HEINONLINE

Citation: 2 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 1 2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Sat Apr 20 11:17:18 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

Calendar No. 546

104TH CONGRESS
2d Session

SENATE

REPORT
104–359

THE INDUSTRIAL ESPIONAGE ACT OF 1996

AUGUST 27, 1996.—Ordered to be printed

Filed under authority of the order of the Senate of August 2, 1996

Mr. HATCH, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany S. 1556]

The Committee on the Judiciary, to which was referred the bill (S. 1556) to amend provisions of title 18, United States Code, with respect to the prohibition of industrial espionage, and for other purposes, having considered the same, reports favorably thereon, with an amendment in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose	4
II. Legislative history	4
III. Discussion	5
IV. Section-by-section analysis	13
V. Regulatory impact statement	18
VI. Cost estimate	18
VII. Changes in existing law	19

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

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

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds that—

(1) sustaining a healthy and competitive national economy is imperative;

(2) the development and production of proprietary economic information involves every aspect of interstate commerce and business;

29–010

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 1 2002

(3) the development, production, protection, and lawful exchange, sale, and transfer of proprietary economic information is essential to maintaining the health and competitiveness of interstate commerce and the national economy;

(4) much proprietary economic information moves in interstate and foreign commerce and proprietary economic information that does not move in interstate or foreign commerce directly and substantially affects proprietary economic information that does;

(5) the theft, wrongful destruction or alteration, misappropriation, and wrongful conversion of proprietary economic information substantially affects and harms interstate commerce, costing United States firms, businesses, industries, and consumers millions of dollars each year; and

(6) enforcement of existing State laws protecting proprietary economic information is frustrated by the ease with which stolen or wrongfully appropriated proprietary economic information is transferred across State and national boundaries.

(b) PURPOSE.—The purpose of this Act is—

(1) to promote the development and lawful utilization of United States proprietary economic information produced for, or placed in, interstate and foreign commerce by protecting it from theft, wrongful destruction or alteration, misappropriation, and conversion; and

(2) to secure to authors and inventors the exclusive right to their respective writings and discoveries.

SEC. 3. PREVENTION OF ECONOMIC ESPIONAGE AND PROTECTION OF PROPRIETARY ECONOMIC INFORMATION IN INTERSTATE AND FOREIGN COMMERCE.

(a) IN GENERAL.—Title 18, United States Code, is amended by inserting after chapter 89 the following new chapter:

"CHAPTER 90—PROTECTION OF PROPRIETARY ECONOMIC INFORMATION

"Sec.
"1831. Definitions.
"1832. Criminal activities affecting proprietary economic information.
"1833. Criminal forfeiture.
"1834. Import and export sanctions.
"1835. Extraterritoriality.
"1836. Construction with other laws.
"1837. Preservation of confidentiality.
"1838. Prior authorization requirement.
"1839. Law enforcement and intelligence activities.

"1831. Definitions

"As used in this chapter:

"(1) The term 'person' means a natural person, corporation, agency, association, institution, or any other legal, commercial, or business entity.

"(2) The term 'proprietary economic information' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, procedures, programs, codes, or commercial strategies, whether tangible or intangible, and whether stored, complied, or memorialized physically, electronically, graphically, photographically, or in writing that—

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

"(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable, acquired, or developed by legal means by the public.

The term does not include any knowledge, experience, training, or skill that a person lawfully has acquired due to his work as an employee of or as an independent contractor for any person.

"(3) The term 'owner' means the person or persons in whom, or United States Government component, department, or agency in which, rightful legal, beneficial, or equitable title to, or license in, proprietary economic information is reposed.

"(4) The term 'United States person' means—

"(A) in the case of a natural person, a United States citizen or permanent resident alien; and

"(B) in the case of a nonnatural person, an entity substantially owned or controlled by the United States Government or by United States citizens or permanent resident aliens, or incorporated in the United States.

"(5) The term 'without authorization' means not permitted, expressly or implicitly, by the owner.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 2 2002

"1832. Criminal activities affecting proprietary economic information

"(a) Any person, with intent to, or reason to believe that it will, injure any owner of proprietary economic information having a value of not less than $100,000 and with intent to convert it to his or her own use or benefit or the use or benefit of another, who 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);

"(5) wrongfully solicits another to commit any offense described in paragraphs (1) through (3); or

"(6) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined up to $250,000, or twice the value of the proprietary economic information, whichever is greater, or imprisoned not more that 10 years, or both.

"(b) Any corporation that commits any offense described in paragraphs (1) through (6) of subsection (a) shall be fined up to $10,000,000, or twice the economic value of the proprietary economic information, whichever is greater.

"(c) This section does not prohibit the reporting of any suspected criminal activity or regulatory violation to any appropriate agency or instrumentality of the United States, or a political subdivision of a State, or to Congress.

"1833. Criminal forfeiture

"(a) Notwithstanding any provision of State law, any person convicted of a violation under this chapter shall 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.

"(b) the court, in imposing a sentence on such person, shall order, in addition to any other sentence imposed pursuant to this chapter, that the person forfeit to the United States all property described in this section.

"(c) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsection 413(d) which shall not apply to forfeitures under this section.

"(d) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this section remaining after the payment of expenses and sale authorized by law.

"1834. Import and export sanctions

"(a) The President may, to the extent consistent with international agreements to which the United States is a party, prohibit, for a period of not longer than 5 years, the importation into, or exportation from, the United States, whether by carriage of tangible items or by transmission, any merchandise produced, made, assembled, or manufactured by a person convicted of any offense described in section 1832 of this title, or in the case of an organization convicted of any offense described in such section, its successor entity or entities.

"(b)(1) The Secretary of the Treasury may impose on any other person who knowingly violates any order of the President issued under the authority of this section, a civil penalty equal to not more than 5 times the value of the exports or imports involved, or $100,000, whichever is greater.

