington, a maintenance supervisor at PPG Industries' fiberglass research center, misappropriated diskettes, blueprints and other types of confidential research information and offered them to the chief executive officer of Corning Glass, which is PPG's chief competitor. The Corning Glass CEO alerted PPG and the FBI. An undercover FBI agent met with Worthington and his brother, Daniel, to provide them with a \$1,000 down payment for the trade secrets. Both Patrick and Daniel Worthington were indicted under the Economic Espionage Act.²⁰ Patrick Worthington pled guilty and was sentenced on June 5, 1997 to fifteen months in jail. His brother, Daniel, who was in the deal for \$100, was sentenced to five years probation, including six months of home detention.

2. United States v. Kai-Lo Hsu²¹

Kai-Lo Hsu, a technical director for Taiwan's Yuen Foong Paper Co., and Chester S. Ho, a biochemist and professor at a university in Taiwan, were arrested as part of an FBI sting operation at the Four Seasons Hotel in Philadelphia on June 14, 1997. An agent, posing as a corrupt Bristol-Myers scientist and a technology information broker, met with Mr. Kai-Lo Hsu and Mr. Ho. The objective was to steal trade secrets relating to Bristol Myers' anti-cancer drug, Taxol. Reportedly Mr. Ho was present at the meeting to verify the value of the Taxol technology which was confidential while Kai-Lo Hsu and Jessica Chou agreed to pay

19. R. Mark Halligan, *Reported Criminal Arrests Under the Economic Espionage Act of 1996* (visited Mar. 28, 1998) <<http://www.execpc.com/~mhalign/indict.html>> (citing *United States v. Worthington*, Criminal No. 97-9 (W.D. Pa. 1996)).

20. 18 U.S.C. § 1832(a)(1), (3), (5) (1996).

21. Halligan, *supra* note 19 (citing *United States v. Kai-Lo Hsu*, Criminal No. 97-323 (E.D. Pa. 1997)).

\$400,000 for it. Ms. Chou is reportedly in Taiwan which does not have an extradition treaty with the United States. Kai-Lo Hsu and Chester Ho have been indicted under 18 U.S.C. § 1832(a)(4) for attempted theft of trade secrets and 18 U.S.C. § 1832(a)(5) for conspiracy to steal trade secrets.

3. United States v. Pin Yen Yang²²

Pin Yen Yang and his daughter, Hwei Chen Yang (a/k/a Sally Yang) were arrested on September 4, 1997 at Cleveland's airport as they were about to embark on a trip to New York. Mr. Yang, age seventy, is the president of Four Pillars Enterprise Company, Ltd. of Taiwan. The company manufactures and sells pressure-sensitive products in Taiwan, Malaysia, the People's Republic of China, Singapore, and the United States. Sally Yang is an officer of the company which has more than 900 employees and annual revenues of more than \$150 million. The arrest followed conversations by Mr. Yang and his daughter with an employee of Avery Dennison Corporation, of Pasadena, California, which manufactures adhesive products such as postage stamps and mailing labels. The Yangs wanted to obtain Avery's trade secrets from the employee, who worked at Avery Dennison Corporation's facility in Concord, Ohio. The Avery employee cooperated with the FBI. Federal prosecutors estimate that the research and development costs expended to develop the information obtained by the defendants from Avery Dennison prior to their arrest at between \$50 and \$60 million. The Yangs were charged with mail and wire fraud, conspiracy to steal trade secrets under the Economic Espionage Act, money laundering, and receipt of stolen goods under 18 U.S.C. §§ 1341, 1343, 1832, 1956, and 2315 (1994).

4. United States v. Steven Louis Davis²³

Steven Davis, a process control engineer for Wright Industries in Nashville was assigned to be the lead process control engineer when Gillette Company retained Wright Industries to assist in developing a new generation of razor systems. After working on the project for a few months, Wright Industries, at the request of Gillette, removed Davis from the project in late September 1996. Davis thereafter sent highly confidential engineering drawings to competitors of Gillette, including Bic Corporation, American Safety Razor, and Warner Lambert. Davis contacted potential purchasers by facsimile and E-mail and represented that he had 600 megs of Gillette's product, equipment, and assembly drawings for sale. In addition to violations of the Economic Espionage Act, 18

22. United States v. Pin Yen Yang, Criminal No. 1:97MG0109 (N.D. Ohio 1997).

23. United States v. Steven Louis Davis, (M.D. Tenn. 1997).

U.S.C. § 1832(a)(2) and (3), Davis has been charged with wire fraud under 18 U.S.C. § 1343.

V. CONCLUDING THOUGHTS

The Economic Espionage Act of 1996 is one more step in the relentless march of the Congress toward criminalizing behavior hitherto considered the subject for civil litigation only. The Act provides a powerful new tool to protect the industrial and intellectual patrimony of corporate America. It also raises the stakes when a company fires an employee or hires a disgruntled employee of a competitor, acquires another company in the same or a related industry, or even when it trains its own employees on internal trade secrets. Corporate counsel should well develop procedures to guard against inadvertent violations.