A Guide to Lessons Learned and Best Practices in Using the Statutes in the Economic Espionage Act of 1996

Approved By: Mike Klemp-North, PhD Date: August 5, 2019

A Guide to Lessons Learned and Best Practices in Using the Statutes in the Economic Espionage Act of 1996

A Seminar Paper

Presented to the Graduate Facility

University of Wisconsin-Platteville

In Partial Fulfillment of the Requirement for the Degree

Master of Science in Criminal Justice

Edward T. Lawson

August 2019

Acknowledgements

I would like to thank my family for their patience and understanding. This was a three year effort sandwiched between a career in federal law enforcement, a retirement and a new career, as well as family life. My wife, children and grandchildren were very understanding and supportive. I understand the sacrifice they made for me in order for me to reach my goal of earning a Master's degree.

I would also like to thank my coworkers and all the other resources that I tapped into to assist me in my efforts. This undertaking involved my decision to expend time, effort and funds to pursue this goal. This was not done in a vacuum and I appreciate everyone that assisted me.

I also want to thank the folks I worked with at the FBI and U.S. Attorney's Office for their insight into the challenges of the legal aspects of this violation. We were involved with a couple of the case examples in this paper and being able to produce a product that others can use to assist in their decision making, means a great deal to me.

Finally, I want to express my appreciation to my seminar paper advisor, Dr. Michael Klemp-North, for his patience and guidance with my research and writing efforts. He was also one of my course instructors and I thank him for all his efforts in guiding me in this process.

Abstract

A Guide to Lessons Learned and Best Practices in Using the Statutes in the Economic Espionage Act of 1996

Edward t. Lawson

Under the Supervision of Dr. Michael Klemp-North

Statement of the Problem

The Economic Espionage Act (EEA) of 1996 was signed into law by President Clinton in an effort to slow down or stop the theft of U.S. Trade Secrets (TS) and Intellectual Property (IP) from United States companies that spend hundreds of millions of dollars annually resulting in the U.S. being the leaders of technology development in the world. In 2014 it was estimated that $300 billion was lost to economic espionage. Federal prosecutors have 18 U.S.C. §1832, the theft of trade secrets under the EEA to use in prosecuting the theft of trade secrets. EEA 1996 also included alternatives to use civil courts, 18 U.S.C.A. §1836, civil proceeding in the misappropriation of a trade secret, allowing companies to address the theft of their trade secrets through civil remedies. This research paper will explain the history and definitions on economic espionage, also known in the past as industrial espionage. It will also outline the states individual efforts to curtail economic espionage prior to EEA 1996. There are times when criminal charges will have more of an impact verses civil charges and/or the government agrees to honor the requests of the companies and not pursue criminal charges while civil litigation is proceeding.

Methods of Approach

The research will include secondary research (Priebe 2014, Krotoski 2009, & FBI.CI), as well as archival data analysis on 18 U.S.C. §1832 and §1836 cases from 2008-2018 (FBI.gov). This could include cases that were not reported to U.S. government authorities but handled internally by the U.S. corporations in federal civil courts. The research will include possible motivations and theories behind why people and companies plan and commit the thefts (Barack et al 2010). This paper will also review policies and procedures for protecting trade secrets and intellectual property during trial preparation, trial and all appeals. This paper will compare the cases prosecuted by the government to civil cases to determine any best practices and procedures. The research questions include: outcomes of §1832 and §1836 cases, penalties and dollar amount as fines and how the government and/or the company protect their trade secrets during trial proceedings.

Anticipated Outcomes

This paper will analyze the techniques available to both U.S. companies and the U.S. government that are attempting to stop or deter the theft of U.S. trade secrets and technologies. It will review the history that led to EEA 1996 and the expanded penalties since 1996. It will discuss best practices for protecting trade secret material during all phases of the trial, as well as determining the best practice for selecting which statute to use. The lessons learned from this research can assist the government and companies in designing insider threat training and awareness programs. This paper can also serve as a guide for criminal and civil attorneys to determine the best practices that are being used to deter and/or stop the theft of U.S trade secrets and intellectual property.

Table of Contents

II. Introduction & Literature Review

The United States is one of the leaders in production, quality products and high technology. The U.S. was listed as the largest world economy in 2010. The U.S. showed revenues and Gross Domestic Product (GDP) of over 15 trillion US Dollars, Canada was second with 1.75 trillion dollars and Saudi Arabia third at 560 billon dollars (Barack et al 2015). When it comes to hanging onto that technical edge, the U.S. has been fighting an up-hill battle since the Second World War. The United States' ability to ramp up from a consumer industry to a war industry footing grabbed the attention of our future enemies. Prior to the Cold War, the focus was on protecting military intelligence, but has now shifted towards protecting the Unites States' corporations (Priebe 2014). It is estimated that of the 173 nations worldwide, approximately 57 or more are actively seeking to steal trade secrets and intellectual property from the United States' corporations. The enactment of the U.S. Economic Espionage Act 1996 is evidence of our government efforts to protect our technology, not only domestically, but internationally as well (see the entire Economic Espionage Act 1996 at Annex A). The Act was given more teeth with the Economic Espionage Penalty Act of 2012. This act increased the maximum fines for foreign and economic espionage to not more than $5 million for individuals and not more than $10 million or 3 times the value of the trade secret. However, the increase in fines focused on 18 U.S.C. §1831 charges, involving a foreign nexus. Legislators saw the need to adjust it 16 years after the original version was signed in 1996 by increasing the financial penalties and prison sentences regarding 18 U.S.C. §1832 (Priebe 2015).