"(2) Any merchandise imported or exported in violation of an order of the President issued under this section shall be subject to seizure and forfeiture in accordance with sections 602 through 619 of the Tariff Act of 1930.

"(3) The provisions of law relating to seizure, summary and judicial forfeiture, and condemnation of property for violation of the United States customs laws, the disposition of such property or the proceeds from the sale thereof, the remission or mitigation of such forfeiture, and the compromise of claims, shall apply to seizures and forfeitures incurred, or alleged to have been incurred under this section to the

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 3 2002

extent that they are applicable and not inconsistent with the provisions of this chapter.

"1835. Extraterritoriality

"(a) This chapter applies to conduct occurring within the United States.

"(b) This chapter applies to conduct occurring outside the territorial and special maritime jurisdiction of the United States, its territories, and possessions if—

"(1) the offender is a United States person; or

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

"1836. Construction with other laws

"This chapter shall not be construed to preempt or displace any other Federal or State remedies, whether civil or criminal, for the misappropriation of proprietary economic information, or to affect the otherwise lawful disclosure of information by any government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

"1837. Preservation of confidentiality

"In any prosecution under this chapter, the court may enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of proprietary economic information, consistent with rule 16 of the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, and other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing the disclosure of proprietary economic information.

"1838. Prior authorization requirement

"The United States may not file a charge under this chapter or use a violation of this chapter as a predicate offense under any other law without the personal approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division of the Department of Justice.

"1839. Law enforcement and intelligence activities

"This chapter does not prohibit any and shall not impair otherwise lawful activity conducted by any agency or instrumentality of the United States, a State, or a political subdivision of a State, or an intelligence agency of the United States.".

(b) TECHNICAL AMENDMENT.—The table of chapters for title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following new item:

"90 Protection of Proprietary Economic Information .... 1831".

SE

SEC. 4. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS.

Section 2516(1)(a) of title 18, United States Code, is amended by inserting "chapter 90 (relating to economic espionage and protection of proprietary economic information in interstate and foreign commerce)," after "title:".

I. PURPOSE

The Industrial Espionage Act of 1996, S. 1556, would provide for Federal criminal penalties for the theft, unauthorized appropriation, or other misuse of proprietary economic information.

II. LEGISLATIVE HISTORY

The basis for the protection of proprietary economic information is rooted in the U.S. Constitution, which explicitly grants Congress the power "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries," U.S. Const. art. I, sec. 8, cl. 8, and which also gives Congress the power "[t]o regulate Commerce * * * among the several States." U.S. Const. art. I, sec. 8, cl. 3.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 4 2002

The goal of this legislation is to punish the theft, unauthorized appropriation, or unauthorized dissemination of proprietary economic information.

This legislation was introduced by Senators Kohl and Specter on February 1, 1996, in the 104th Congress. On February 28, 1996, the Subcommittee on Terrorism, Technology and Government Information held a hearing jointly with the Select Committee on Intelligence on the measure and the general issue of the theft of proprietary economic information. The Director of the Federal Bureau of Investigation, Louis Freeh, testified. The Committee also heard testimony from Geoffrey Shaw, the former CEO of Ellery Systems, Inc., of Boulder, CO, and Dr. Raymond Damadian, president and chairman of Fonar Corporation of Melville, NY. In addition, written statements were received from John J. Higgins, senior vice president and general counsel of the Hughes Electronics Corp.; Norman Augustine, president and CEO of Lockheed Martin Corp.; and the National Information Infrastructure Testbed. A classified briefing by the FBI Director for members of the Judiciary and Intelligence Committees was held on March 13, 1996. The House Committee on the Judiciary, Subcommittee on Crime, also held hearings on this issue on May 9, 1996.

On July 25, 1996, the Judiciary Committee met in executive session to consider the bill. The Committee unanimously approved the measure, with an amendment in the nature of a substitute, proposed by Senators Kohl and Specter. Embodied in the substitute amendment were several changes to the original text of the bill. The first was a change in the definition of "owner" intended to bring the bill into full accord with the General Agreement on Trade and Tariffs. The second was a change in the definition of "proprietary economic information" designed to clarify the scope of the definition. The third was a change in the elements of the offense designed to clarify the exact nature of the act criminalized. The fourth was a reduction in the possible prison term in order to align the penalties with those available under the National Stolen Property Act, 18 U.S.C. 2314. The fifth was an alteration in the available fines in order to allow fines be levied in relation to the value of the stolen information. The sixth was an alteration in the import and export sanctions provisions in order to clarify the procedures for their use. The seventh narrowed the extraterritorial application of the legislation. The eighth was the requirement of prior authorization by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division of the Justice Department before a prosecution under the measure can be commenced.

III. Discussion

Congress has heretofore confined its protection of intellectual property to patented and copyrighted material. With this legislation, Congress extends the protection of Federal law to the equally important area of proprietary economic information. During the course of the Committee's hearings, we documented that proprietary economic information is vital to the prosperity of the American economy, that it is increasingly the target of thieves, and that

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 5 2002

our current laws are inadequate to punish people who steal the information.

In a world where a nation's power is now determined as much by economic strength as by armed might, we cannot afford to neglect to protect our intellectual property. 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. But our Federal criminal laws do not recognize this and do not punish the information thief. This is an unacceptable oversight. The Industrial Espionage Act is an effort to remedy the problem.

GROWING IMPORTANCE OF PROPRIETARY ECONOMIC INFORMATION

The United States produces the vast majority of the intellectual property in the world. This includes patented inventions, copyrighted material, and proprietary economic information. Proprietary information, in contrast with copyrighted material and patented inventions, is secret. The value of the information is almost entirely dependent on its being a closely held secret. It includes, but is not limited to, information such as production processes, bid estimates, production schedules, computer software, technology schematics, and trade secrets. It is, in short, the very information that drives the American economy. For many companies this information is the keystone to their economic competitiveness. They spend many millions of dollars developing the information, take great pains and invest enormous resources to keep it secret, and expect to reap rewards from their investment.

In the last few decades, intangible assets have become more and more important to the prosperity of companies. A recent analysis by the Brookings Institute indicates that in 1982, the tangible assets of mining and manufacturing companies accounted for 62 percent of their market value. By 1992, they represented only 38 percent of the market value. Blair, "Ownership and Control: Rethinking Corporate Governance for the Twenty-First Century", 234 n.57 (1995). As this Nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow. Ironically, the very conditions that make this proprietary information so much more valuable make it easily stolen. Computer technology enables rapid and surreptitious duplications of the information. Hundreds of pages of information can be loaded onto a small computer diskette, placed into a coat pocket, and taken from the legal owner.

This material is a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft. The information is pilfered by a variety of people and organizations for a variety of reasons. A great deal of the theft is committed by disgruntled individuals or employees who hope to harm their former company or line their own pockets. In other instances, outsiders target a company and systematically infiltrate the company then steal its vital information. More disturbingly, there is considerable evidence

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 6 2002

that foreign governments are using their espionage capabilities against American companies.[1]

We use the term economic or industrial espionage advisedly. Espionage is typically an organized effort by one country's government to obtain the vital national security secrets of another country. Typically, espionage has focused on military secrets. But even as the cold war has drawn to a close, this classic form of espionage has evolved. Economic superiority is increasingly as important as military superiority. And the espionage industry is being retooled with this in mind.

It is important, however, to remember that the nature and purpose of industrial espionage are sharply different from those of classic political or military espionage. When we use the phrase industrial espionage, we include a variety of behavior—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, to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics. All of these forms of industrial espionage are troubling, and they are punished as the theft of proprietary economic information in this measure.

INCREASING INCIDENTS OF THEFT OF PROPRIETARY ECONOMIC INFORMATION

Director Freeh testified at the Subcommittee's February hearing that "[f]oreign governments * * * actively target U.S. persons, firms, industries, and the U.S. Government itself to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage." Director Freeh reported that in the last year, the number of cases of economic espionage that the FBI is investigating doubled from 400 to 800. Twenty-three countries are involved in those cases.

During 1992 hearings before the House Committee on the Judiciary, Subcommittee on Economic and Commercial Law, the Director of the Central Intelligence Agency, Robert Gates, stated that:

> Our fundamental assessment is that while the end of the Cold War did not bring an end to the foreign intelligence threat, it did change the nature of that threat. The threat has become more diversified and more complex. In a world that increasingly measures national power and national security in economic terms as well as military terms, many foreign intelligence services around the world are shifting the emphasis in targeting. Foreign targeting of American technology continues; technology is important for economic as well as military reasons. Since the U.S. continues to be on the cutting edge of technological innovation, technology theft will remain a major concern for us.

[1] S. 1556 was introduced in tandem with S. 1557, "The Economic Security Act of 1996" S 1557, which was referred to the Select Committee on Intelligence, specifically addresses the problem of foreign government-sponsored theft of proprietary economic information. S. 1557 includes enhanced penalties when the theft is sponsored by a foreign government. On April 30, 1996, the Intelligence Committee favorably reported a measure almost identical to S. 1557 as title V of S. 1718, "The Intelligence Authorization Act for Fiscal Year 1997."

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 7 2002

"The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings Before the Subcomm. on Economic and Commercial Law of the House Comm. on the Judiciary," 102d Cong., 2d sess. 59 (1977).

A report of the National Counterintelligence Center in 1995 indicated that biotechnology, aerospace, telecommunications, computer software, transportation, advanced materials, energy research, defense, and semiconductor companies are all top targets for foreign economic espionage. These sectors are "aggressively targeted" according to the report. "National Counterintelligence Center, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage," 15 (1995). That report identified 20 different methods used to conduct industrial espionage. The traditional methods include recruiting an agent and then inserting the agent into the target company, or breaking into an office to take equipment and information. According to the report, "computer intrusions, telecommunications targeting and intercept and private-sector encryption weaknesses * * * account for the largest portion of economic and industrial information lost by U.S. corporations." Id. at 16. Most American companies are poorly prepared to deal with these sophisticated and coordinated efforts to obtain their proprietary economic information.

But even as American companies are attempting to deal with foreign espionage, they also have to deal with theft by insiders. A survey by the American Society for Industrial Security of 325 companies in 1995 found that almost half of them had experienced trade secret theft of some sort during the previous two years. Heffernan and Smartwood, "Trends in Intellectual Property Loss Survey," 4 (1996). They also reported a 323-percent increase in the number of incidents of intellectual property loss. Id. A 1988 National Institute of Justice study of trade secret theft in high technology industries found that 48 percent of 150 research and development companies surveyed had been the victims of trade secrets theft. Mock and Rosenbaum, "A Study of Trade Secrets Theft in High-Technology Industries," National Institute of Justice Discussion Paper 6 (1988). Almost half of the time the target was research and development data while 38 percent of the time the target was new technology. Id. at 16. Forty percent of the victims found out about the theft from their competitors. Id.

The Committee has learned of several disturbing examples of how this theft is occurring. For example, in Arizona, an engineer for an automobile air bag manufacturer was arrested in 1993 for selling manufacturing designs, strategies, and plans. He asked the company's competition for more than half a million dollars—to be paid in small bills. And he sent potential buyers a laundry list of information they could buy. He asked $500 for the company's capital budget plan; $1,000 for a piece of equipment; and $6,000 for planning and product documents. See "Industrial Espionage By 2 Mesa Men Alleged," the Phoenix Gazette, Aug. 31, 1993, at A1. The engineer subsequently reached a plea agreement with the U.S. Government and was sentenced to less than 6 months in prison.