President Obama's administration also saw the need to enact "The Defend Trade Secrets Act of 2016" (DTSA). It amends chapter 90 of title 18 of the United States Code. A perceived problem with the pre-existing chapter of 90 of title 18 is that it only provided for government

action against entities stealing TS and IP. The DTSA now provides avenues for private parties to sue for the theft of TS & IP. It provides steps for the private party to seek court action to protect its TS & IP during the court proceedings (Neifeld 2016).

It must be very frustrating to spend years to decades developing product(s) and establishing services to consumers. There are years of research and development, hundreds of thousands to millions of dollars spent and trusted employees developed in their companies. Then you discover that a trusted employee and/or subcontractor has taken steps to steal your TS/IP. Maybe for personal financial gain, maybe for a better position at a competing company or to make you pay for a perceived injustice. You are faced with decisions that will affect your company's future, not only the financial future, but the financial security of your employees. What can you do? Who can you contact? Does this news stay internal? Do you get the federal government involved? How will the media portray your company in the spotlight of public option? What will your stockholders and sponsors think? Two large companies in the Chicago area dealt with these concerns.

In 2008, Hanjuan Jin, a trusted Motorola software engineer for ten years was part of a spot search at the Chicago International Airport and found to have over 1,000 electronic and paper documents belonging to Motorola, which is based in Schaumburg, Illinois. She had accepted a job offer with the Chinese competitor, Sun Kaisens. Her trail preparations, delays and medical issues dragged the court proceedings out for over four years. She was found guilty of stealing Motorola's Trade Secrets pursuant to EEA 1996, but acquitted on espionage charges. The prosecutors recommended a sentence of six to eight years, but she was sentenced to four years in prison (TSI Brookslaw 2013). Every time a court appearance was made, a defense

lawyer change happened and other court events, this made the local and sometimes the national news, bringing unwanted attention to the company.

In March of 2009, David Yen Lee notified Valspar, a paint company in Wheeling, Illinois, where he was the technical director, that he was resigning. He did not inform them that he had accepted a position with the Shanghai, China competitor, Nippon, as the vice president of technology and administrator of research and development. Nor did he mention that he had been downloading over 160 original batch tickets, secret formulas for paints and coatings from Valspar's protected database, valued at over $20 million. He plead guilty to one count of theft of trade secrets and was sentenced to 15 months in a federal prison in December 2010 (FBI Archives 2009). This case moved much quicker and reduced the amount of time in the media. Both cases involved the companies dedicating many hours and financial resources in assisting the federal prosecution, with the possibility of their trade secrets being exposed to competitors in court records.

Finally, greed knows no status limits or concerns for victims. History has shown that it is always cheaper to steal than to put the effort and money into research and development. There are foreign companies that seek to improve their business competitiveness and their countries' economies by stealing TS/IP from a world technology leader like the United States. There are also foreign adversaries that seek to gain technological and economic advantages over the United States (FBI White Paper). The committee that submitted H.Rept. 104-788-Economic Espionage Act of 1996 believed that such a scheme (set of laws) will serve as a powerful deterrent to this type of crime. Additionally, they believed that a comprehensive federal criminal statute will better facilitate the investigation, prosecution, restitution and resources for the victims of this

crime (H.Rept. 104-788). This paper will serve as a guide to which parts of the EEA 1996 best serves that purpose.

A. §1832. Theft of trade secrets

The following is the specific paragraphs involving the criminal statute 18 U.S.C. §1832 in EEA 1996. The legislators relied on the histories of the previous legislations at the federal and state level to find a way to narrow down the criminal activity and provide law(s) to deter or stop the theft of TS/IP.

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

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

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

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

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

(Added Pub. L. 104–294, title I, §101(a), Oct. 11, 1996, 110 Stat. 3489; amended Pub. L. 112–236, §2, Dec. 28, 2012, 126 Stat. 1627; Pub. L. 114–153, §3(a)(1), May 11, 2016, 130 Stat. 382.)

Amendments

2016—Subsec. (b). Pub. L. 114–153 substituted "the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided" for "$5,000,000".

2012—Subsec. (a). Pub. L. 112–236 substituted "a product or service used in or intended for use in" for "or included in a product that is produced for or placed in" in introductory provisions.

By way of introduction to the Economic Espionage Act of 1996:

Key wording for our use:

‘‘(e) ORDERS TO PRESERVE CONFIDENTIALITY.—In any prosecution or other proceeding(s) under this section, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An inter-locutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.‘‘(f) CIVILPROCEEDINGS TOENJOINVIOLATIONS.—
3‘‘(1) GENERALLY.—The Attorney General may, in a civil action, obtain appro-priate injunctive relief against any violation of this section.‘‘(2) EXCLUSIVEJURISDICTION.—The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection (H.Rept 104-788).

B. Criminal Statute Case studies

In May 2007 two former Coca Cola employees were sentenced for conspiring to steal and sell trade secrets to rival PepsiCo (hereafter Pepsi) for as much as $1.5 million (Reuters 2007). A third defendant was sentenced to two years in prison after agreeing to a plea deal and testifying against one of the Coca-Cola insiders (NBCNews 2017). Joya Williams, Edmund Duhaney, from Decatur, Georgia and Ibrahim Dimson, from New York, plotted to steal

confidential to highly restricted documents and a sample of a new Coke formula to PepsiCo Inc., (Pepsi). Williams was a Coca-Cola Company executive assistant that planned the theft of a new formula and offer it to their competitor, Pepsi. However, in this case, the Pepsi representatives were undercover FBI agents who were alerted by Coca Cola that Pepsi referred a possible insider threat complaint to them in the summer of 2006 (CNN 2007).