Just last year, Bill Gaede, the former employee of two major computer companies, admitted to stealing vital information on the manufacture of microchips and selling it to China, Cuba, and Iran.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 8 2002

For almost a decade, he copied manufacturing specifications worth millions of dollars. And armed with this material, the Chinese, Cubans, and Iranians have been able to close the gap on our technology leads. Late last year, the FBI arrested this man and charged him under the Federal stolen property and mail fraud laws. See "Troubling Issues in a Silicon Valley Spy Case," the New York Times, July 8, 1996, at D1. Gaede has recently reached a plea agreement with the U.S. Government.

During its hearings, the Committee learned how an employee of Ellery Systems in Boulder, CO, transmitted that company's source code to another person in what appeared to be an attempt to appropriate the source code for his own personal use. Ellery Systems was a computer firm that supplied software technology to various government projects, primarily in NASA astrophysics activities. That theft of their source code, possibly at the behest of a foreign government, ultimately destroyed the financial viability of Ellery Systems. But all efforts to prosecute the putative thief failed because of gaps in current law.

Dr. Raymond Damadian, the inventor of magnetic resonance imaging technology and founder of an MRI manufacturing company, Fonar Corp., told the Committee that his company had been the subject of persistent infiltration and theft. In one case, an unauthorized service company hired former Fonar engineers to give them the proprietary technology—the diagnostic software and schematics—needed to service Fonar MRI machines. When Fonar discovered the misappropriation, it sought an injunction in Federal court. The injunction was issued, but the service company simply violated the injunction, flouting all possible penalties.

Director Freeh told the Committee about an FBI investigation involving the theft of proprietary information from two major pharmaceutical manufacturers. Two people were offering to sell trade secrets involving two fermentation processes covered by active patents. In February 1990, an FBI undercover agent posed as a potential buyer and was offered the information on one process for $1.5 million. The second process was for sale for $6 to $8 million.

As a result of industrial espionage, American companies have been severely damaged. The NCIC report concluded that "[i]ndustry victims have reported the loss of hundreds of millions of dollars, lost jobs, and lost market share." NCIC, supra, at 16. The ASIS survey concluded that the potential losses could total $63 billion. Heffernan and Smartwood, supra, at 15.

In response to the growing problem of the theft of proprietary economic information, the FBI has shifted the focus of its Development of Espionage, Counterintelligence and Counterterrorism Awareness (DECA) Program. This program has been in place for more than 20 years. But in the last few years, DECA has widened its efforts to address industrial espionage. DECA coordinators in each of the FBI's 56 field offices maintain contact with companies in their region and now regularly brief them about methods and prevention of industrial espionage. During the 1993 and 1994 fiscal years, the FBI briefed almost 20,000 companies under the DECA Program.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 9 2002

GAPS IN CURRENT FEDERAL LAW

Developments in the law, however, have not kept pace with this rapidly changing environment. Although Congress has enacted patent and copyright protection laws, and computer crime statutes, no Federal law protects proprietary economic information from theft and misappropriation in a systematic, principled manner. As a result, prosecutors have had trouble shoe-horning economic espionage into these laws. Sometimes they have succeeded, but often they have failed. See Toren, "The Prosecution of Trade Secrets Thefts Under Federal Law," 22 Pepp. L. Rev. 59, 64–94 (1994).

One provision Federal prosecutors have attempted to use is the Depression-era National Stolen Property Act, 18 U.S.C. 2314–15. This law was designed to foil the "roving criminal" whose access to automobiles made movement of stolen property across State lines so easy that State and local officials were stymied in their pursuit. While the law works well enough for crimes involving traditional "goods, wares, and merchandise," it was drafted at a time when computers, biotechnology, and copy machines did not even exist. Consequently, it is not particularly well suited to deal with situations in which intangible information alone is wrongfully duplicated and transmitted electronically with a few keystrokes.

Moreover, recent court decisions suggest that this statute is limited to tangible property. In *Dowling* v. *United States,* 473 U.S. 207 (1985), the Supreme Court reversed the conviction of a man who had distributed bootlegged Elvis Presley records. He violated copyright law, but the Court suggested that the National Stolen Property Act only applies to tangible goods. Id. at 216. Later appellate courts have interpreted *Dowling* to preclude prosecution of the theft of "purely intellectual property." *United States* v. *Brown,* 925 F.2d 1301, 1307 (10th Cir. 1991). We do not address whether these cases properly understood the legislative intent of the National Stolen Property Act, but merely point out that this caselaw makes prosecutions for the theft of proprietary economic information under the act difficult, making the need for this legislation more and more urgent.

Other existing statutes used by law enforcement agencies to combat economic espionage have similar limitations. Although proprietary information is property under the mail and wire fraud statutes, 18 U.S.C. 1341–43, see *U.S.* v. *Carpenter,* 484 U.S. 19, 28 (1987), prosecutors have found it difficult to use these statutes because the theft often does not involve the use of mail or wire. In addition, since a thief merely copies information and does not necessarily "defraud" the company permanently of the data, prosecutions are more difficult.

Under many Federal statutes, even basic concepts can prove problematic. For example, if an individual "downloads" computer source code without permission of the owner, has a theft occurred even though the true owner never lost possession of the original and is not permanently deprived of its use? Another difficulty with existing law is that it fails to afford explicit protection to the confidential nature of the information in question during enforcement proceedings. By its nature, proprietary economic information derives value from its exclusivity and confidentiality. If either or both

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 10 2002

are compromised during legal proceedings, the value of the information is diminished.

As a result of these problems, the FBI has had difficulty conducting investigations or had prosecutions declined. Director Freeh pointed to one case in which an association of consultants, all of whom were long-term employees of U.S. corporations, attempted to sell proprietary high technology to foreign powers. The FBI sought consensual monitoring of a subject. Its request was turned down by an Assistant U.S. Attorney, citing *Brown* as holding that the consultants' actions did not constitute criminal behavior. Director Freeh pointed to another example in which the FBI investigated an information broker who was engaged by two foreign companies to gather proprietary bid information from a major U.S. company regarding a multimillion dollar international construction project. The information broker contacted several employees from the U.S. company, paid them for information, and passed the information onto the foreign companies. The broker was then paid a large sum of money for his services. For lack of a more applicable violation, the case was investigated as a wire fraud violation, but a U.S. Attorney's office declined to prosecute. Significantly, a similar investigation regarding the same construction project and foreign companies was initiated in the United Kingdom. This investigation resulted in prison sentences for two other information brokers headquartered in England.