Surveillance video shows Williams searching files and putting some of the sensitive files in her personal bag. Duhaney, a family friend of Williams and an ex-convict served as the go between and Dimson was responsible for contacting Pepsi with the offer of inside information on a new Coke product. Dimson interacted with FBI agents posing as Pepsi representatives and provided documents and a sample of the new product. The documents and the sample were later confirmed to be stolen Coca-Cola trade secrets and property. The three defendants were charged with wire fraud, theft of trade secrets and selling trade secrets that belonged to Coca-Cola. (Reuters 2007).

Williams was sentenced to eight years in prison, $40,000 in restitution and three years of supervised probation after serving her jail time. Dimson was sentenced to five years in jail and ordered to pay $40,000 in restitution. Duhaney was sentenced some months after the first two because he agreed to plead guilty and testify for the prosecution. He received a two year sentence, ordered to pay $40,000 in restitution, serve three years of supervised probations and perform 40 hours of community service (NBCNews 2007).

Clark Alan Roberts and Sean Edward Howley were both employed as engineers for Wyko Tire Technology (Wyko), a Tennessee based company, who made a deal to supply Chinese tire maker Hao Hua with certain tire-building parts. However, Wyko did not have the knowledge/technology to build the parts. Roberts and Howley used their relationship with

Goodyear to secretly photograph their proprietary technology. This action not only violated a confidentiality agreement signed with Goodyear, but elements of the Theft of Trade Secrets included in EEA 1996. Roberts and Howley took advantage of a request by Goodyear for repairs to tire assembly machines provided by Wyko at a Goodyear plant (TSI Brookslaw 2013). Wyko sent Roberts and Howley who are engineers instead of technicians. Once in the Goodyear plant, Howley and Roberts were left unescorted for a brief time. Howley used his cell phone camera to take pictures of the swabbing down device they needed for their contract with Hao Hua. Howley sent the photos to his Wyko account and discussed how the pictures could be used to create the swapping process that they needed to meet the Chinese contract (Burr 2013).

The Wyko's IT manager discovered the "Robert's" e-mail and pictures. He then contacted Goodyear and advised them of the possible illicit pictures. Goodyear notified the FBI, who then conducted a Theft of Trade Secrets (18 U.S.C. §1832) investigation (Burr 2013). Howley and Roberts were found guilty by a jury in December 2012 and prison sentences of at least 10 months were requested. Later a federal Appeals Courts determined that there were procedural errors in determining the value of the trade secrets/technology. Their sentences were reduced to four months of home confinement, 150 hours of community service and four years of probation each (TSI Brookslaw 2013).

In 2011, the Sinovel Wind Group, headquartered in Beijing, China encouraged Dejan Karabasevic, an employee of the U.S. based American Semi-Conductor (AMSC) to steal and convert source code needed to bypass a fee licensed device used in their hundreds of wind turbines produced by AMSC. Karabasevic is a Serbian national who worked for a AMSC subsidiary in Austria called AMSC Windtec. He gained access to a controlled computer network in Middleton, Wisconsin and stole the source code (Trelevon 2018).

Karabasevic was promised a contract with a Sinovel subsidiary in China for over one million dollars and an apartment. Once the theft was discovered, Austrian law enforcement arrested Karabasevic, prosecuted him on industrial espionage charges and he served a one year house arrest sentence. Later Karabasevic, Sinovel and two senior executives at Sinovel were indicted by a Western District of Wisconsin Grand Jury. "The allegations in this indictment describe a well-planned attack on an American business by international defendants – nothing short of attempted corporate homicide" said U.S. Attorney John Vaudreuil (US Attorney News Release). Following an 11-day trial, a jury sitting in Madison, Wisconsin, convicted Sinovel Wind Group of conspiracy to commit trade secret theft, theft of trade secrets and wire fraud. The financial impact estimated as a loss of $800 million in past non-payments from Sinovel also resulted in approximately 700 people, about half the companies' workforce, being fired/released (Trelevon 2018).

C. §1836. Civil proceedings

The following is the specific paragraphs involving the civil mediation statute 18 U.S.C. §1836 in EEA 1996. The legislators relied on the histories of the previous legislations at the federal and state level to find a way to narrow down the criminal activity and provide law(s) to deter or stop the theft of TS/IP. They seemed to have felt it necessary to give the victim company's options.

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this chapter.

(b) Private Civil Actions.—

(1) In general.—An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.

(2) Civil seizure.—

(A) In general.—

(i) Application.— Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.

(ii) Requirements for issuing order.—The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that—

(I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;

(II) an immediate and irreparable injury will occur if such seizure is not ordered;

(III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;

(IV) the applicant is likely to succeed in showing that—

(aa) the information is a trade secret; and

(bb) the person against whom seizure would be ordered—

(AA) misappropriated the trade secret of the applicant by improper means; or

(BB) conspired to use improper means to misappropriate the trade secret of the applicant;

(V) the person against whom seizure would be ordered has actual possession of—

(aa) the trade secret; and

(bb) any property to be seized;

(VI) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;

(VII) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and

(VIII) the applicant has not publicized the requested seizure.

(B) Elements of order.—If an order is issued under subparagraph (A), it shall—

(i) set forth findings of fact and conclusions of law required for the order;

(ii) provide for the narrowest seizure of property necessary to achieve the purpose of this paragraph and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;

(iii)(I) be accompanied by an order protecting the seized property from disclosure by prohibiting access by the applicant or the person against whom the order is directed, and prohibiting any copies, in whole or in part, of the seized property, to prevent undue damage to the party against whom the order has issued or others, until such parties have an opportunity to be heard in court; and

(II) provide that if access is granted by the court to the applicant or the person against whom the order is directed, the access shall be consistent with subparagraph (D);

(iv) provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials, including—

(I) the hours during which the seizure may be executed; and

(II) whether force may be used to access locked areas;

(v) set a date for a hearing described in subparagraph (F) at the earliest possible time, and not later than 7 days after the order has issued, unless the party against whom the order is directed and others harmed by the order consent to another date for the hearing, except that a party against whom the order has issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the applicant who obtained the order; and

(vi) require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure under this paragraph

(C) Protection from publicity.—The court shall take appropriate action to protect the person against whom an order under this paragraph is directed from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order.