STATE LAWS INADEQUATE

State laws do not fill in the gaps left by Federal law. 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 chose to forgo civil suits because the thief is essentially judgment proof—a young engineer who has few resources—or too difficult to pursue—a sophisticated foreign company or government. In addition, companies often do not have the resources or the time to bring suit. They also frequently do not have the investigative resources 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.

NEED FOR A COMPREHENSIVE FEDERAL LAW

These, and other problems, underscore the importance of developing a systematic approach to the problem of economic espionage. Only by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security. Foremost, we believe that the greatest benefit of the Federal statute will be as a powerful deterrent. In addition, a Federal criminal law is needed

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 11 2002

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.

S. 1556 DOES NOT APPLY TO GENERAL KNOWLEDGE AND SKILLS

This legislation does not apply to innocent innovators or to individuals who seek to capitalize on their lawfully developed knowledge, skill or abilities. Employees, for example, who change employers or start their own companies should be able to apply their talents without fear of prosecution because two safeguards against overreaching are built into the law.

First, protection is provided by the definition of "proprietary economic information" itself. The definition requires that an owner take objectively reasonable, proactive measures, under the circumstances, to protect the information. If, consequently, an owner fails to safeguard his or her proprietary information, then no one could be rightfully accused of misappropriating it. Most owners do take reasonable measures to protect their proprietary economic information, thereby placing employees and others on clear notice of the discreet, proprietary nature of the information.

The bill explicitly states that the term proprietary economic information does not include the general knowledge, skills or experience that a person has. A prosecution under this statute must establish a particular piece of information that a person has stolen or misappropriated. It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was exposed to proprietary economic information while employed. A prosecution that attempts to tie skill and experience to a particular piece of proprietary economic information cannot succeed without showing that the particular material was stolen or misappropriated. The Government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his tenure with a company. Allowing such prosecutions to go forward and allowing the risk of such charges to be brought would unduly endanger legitimate and desirable economic behavior.

As the Pennsylvania Supreme Court noted in *Spring Steels* v. *Molloy,* 400 Pa. 354, 363 (1960):

> It is not a phenomenal thing in American business life to see an employee, after a long period of service, leave his employment and start a business of his own or in association with others. And it is inevitable in such a situation, where the former employee has dealt with customers on a personal basis that some of those customers will want to continue to deal with him in [that] new association. This is * * * natural, logical and part of human fellowship * * *

This legislation does not criminalize or in any way hamper these natural incidents of employment. The free and unfettered flow of

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 12 2002

individuals from one job to another, the ability of a person to start a new business based upon his or her experience and expertise, should not be injured or chilled in any way by this legislation. Individuals must have the opportunity to take advantage of their talents and to seek and accept other employment that enables them to profit from their abilities and experience. And companies must have the opportunity to employ these people. This measure attempts to safeguard an individual's career mobility and at the same time to preserve the proprietary economic information that underpins the economic viability of the very company that would offer a person a new job.

The second safeguard is provided by the bill's use of the term "knowingly." For a person to be prosecuted, the person must know or have a firm belief that the information he or she is taking is in fact proprietary. Under theft statutes dealing with tangible property, normally, the thief knows that the object he has stolen is indeed a piece of property that he has no lawful right to convert for his personal use. The same principle applies to this measure—for someone to be convicted under this statute he must be aware or substantially certain that he is misappropriating proprietary economic information (although a defense should succeed if it is proven that he actually believed that the information was not proprietary after taking reasonable steps to warrant such belief). A person who takes proprietary economic information because of ignorance, mistake or accident cannot be prosecuted under the act. (The bill also provides a similar safeguard by requiring that the appropriation be without authorization.)

This requirement should not prove a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their proprietary economic information. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.

IV. Section-by-Section Analysis

SECTION 1. SHORT TITLE

This section sets forth the short title of the Act, which emphasizes that the focus of the bill is on "industrial espionage" and the protection of trade secrets. "Industrial espionage" means activity directed at the U.S. Government or U.S. corporations, establishments, or persons for the purpose of unlawfully obtaining proprietary economic information. The emphasis of this legislation is on the theft of that proprietary economic information.

SECTION 2. FINDINGS AND PURPOSE

This section sets forth the congressional findings upon which the Act is predicated and the remedial purposes of the Act. The section reflects congressional determinations that the development and production of trade secrets is integral to the maintenance of a healthy and competitive national economy and that, in turn, maintenance of a competitive national economy is imperative to national security. This section also recognizes that the Constitution grants Congress the power to protect and enforce the exclusive rights of authors and inventors to their writings and discoveries. One of the

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 13 2002

Act's purposes is, therefore, to promote the development and lawful utilization of proprietary economic information by protecting it from theft, unauthorized misappropriation or conversion. Notwithstanding the holding of *Dowling* v. *United States*, 473 U.S. 207 (1985), it is intended that the provisions of the Act should apply regardless of whether the conduct at issue could also fall within the prohibitions of the copyright laws.

SECTION 3. PREVENTION OF INDUSTRIAL ESPIONAGE

This section is the core component of the Act and would add a new Chapter "90—Protection of Proprietary Economic Information" to title 18, United States Code.

§ 1831. Definitions

This section sets forth definitions of certain key items used in the new chapter and builds upon the definitions already set out in chapter 1 of title 18.

(a) "Person" is defined to include both individuals and entities, such as corporations, agencies, and associations.