(D) Materials in custody of court.—

(i) In general.—Any materials seized under this paragraph shall be taken into the custody of the court. The court shall secure the seized material from physical and electronic access during the seizure and while in the custody of the court.

(ii) Storage medium.—If the seized material includes a storage medium, or if the seized material is stored on a storage medium, the court shall prohibit the medium from being connected to a network or the Internet without the consent of both parties, until the hearing required under subparagraph (B)(v) and described in subparagraph (F).

(iii) Protection of confidentiality.—The court shall take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information ordered seized pursuant to this paragraph unless the person against whom the order is entered consents to disclosure of the material.

(iv) Appointment of special master.—The court may appoint a special master to locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized. The special master appointed by the court shall agree to be bound by a non-disclosure agreement approved by the court.

(E) Service of order.—The court shall order that service of a copy of the order under this paragraph, and the submissions of the applicant to obtain the order, shall be made by a Federal law enforcement officer who, upon making service, shall carry out the seizure under the order. The court may allow State or local law enforcement officials to participate but may not permit the applicant or any agent of the applicant to participate in the seizure. At the request of law enforcement officials, the court may allow a technical expert who is unaffiliated with the applicant and who is bound by a court-approved non-disclosure agreement to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.

(F) Seizure hearing.—

(i) Date.—A court that issues a seizure order shall hold a hearing on the date set by the court under subparagraph (B)(v).

(ii) Burden of proof.—At a hearing held under this subparagraph, the party who obtained the order under subparagraph (A) shall have the burden to prove the facts supporting the findings of fact and conclusions of law necessary to support the order. If the party fails to meet that burden, the seizure order shall be dissolved or modified appropriately.

(iii) Dissolution or modification of order.—A party against whom the order has been issued or any person harmed by the order may move the court at any time to dissolve or modify the order after giving notice to the party who obtained the order.

(iv) Discovery time limits.—The court may make such orders modifying the time limits for discovery under the Federal Rules of Civil Procedure as may be necessary to prevent the frustration of the purposes of a hearing under this subparagraph.

(G) Action for damage caused by wrongful seizure.—A person who suffers damage by reason of a wrongful or excessive seizure under this paragraph has a cause of action against the applicant for the order under which such seizure was made, and shall be entitled to the same relief as is provided under section 34(d)(11) of the Trademark Act of 1946 (15 U.S.C. 1116(d)(11)). The security posted with the court under subparagraph (B)(vi) shall not limit the recovery of third parties for damages.

(H) Motion for encryption.—A party or a person who claims to have an interest in the subject matter seized may make a motion at any time, which may be heard ex parte, to encrypt any material seized or to be seized under this paragraph that is stored on a storage medium. The motion shall include, when possible, the desired encryption method.

(3) Remedies.—In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may—

(A) grant an injunction—

(i) to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not—

(I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or

(II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business;

(ii) if determined appropriate by the court, requiring affirmative actions to be taken to protect the trade secret; and

(iii) in exceptional circumstances that render an injunction inequitable, that conditions future use of the trade secret upon payment of a reasonable royalty for no longer than the period of time for which such use could have been prohibited;

(B) award—

(i)(I) damages for actual loss caused by the misappropriation of the trade secret; and

(II) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or

(ii) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriation's unauthorized disclosure or use of the trade secret;

(C) if the trade secret is willfully and maliciously misappropriated, award exemplary damages in an amount not more than 2 times the amount of the damages awarded under subparagraph (B); and

(D) if a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith, or the trade secret was willfully and maliciously misappropriated, award reasonable attorney's fees to the prevailing party.

(c) Jurisdiction.—The district courts of the United States shall have original jurisdiction of civil actions brought under this section.

(d) Period of Limitations.—A civil action under subsection (b) may not be commenced later than 3 years after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered. For purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation.

(Added Pub. L. 104–294, title I, §101(a), Oct. 11, 1996, 110 Stat. 3490; amended Pub. L. 107–273, div. B, title IV, §4002(e)(9), Nov. 2, 2002, 116 Stat. 1810; Pub. L. 114–153, §2(a), (d)(1), May 11, 2016, 130 Stat. 376, 381.)

References in Text

The Federal Rules of Civil Procedure, referred to in subsec. (b)(2)(A)(ii)(I), (F)(iv), are set out in the Appendix to Title 28, Judiciary and Judicial Procedure.

Amendments

2016—Pub. L. 114–153, §2(d)(1), substituted "Civil proceedings" for "Civil proceedings to enjoin violations" in section catchline.

Subsecs. (b) to (d). Pub. L. 114–153, §2(a), added subsecs. (b) to (d) and struck out former subsec. (b) which read as follows: "The district courts of the United States shall have exclusive original jurisdiction of civil actions under this section."

2002—Subsec. (a). Pub. L. 107–273, §4002(e)(9)(A), substituted "this chapter" for "this section".

Subsec. (b). Pub. L. 107–273, §4002(e)(9)(B), substituted "this section" for "this subsection".

Effective Date of 2016 Amendment

Amendment by Pub. L. 114–153 applicable with respect to any misappropriation of a trade secret (as defined in section 1839 of this title) for which any act occurs on or after May 11, 2016, see section 2(e) of Pub. L. 114–153, set out as a note under section 1833 of this title. (H. Rept 104-788).