(b) "Proprietary economic information" is defined as a type of intellectual property connoted by four characteristics: (1) it is proprietary; (2) its nature is economic, business, scientific, technical, or engineering; (3) it consists of information, data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, procedures, programs, codes, or commercial strategies; and (4) it derives value from its exclusivity. These features distinguish it from other forms of intellectual property, such as literary or artistic works. Both tangible and intangible forms of property and all forms of data or information are covered, regardless of how stored or memorialized. Additionally, the definition makes clear that the owner of the property must have taken objectively reasonable and proactive steps to keep the information confidential; that is, information or data that is available generally to the public is not included. The efforts to protect material, however, need not be heroic merely reasonable. The term "proprietary economic information" also does not include general knowledge, experience, training, or skill acquired by a person as a result of his or her employment or hire by any owner.

This definition is closely modeled on the definition of a "trade secret" used in the Uniform Trade Secrets Act. It parallels similar definitions used by many States in their own trade secrets legislation. Thus, it is familiar to most firms, businesses, and individuals who commonly deal with trade secrets and intellectual property. Congress intends to draw upon the considerable case law and experience interpreting "trade secrets" to illuminate the meaning of the term "proprietary economic information."

(c) "Owner" is defined to include any person, including the U.S. Government, having legal, beneficial, or equitable title to, or license in, the proprietary economic information in question.

(d) "U.S. Person" is defined to mean U.S. citizens or permanent resident aliens in the case of natural persons; and, in the case of nonnatural persons, entities substantially owned or controlled by the U.S. Government or by U.S. citizens or permanent resident aliens, or incorporated in the United States.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 14 2002

(e) "Without authorization" is defined to mean without permission of the owner. It is intended to emphasize that innocent or negligent actors cannot be prosecuted under the statute. See, in this regard, the additional comments regarding section 1832 in the Discussion and below.

§ 1832. Criminal activities affecting proprietary economic information

This section punishes the theft, unauthorized appropriation, and unauthorized conversion, duplication, alteration, or destruction of proprietary economic information. This section is written to cover both traditional instances of theft, where the object of the crime is removed from the rightful owner's control and possession, as well as nontraditional methods of misappropriation and destruction, involving electronic duplication or alteration. With these nontraditional methods the original property never leaves the dominion or control of the rightful owner, but the unauthorized duplication or misappropriation effectively destroys the value of what is left with the rightful owner. In an electronic environment, information can be stolen without asportation, and the original usually remains intact. Our intent, therefore, is to ensure that the theft of intangible information is prohibited in the same way that theft of physical items are protected.

This section requires that the person intends that his actions will injure the owner of the information. This does not require that the prosecution prove malice or evil intent. It merely requires that the actor knew or was aware to a practical certainty that his conduct would cause such a result. The actor must intend to use the information for his or her personal benefit or the benefit of another. By benefit we mean economic benefit not abstract or reputational enhancements. This provision means that a person who discloses proprietary economic information but does not intend to materially gain from it or intend the recipient to so benefit cannot be prosecuted.

The requirement that the information have a value of not less than $100,000 is jurisdictional and is not intended to be an element of the crime; the prosecution need not prove that the person knew the exact value of the information. In determining the value of the information, the prosecution may use the valuation technique that is appropriate in light of the circumstances of the case. A variety of valuation methods have been used in civil and criminal cases involving trade secrets. See generally Rosenhouse, Annotation, Proper Measure of Damages for Misappropriation of Trade Secrets, 11 A.L.R.4th 12.[2] They include determining the profits that the owner would have realized had the information remained proprietary. See, e.g., *Sperry Rand Corp.* v. *A-T-O, Inc.*, 447 F.2d 1387, 1392–94 (4th Cir. 1971). In other cases, the value of the stolen information has been calculated by determining the profits that the defendant gained by selling it. See, e.g., *Univ. Computing Co.* v. *Lykes-Youngstown Corp.*, 504 F.2d 518, 535–36 (5th Cir. 1974). Courts have also recognized the research and development costs of the pro-

[2] We recognize that damages in a civil suit are not the exact equivalent of value. But in the course of determining the compensatory damages available to a victorious plaintiff, many courts have developed methods for valuing trade secrets.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 15 2002

prietary economic information as a proper measure of its value. See, e.g., *Salsbury Lab., Inc.* v. *Merieux Lab., Inc.,* 735 F. Supp. 1555, 1579 (M.D. Ga. 1989), aff'd in part and rev'd in part, 908 F.2d 706 (11th Cir. 1990). Other methods of valuing proprietary economic information may also be available. The Committee believes that these techniques are valid.

The actor must knowingly steal the information, or take it without authorization, or transmit it without authorization. A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one's conduct, and (2) an awareness of or a firm belief in or knowledge to a substantial certainty of the existence of a relevant circumstance, such as whether the information is proprietary economic information as defined by this statute. The statute does not require proof that the actor knew that his conduct violated Federal law. The Committee intends that the knowing state of mind requirement may be satisfied by proof that the actor was aware of a high probability of the existence of the circumstance, although a defense should succeed if it is proven that the actor actually and reasonably believed that the circumstance did not exist. This is similar to the practice of the proposed Model Penal Code (section 2.02(7)). This approach deals with the situation that has been called willful blindness, the case of the actor who is aware of the probable existence of a material fact—for example, that he has no authority, or that the information is proprietary—but does not satisfy himself that it does not in fact exist.

§ 1833. Forfeiture

This section is designed to permit recapture of both the proceeds and implements of the offenses specified in the chapter. This provision may prove especially telling, since the proceeds of proprietary economic property theft may be staggering in certain cases. These forfeiture provisions are meant to supplement, not replace, the authorized punishments in appropriate cases. The section incorporates through reference existing law that sets forth procedures to be used in the detention, seizure, forfeiture, and ultimate disposition of property forfeited under this section. It provides for an in personam action against the offender, rather than only one against the property itself, and it preserves the rights of innocent third parties.

§ 1834. Import and export sanctions

This section authorizes the President to prohibit, for a period of up to 5 years, the importation into, or exportation from, the United States of any product produced, made, assembled, or manufactured by a person convicted of any offense under section 1832. This sanction, too, is meant to enhance the bill's prophylactic effect by imposing another important sanction on offenders. Any sanctions so imposed are enforceable through a civil action that may be brought by the Secretary of the Treasury and which could result in the imposition of a civil penalty of not less than $100,000. It is anticipated that this sanction will generally be used against egregious and persistent violators.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 16 2002

§1835. Extraterritoriality

To rebut the general presumption against the extraterritoriality of U.S. criminal laws, this section makes it clear that the Act is meant to apply to certain conduct occurring beyond U.S. borders. To ensure that there is some nexus between the assertion of such jurisdiction and the offense, extraterritorial jurisdiction exists only if the offender is a citizen, permanent resident alien, or corporation of the United States; or an act in furtherance of the offense is committed in the United States. In pursuing such cases, it is expected that the Department of Justice will focus its investigative and prosecutorial resources on those instances in which there has been a substantial harm to U.S. interests.

§1836. Construction with other laws

This section makes clear that the Act does not preempt non-Federal remedies, whether civil or criminal, for dealing with the theft or misappropriation of economic proprietary information. Many States have criminalized the theft of intellectual property, but enforcement may be frustrated by the ease with which such property is transferred across State or national boundaries.

§1837. Preservation of confidentiality

This section authorizes a court to preserve the confidentiality of alleged proprietary economic information during legal proceedings under the Act consistent with existing rules of criminal procedure and evidence, and other applicable laws. This preserves the information's confidential nature and, hence, its value. Without such a provision, owners may be reluctant to cooperate in prosecutions for fear of exposing their proprietary information to public view—thereby destroying its worth.

§1838. Prior authorization requirement

This section requires that the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division of the Department of Justice must personally approve in advance any charge under this bill. This duty is nondelegable. This provision has been added as a safeguard against overzealous invocation of this new law. It is intended to help ensure that businesses and individuals are not chilled from making legitimate business decisions.

§1839. Law enforcement and intelligence activities

This section makes clear that the new chapter does not prohibit any lawfully authorized investigative, protective, or intelligence activity of the United States.

SECTION 4. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

This provision adds newly created crimes to the list of offenses which may be investigated with authorized wire, oral, or electronic intercepts.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 17 2002

V. Regulatory Impact Statement

Pursuant to paragraph 11(b), rule XXVI of the Standing Rules of the Senate, the Committee, after due consideration, concludes that Senate bill 1556 will not have direct regulatory impact.

VI. Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, August 21, 1996.

Hon. Orrin G. Hatch,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has reviewed S. 1556, the Industrial Espionage Act of 1996, as reported by the Senate Committee on the Judiciary on July 30, 1996. CBO estimates that enacting the bill would result in no significant net impact on the federal budget. Enacting S. 1556 would affect direct spending and receipts by increasing the amount of forfeiture receipts and penalties collected and spent by the government, but we estimate that such effects would not occur until after fiscal year 1998. Thus, the bill would not be subject to pay-as-you-go procedures, which apply only through fiscal year 1998. In any event, we expect that the bill would have no significant net effect on the federal budget over time because receipts from criminal fines and the sale of forfeited property would be spent, generally within one year of receipt.

Bill Purpose. Enacting S. 1556 would make it a federal crime to steal proprietary economic information having a value of at least $100,000 from an owner of such information. Under current law, cases involving economic espionage are prosecuted under various statutes; however, none is broad enough to accommodate most cases of economic espionage. Under this bill, economic information would include intellectual property as well as physical property, and violations would include duplication of information as well as physical theft. Violators would be subject to imprisonment, criminal fines, and forfeiture of the property involved in the crime. Enacting this bill also would allow the President to prohibit a person convicted of economic espionage from importing goods into, or exporting goods from, the United States for a period up to five years. Violators of such Presidential orders would be subject to civil fines and the forfeiture of related property.

Federal Budgetary Impact. While pursuing investigations would consume staff time and other resources of the federal government, CBO estimates that the Department of Justice and the Federal Bureau of Investigation (FBI) would not need significant additional resources to enforce the provisions of the bill over the next several years. Based on information from the FBI, CBO assumes that few cases would be investigated and prosecuted over the next several years, but that the caseload would grow over time. Corporations, which constitute the majority of victims of industrial espionage, are reluctant to publicly admit theft out of fear that they would be forced to reveal proprietary information when the case goes to court. In addition, prosecutions under this bill would require prior

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 18 2002

approval of the Attorney General (AG) or certain members of the AG staff. As a result of this requirement, CBO anticipates that the number of cases prosecuted would be kept to a minimum because prosecutors would only pursue those cases with substantial evidence. CBO estimates that, in the long term, the government's caseload could significantly increase and additional resources could be needed if corporations become more comfortable with reporting economic espionage and the government pursues more cases involving economic espionage. Any such additional resources would be subject to the availability of appropriated funds.

This bill also would establish penalties—including fines, imprisonment, and the forfeiture of property involved in the crime—for violations of the provisions of this bill. Such criminal fines and receipts from the sale of forfeited property would be deposited in the Crime Victims Fund and spent in the following year. Civil penalties would be paid to a receipt account in the Treasury, but we expect that any such revenues would not be significant. CBO estimates that because it would take at least two years to investigate and prosecute a case, the government would not collect any fines or receipts from the sale of forfeited property through 1998. Based on conversations with the FBI, we estimate that additional receipts paid into the Crime Victims Fund after fiscal year 1998 could exceed $5 million a year. Spending from the fund would increase in the same amounts, but with a one-year lag. In addition, CBO does not expect any significant increase in prison costs as a result of this bill.

Mandate Statement. S. 1556 contains no private-sector or intergovernmental mandates as defined in the Unfunded Mandates Reform Act of 1995 (Public Law 104–4), and would have no impact on the budgets of state, local, or tribal governments.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Jonathan Womer and Susanne Mehlman.