D. Civil Remedies Case studies

Epic, a privately held company based in Verona, Wisconsin, is the leading developer of medical records programs used in health care systems and hospitals in the United States. Epic sued Tata Consultancies, a part of the Tata conglomerate, in 2014 for illegally downloading software technology that is deemed confidential information by Epic. Tata is one of the largest providers of information technology and services in the world (Yahoo Finance 2018). Epic filed claims in federal civil court in the Western District of Wisconsin. The claims included; breach of contract, misappropriation of trade secrets, unfair competition and unfair enrichment. Epic brought the charges against Tata because of concerns that they illicitly downloaded documentation while Tata consultants were working as contractors for Kaiser Foundation Hospitals. Contractors are not allowed direct access to Epic technology, however, two contractors passed on access information to Tata employees in India (Yahoo Finance 2018).

A federal jury found in Epic's favor on seven of the claims against Tata. They awarded $240 million in damages and $700 million in punitive damages. The judge commented that he would most likely reduce the monetary penalties. Tata commented after the trial that the findings by the jury were unexpected because they believe Epic did not support their claims with supported evidence. Tata plans to appeal the findings (Yahoo Finance 2018).

The International Business Machine (IBM) Corporation in the early 1980s filed a $7.5 billion law suit against National Semiconductor Corporation (NSC) and the Japanese company Hitachi Ltd., for working together to steal IBM trade secrets. IBM was concerned that they had

taken over a years' worth of research and development for a new computer design. The charges include theft of trade secrets, racketeering and unfair competition. The main criminal charge originated from a Federal Bureau of Investigation (FBI) sting operation for theft of computer-design secrets from IBM. The criminal charges also included several top executives (Potts 1983).

Hitachi allegedly agreed to pay IBM 300 million dollars in the civil suit filed by IBM. They also agreed to take steps to ensure that the information that was taken from IBM is not used to benefit Hitachi. Two employees of Hitachi plead guilty to criminal charges of conspiring to transport stolen property from the United States to Japan. NSC was not named in the criminal charges but was named in the newer racketeering and unfair competition suit, along with Hitachi. NSC and Hitachi were accused of forming the System Study Group (SSG), a joint information-gathering team. Hitachi agreed to not only pay the agreed upon fine of 300 million dollars plus additional licensing fees for the use of any IBM technology (Potts 1983).

IBM was recently involved in a criminal case that sounds very similar to the case from the 1980s. A former software engineer for IBM in China was sentenced to five years in prison after pleading guilty to three counts of economic espionage and three counts of theft, possession and distribution of trade secrets. The court documents took steps to protect IBM, but reporters connected the defendant to IBM through social media. The FBI was involved after a tip pointed them to a former IBM employee, Xu Jiaqiang. Xu attempted to sell software to undercover FBI agents that he admitted he had built with stolen source code. It was later confirmed that the source code was the property of IBM (Farivar 2018).

The Chinese based global communications company, Huawei, is described as one of the world's largest telecommunications equipment and smart phone makers was a defendant in both

a criminal and civil case. Huawei is accused of stealing IP related technology used in a robot designed to diagnose quality control issues in mobile phones. The technology is owned by T-Mobile, a U.S. telecom provider. The civil case was filed in 2014 and a federal jury found Huawei guilty in May 2017 (Benner, Mozur & Zhong 2019).

The criminal portion of this case involves the daughter of Huawei's founder who is accused of misleading banks concerning Huawei's business in Iran. This violated America's sanctions on Iran inadvertently. Huawei also fired an employee after they were arrested in Poland and charged with spying for the Chinese government. The employee, Wang Weijing, was a former Chinese national employee at the Chinese Consulate in Gdansk, Poland before working for Huawei in public relations and sales (Benner, Mozur and Zhong 2019). This is not the first time Huawei has been accused of stealing TS/IP. In 2003, the company admitted it had stolen portions of the software that runs network equipment for Cisco Systems, a U.S. company. The patent infringement lawsuit was dropped when Huawei agreed to modify some of their products (Benner, Mozur and Znong 2019).

E. Analysis of the case studies

When our law makers designed the EEA 1996 they were very specific in the way they described a trade secret, who was stealing it and who would it benefit. They were very clear that the development of proprietary economic information is a key element in America's economic success. They also spelled out the requirements that would qualify as theft of a trade secret. They deemed that stealing a trade secret included; whoever, with the intent, or with reason to believe that the theft will benefit any foreign government, foreign instrumentality or foreign agent, it also included that the theft would benefit anyone else than the owner of that information, product, equipment, etc, (H.Rept. 104-788).

The law makers also explained that the intent of the bill/law was not to punish innovators or individuals seeking to benefit from private knowledge. It sought to deter/stop people from taking TS/IP from one company to a competitor. Therefore, the guidance in the law explains that it is unlawful to copy or otherwise exert control over a trade secret and that the owner of the trade secret has taken reasonable and active measures to protect that information. The final element of proving the theft of a trade secret is to ensure that the information taken has independent economic value, whether actual or potential and that the information is not generally accessible to the public (H.Rept 104-788). Please note that 18 U.S.C. §1836 has more details and guidance in pursuing civil remedies than 18 U.S.C. §1832, the criminal charge.

The case examples will be reviewed/ analyzed keeping in mind the elements explained above. The following elements will be addressed; were the trade secrets/intellectual property protected by reasonable measures? Were the people that conducted the theft of trade secrets a trusted employee? Did they have rightful access to the material taken? Did they abuse their access to gain control of the information/material taken? Did they take it for personal gain and/or provide it to a competitor?

The theft of a new Coca-Cola product formula and liquid sample was planned by a trusted Coca-Cola trusted insider, Williams, who was employed as an executive assistant with approved access to the material she stole. The prosecution proved the elements of reasonable measures to protect, that they were indeed a trade secret/intellectual property of Coca-Cola and that it had potential value. Williams abused her access to the information in an effort to receive personal monetary gain and it involved offering the stolen material to

Pepsi, one of its main competitor. The other two defendants were enlisted to assist in the selling of the stolen property and were not employed by Coca-Cola (Reuters 2007).

Roberts and Howley were trusted insiders of Wyko, a company that was contracted to repair and maintain equipment for Goodyear. The engineers used this relationship to access equipment that they required in order to meet a production agreement for a third party. The unauthorized photographing of the Goodyear equipment was needed to re-engineer it for their companies' benefit, which violated agreements between Wyko and Goodyear. The theft was conducted in order for Wyko to meet a contractual agreement with a foreign tire maker that competed with Goodyear (TSI Brookslaw 2013). The prosecution proved the elements of reasonable measures to protect, that they were indeed a trade secret/intellectual property of Goodyear and that it had potential value.

The theft of source code from a Middleton, Wisconsin computer network was orchestrated by a trusted insider employed by a subsidy of AMSC in Austria. Karabasevic had limited access and requested additional access for the sole purpose of stealing and modifying the source code of a licensing program to benefit a Chinese company. This was done for personal monetary gain and to benefit the foreign company, Sinovel, which had a severe economic effect on AMSC (Trelevon 2018). The prosecution proved the elements of reasonable measures to protect, that they were indeed a trade secret/intellectual property of AMSC and that it had potential value.

The use of 18 U.S.C. §1832 involves federal law enforcement elements and federal level prosecutors and provides the victim company resources not always available to a company acting on its own. This can include, but not limited to sanctioned undercover operations, overseas contacts and legal authorities in cooperating countries, search warrants, arrest

warrants, T-3 Wire taps, Foreign Intelligence Surveillance Act (FISA) Court orders and interviews. Investigative and prosecution authorities can be leveled against the suspected person or companies/countries believed to be involved with the theft of trade secrets. All three companies described in the cases studies for criminal prosecution resulted in the defendants being found guilty and in some cases directed to pay restitution. This is considered to be a success. However, these proceedings brought media attention to the companies and in some instances, it could make the stock holder leery of the future of the company. Going with federal authorities could be interpreted as unsuccessful business because the company had to rely on an outside entity to deal with its problems. Another unsuccessful element is that the company did not catch the theft prior to it happening and taking steps to mitigate it prior to the theft.

The subcontractor hired by a second party user of EPIC's source code and programs gained unlawful access to the trade secrets and provided further access to at least two other individuals operating in India. EPIC made it very clear through training, agreements and monitoring of the system that contractors were not allowed access to their network where the stolen material was kept and the theft was conducted to benefit a foreign competitor. EPIC proved that the elements of reasonable measures to protect, that they were indeed a trade secret/intellectual property of EPIC and that it had potential value. The civil affidavit also cited Wisconsin state statutes regarding theft of trade secrets.

Two foreign companies formed a special System Study Group in order to gain access and steal IBM proprietary information on a new computer product. The members of this group were not IBM employees, they did not have lawful access to the information, driving them to formulate a plan to gain unlawful access. IBM proved the elements of reasonable measures

to protect, that they were indeed a trade secret/intellectual property of IBM and that it had potential value. IBM also took additional steps to reduce the chances the two foreign companies would use that stolen information in future products and thus compete with them internationally (Potts 1983). This is an older law suit that pre-dates EEA 1996, showing the continuing struggle the United States is in to stop competitors from stealing TS/IP.

A senior employee of Huawei was involved in gaining unauthorized access to technology owned by T-Mobile. The Huawei employee was not a T-Mobile employee, they did not have lawful access to the information and the theft was conducted to benefit a foreign competitor of T-Mobile. This case also involved possible tradecraft, or spying techniques used by a fired Huawei employee that had worked as a Chinese official in Poland. T-Mobile proved the elements of reasonable measures to protect, that they were indeed a trade secret/intellectual property of T-Mobile and that it had potential value (Benner, Mozur and Zhong 2019).

The use of 18 U.S.C. §1836 in bringing civil charges against a person or company/country suspected of stealing trade secrets can be more involved for the victim company. The company must use internal legal resources. If they are not capable of this type of court proceedings, then an outside firm must be hired and trusted to protect their TS/IP in future court proceedings. The victim company can be limited in investigations, especially undercover operations and keeping the investigation(s) from the suspected defendants. Most private companies do not have the overseas networks that the U.S. Government has in order to request investigative and apprehension assistance. The company can hire a professional investigative firm to do some of these tasks. There is a limited amount of steps the victim company can take, whereas the U.S. Government, through the

federal law enforcement agencies and the U.S. Attorney's Office, has a broader reach and span of control. It is possible that a victim company would have more failures than the government entities.

III. Theoretical Framework

A. Motivations to Commit Economic Espionage

Committing espionage or spying might seem like a thing of the cold war, but it happens more often that most people think. People committing economic espionage are targeting our nation's valuable secrets. The use of spying techniques is no longer reserved for one government stealing classified information from another but stealing valuable research and trade secrets from U.S. universities and businesses (FBI Counterintelligence).