Sincerely,

JUNE E. O'NEILL, *Director.*

VII. CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the changes in existing law made by the bill, as reported by the committee, are shown as follows (existing law proposed to be omitted is enclosed in bold brackets, new matter is printed in italic, and existing law with no changes is printed in roman):

UNITED STATES CODE

* * * * * * *

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 19 2002

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I.—CRIMES

Chapter	*Sec.*
1. General provisions	1
* * * * * * *	
89. Professions and occupations	1821
90. Protection of Proprietary Economic Information	*1831*
* * * * * * *	

CHAPTER 90—PROTECTION OF PROPRIETARY ECONOMIC INFORMATION

Sec.
1831. Definitions.
1832. Criminal activities affecting proprietary economic information.
1833. Criminal forfeiture.
1834. Import and export sanctions.
1835. Extraterritoriality.
1836. Construction with other laws.
1837. Preservation of confidentiality.
1838. Prior authorization requirement.
1839. Law enforcement and intelligence activities.

§1831. Definitions

As used in this chapter:

(1) The term "person" means a natural person, corporation, agency, association, institution, or any other legal, commercial, or business entity.

(2) The term "proprietary economic information" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including data, plans, tools, mechanisms, compounds, formulas, designs, prototypes, processes, procedures, programs, codes, or commercial strategies, whether tangible or intangible, and whether stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing that—

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

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

The term does not include any general knowledge, experience, training, or skill that a person lawfully has acquired due his work as an employee of or as an independent contractor for any person.

(3) The term "owner" means the person or persons in whom, or United States Government component, department, or agency in which, rightful legal, beneficial, or equitable title to, or license in, proprietary economic information is reposed.

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 20 2002

(4) The term "United States person" means—

(A) in the case of a natural person, or United States citizen or permanent resident alien; and

(B) in the case of nonnatural person, an entity substantially owned or controlled by the United States Government or by United States citizens or permanent resident aliens, or incorporated in the United States.

(5) The term "without authorization" means not permitted, expressly or implicitly, by the owner.

§1832. Criminal activities affecting proprietary economic information

(a) Any person, with intent to, or reason to believe that it will, injure any owner of proprietary economic information having a value of not less than $100,000 and with intent to convert it to his or her own use or benefit or the use or benefit of another, who 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);

(5) wrongfully solicits another to commit any offense described in paragraphs (1) through (3); or

(6) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined up to $250,000, or twice the value of the proprietary economic information, whichever is greater, or imprisoned not more than 10 years, or both.

(b) Any corporation that commits any offense described in paragraphs (1) through (6) of subsection (a) shall be fined up to $10,000,000, or twice the economic value of the proprietary economic information, whichever is greater.

(c) This section does not prohibit the reporting of any suspected criminal activity or regulatory violation to any appropriate agency or instrumentality of the United States, or a political subdivision of a State, or to Congress.

§1833. Criminal forfeiture

(a) Notwithstanding any provision of State law, any person convicted of a violation under this chapter shall 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 violations; and

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 21 2002

(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.

(b) The court, in imposing a sentence on such person, shall order, in addition to any other sentence imposed pursuant to this chapter, that the person forfeit to the United States all property described in this section.

(c) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsection 413(d) which shall not apply to forfeitures under this section.

(d) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund established under section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601) all amounts from the forfeiture of property under this section remaining after the payment of expenses and sale authorized by law.

§1834. Import and export sanctions

(a) The President may, to the extent consistent with international agreements to which the United States is a party, prohibit, for a period of not longer than 5 years, the importation into, or exportation from, the United States, whether by carriage of tangible items or by transmission, any merchandise produced, made, assembled, or manufactured by a person convicted of any offense described in section 1832 of this title, or in the case of an organization convicted of any offense described in such section, its successor entity or entities.

(b)(1) The Secretary of the Treasury may impose on any person who knowingly violates any order of the President issued under the authority of this section, a civil penalty equal to not more than 5 times the value of the exports or imports involved, or $100,000, whichever is greater.

(2) Any merchandise imported or exported in violation of an order of the President issued under this section shall be subject to seizure and forfeiture in accordance with sections 602 through 619 of the Tariff Act of 1930.

(3) The provisions of law relating to seizure, summary and judicial forfeiture, and condemnation of property for violation of the United States customs laws, the disposition of such property or the proceeds from the sale thereof, the remission or mitigation of such forfeiture, and the compromise of claims, shall apply to seizures and forfeitures incurred, or alleged to have been incurred under this section to the extent that they are applicable and not inconsistent with the provisions of this chapter.

§1835. Extraterritoriality

(a) This chapter applies to conduct occurring within the United States.

(b) This chapter applies to conduct occurring outside the territorial and special maritime jurisdiction of the United States, its territories, and possessions if—

(1) the offender is a United States person; or

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 22 2002

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

§1836. Construction with other laws

This chapter shall not be construed to preempt or displace any other Federal or State remedies, whether civil or criminal, for the misappropriation of proprietary economic information, or to affect the otherwise lawful disclosure of information by any government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

§1837. Preservation of confidentiality

In any prosecution under this chapter, the court may enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of proprietary economic information, consistent with rule 16 of the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, and other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing the disclosure of proprietary economic information.

§1838. Prior authorization requirement

The United States may not file a charge under this chapter or use a violation of this chapter as a predicate offense under any other law without the personal approval of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division of the Department of Justice.

§1839. Law enforcement and intelligence activities

This chapter does not prohibit any and shall not impair otherwise lawful activity conducted by an agency or instrumentality of the United States, a State, or a political subdivision of a State, or an intelligence agency of the United States.

* * * * * * *

CHAPTER 119—WIRE INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

* * * * * * *

§2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 23 2002

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: *chapter 90 (relating to economic espionage and protection of proprietary economic information in interstate and foreign commerce),* chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots) chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

O

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 24 2002

Document No. 24

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 2 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002