The motivations for spying or violating a position of trust and hurting a company or country boils down to seven categories, with some people falling into more than one category (Wikipedia-motivation). 1. Greed is one of the primary motivating factors, the prospect of financial gain. They may be simply seeking a way to supplement whatever income that they are already receiving or are driven to espionage because of financial difficulties. 2. Ideology (patriotism or religion) could compel someone to assist another country or person. This was prevalent during the Cold War, when people were motivated to support the ideological positions of the Western world or the Eastern bloc. In current times, this can be seen as one person strongly believing in their company affiliation/allegiance (FBI Counterintelligence). 3. Coercion, blackmail or threats are used sometimes to get people with access to do something that they would usually not do. This is where a person(s) threaten to release embarrassing information about a person's activities unless that person provides them with the TS/IP (FBI

Counterintelligence). 4. Ego (self-importance) or pride has occasionally been used to give the person committing the act a sense of importance or significance. This often involves the person committing the espionage a sense of superiority over their colleagues or the management they are outwitting (FBI Counterintelligence). 5. Excitement (sex or personal relationships) is rare but has been seen because the person committing the act gets a thrill from doing something secretive using spy-craft or tradecraft. This is especially true if they are bored with their life. Excitement is seldom the primary motivation to commit espionage but may be a contributing factor (FBI Counterintelligence). 6. Disgruntled insiders are a serious threat to companies and/or national security. When one feels that they have been mistreated, they might violate the trust they have built in order to right their perceived injustice. 7. Revenge is a version of the disgruntled employee. However, revenge can be sought by anyone that perceives they need to punish a company or a country (Wikipedia-motivation).

The following is a roll-up of how each case example fits into one or more of the motivations to commit espionage and/or economic espionage.

Williams was a trusted insider at Coca-Cola and abused that position for personal financial gain which falls into the greed category. She could also be considered a disgruntled insider because of dis-satisfaction with her income, position and/or potential for advancement. There are no specific details of this in the articles, however, a satisfied employee does not plot and execute a plan to steal company trade secrets, then offer them to a major competitor if they are a satisfied employee.

Howley and Roberts were trusted confidants at Wyko that earned a position of access and limited trust at Goodyear who subcontracted Wyko to repair production line equipment. They fall into the category of being coerced by Wyko to solve a high pressure problem, possibly stress

from senior people to meet a contractual obligation to a third party. This is hard to prove and can become a case of, they said, they said, once blame/responsibility is sought.

Karabasevic was a trusted insider for a subsidiary at AMSC. He was manipulated by a female at Sinovel promising money, a position at a Sinovel subsidiary, a place to live in China and possibly the enticement of a sexual relationship. He falls into greed, ego, excitement and being a disgruntled employee. Sinovel took advantage of all these indicators to get him to write a computer program that bypassed the licensing fees on hundreds of wind turbines. Court documents show e-mails where he was enjoying the spy like activities and making AMSC pay for not recognizing his skills (Treleven 2018).

Subcontractors to a second party arrangement by EPIC gained access to a controlled database and shared that access with co-workers at Tata in India, thus violating their signed agreements. Those subcontractors were motivated by greed and possible the excitement of beating the system at Epic. Their actions would have given them the gratitude of senior members at Tata, possibly promotions and other financial benefits.

Competitors of IBM set into motion a plan to gain access to new IBM developments through an information collecting group. Hitachi and NSC exploited opportunities to steal technology that would give them a competitive edge against IBM. This falls into the greed category. By unveiling a product first or making one better than a competitor, they can gain more sales and benefit financially. Ideology is also possible here, in the sense of pride in the company and striving for the success of that company at all costs.

A representative of Huawei using spy like trade craft gained access to T-Mobile diagnostic technology. There was also evidence of untruthful banking connections. This falls

into the greed category, where Huawei wanted to gain technology without spending the time and money to research it. When less funds are spent involving Research & Development (R&D) there is more in the profit category for the company.

B. Self-Control and Social Bonding Theory

Self-Control Theory

There have been many theories and studies to determine why people violate trust and commit crimes. One possible theory that applies to the example cases of economic espionage is a combination of a lack of self-control and a loss of bonding with the group, in these cases, a company. Deviance is mainly a function of individual differences in self-control. In 1990, Travis Hirschi along with a colleague, Michael Gottfredson, developed a theory that the lack of self-control can be responsible for criminal behavior. The low self-control theory is referred to as the general theory of crime (Tibbetts & Hemmens 2010). Hirschi and Goofredson attribute the formation of controls as coming from the socialization process. Low self-control indicates that certain traits and behaviors are present. These include; risk-taking, impulsiveness, self-centeredness, short term orientations and quick temper (Tibbets & Hemmens 2010).

All the company/corporations that were the victims in the case studies have well established policies, procedures and attempted to establish a positive work culture. It comes down to the individual to make the decision to cross the line and steal a trade secret. None of these cases have clear cut examples of coercion, where typical blackmail is being used for the employee/insider to violate the trust of their company. They made the decision to violate the company's trust with no outside influence.

Self-control should be the governing factor when even thinking about doing something to violate the trust of the company or doing something against a competitor. The low self-control theory can apply to the motivations of greed and possibly revenge. The risk taking, the some-what impulsiveness of the act and the short term fix aspect can apply. All the case examples, except the Wyko, can be addressed by this theory. In the Coca-Cola case example, Williams and her co-conspirators definitely knew that were committing a crime. The steps they took to shield their identity and association to Coca-Cola is proof. They definitely displayed risk taking when informing FBI undercover agents, known to them as Pepsi representatives, that they were selling trade secrets and a sample of a new Coke product. The Wyko case example does not really reach the main reasons for low self-control besides possibly the short term orientations element. They were trying to find a fix to ensure their company could follow through on a contract obligation. The AMSC case example meets all of the elements. Karabasevic definitely knew that he was crossing the line, he displayed the low self-control in his willingness to assist Sinovel for a price. He seemed to enjoy the risk of getting caught and relished the idea of making AMSC pay for not recognizing his value to the company.

The Epic case example meets the low self-control theory in the way Tata took the time and effort to get access to Epic TS/IP over months of serving as a subcontractor. Once they had the access, they not only gained entry into the database with the TS/IP, they passed that access to co-workers back in India. This shows risk taking and impulsiveness. They were computer experts and knew that their access and passage of material could be traced. In the IBM case, the foreign competitors displayed low self-control in their efforts to get the restricted information in an effort to level the playing field. They meet the elements of impulsiveness and short term orientations. They seemed to be focused on getting the information on a new product without spending the

time and money to research it themselves. The Huawei case example also meets the requirements of the low self-control theory. They knew that they had been under scrutiny for similar attempts at other U.S. companies and they still attempted to steal T-Mobile technology. These efforts show impulsiveness and risk taking.

Social Bonding Theory

The lack of self-control theory conflicts with the theory that deviance is a result of weak social bonds, such as poor attachments to others. However, by looking at this theory we can try to understand why one would violate a company's trust since companies attempt to create close ties as a family. In this case, a poor since of obligation to the employer (Tibbetts & Hemmens 2010). In 1969, Travis Hirschi explained his social bonding theory that humans can socially bond to conventional entities, such as families, schools and communities. For our purposes, the community includes the work place. He believed that the stronger a social bond, the less likely the person would commit crimes. Hirschi's theory is comprised of four elements; attachment, commitment, involvement and moral belief. He believed that attachment was the strongest factor. Hirschi expresses commitment as conformity in conventional lines, such as education or occupational career (Tibbetts & Hemmens 2010). The thought of bonding or committing to an organization, as in a career or to a company, is an element that would bolster why people would not commit economic espionage. They would have more of a sense of belonging and a commitment to protecting the company, preserving their career.

This would address the disgruntled insider/employee motivations seen in the Coca-Cola and AMSC cases. The trusted insiders did not have a sense of bonding or commitment to their employer. This applies to AMSC where the insider seeks revenge for a perceived injustice. Almost all of the case examples could be explained by some element of this theory. If the sense

of obligation to the company was strong, then the employee and subcontractor would feel strongly about protecting the company and its property.

C. Mendlsohn & Schafer's Functional Responsibility Theories

There are other theories that can apply to our case examples. We have concentrated on the offenders, now we will look at the victim companies as possibly sharing some of the responsibility and culpability. There are two possible victim theories; Mendelsohn's Theory and Schafer's Functional Responsibility. Benjamin Mendlsohn was an experienced attorney that devoted some time in evaluating victims, witnesses and bystanders using clearly worded questionnaires. Mendlsohn classified victims into six categories: 1. The completely innocent victim, 2. The victim with minor guilt, 3. The victim who is guilty as the offender, 4. The victim more guilty as the offender, 5. The most guilty victim, and 6. The imaginary victim. (Wallace & Roberson 2015).

Schafer's Functional Responsibility Theory gives the defense team a way to look at the company claiming the loss and apply some responsibility. Stephen Schafer in 1968 examined a few of the established theories and attempted to classify victims on the basis of responsibility instead of risk factors. He went onto explain that crime was not only an act but also a social phenomenon. Schafer believed that not all crimes simply "happen" to be committed, but that victims often contribute to crime by their acts of negligence, precipitate actions or provocations. Schafer explained that the study of criminal-victim relationships emphasizes the need to recognize the role and responsibility of the victim, where the criminal justice system must consider the dynamics of crime and address both criminal and victims (Wallace & Roberson 2015).

The requirements of the EEA 1996 statutes does take some of the burden off the victim if they meet the reasonableness of protecting the trade secret and that it has value. However, some blame/responsibility can be addressed by examining the security culture, management and the competition. We will look at a combination of Mendelsohn and Schafer's theories in regards to our case examples.

The AMSC case study has many facets that can lay possible blame on the victim company. Karabasevic's greed and revenge motives might have been detected by a more due diligent company, and AMSC can be seen as being delinquent in not setting up a system to require employees to report the request and breeches conducted by Karabasevis. He was described as a disgruntled employee/engineer and should have drawn the attention of AMSC security and management (Treleven 2018). Karabasevic conspired with the other defendants (Sinovel managers) to obtain AMSC's copyrighted information and trade secrets in order to produce wind turbines and to retrofit existing wind turbines with AMSC technology without paying AMSC (US Attorney News Release).

The U.S. based company AMSC is the victim and can also be held somewhat responsible for their actions or lack of actions. AMSC is mainly in the completely innocent victim category. They could have set up an insider threat team to identify people resigning, quitting or being fired that are in contact with competitors, as is the case in this theft. Sinovel and the other two Chinese defendants, SU and ZHAO recruited Karabasevic to leave AMSC Windtec and join Sinovel and to secretly copy intellectual property from the AMSC computer system (US Attorney News Release).

The Coca-Cola case and the Epic case examples show how trusted insiders, direct with Coca-Cola and indirectly with Epic, could have had other safeguards in place. They fit into

the victim with minor guilt category. There are security measures for spot checking employee's access to computer files, storage rooms and laboratory facilities. A check would have possibly alerted them to unusual activity and draw attention to them for a closer look before the criminal acts were committed. It is easy to Monday morning quarter back, however, many federal agencies, the FBI, U.S. Commerce Enforcement and the U.S. Department of Homeland Security Investigations, all have outreach programs that teach companies how to protect their TS/IP and monitor insiders. In the IBM and Huawei case examples, the companies were conducting due diligence, however, the efforts of the people trying to gain access took unusual steps to get access to the information they were targeting. These two companies also fall into the victim with minor guilt category. The motivations to commit economic espionage, along with the various theories can help explain why people and companies steal TS/IP. By understanding these forces at work against our companies, we can defend against some or most attempts at stealing it.

IV. Lessons Learned and Best Practices

A. Lessoned Learned

The bulk of the literature for the lessons learned section comes from a 15 year review of the EEA 1996, conducted by Matthew T. Priebe, Grand Valley State University. It will address what was used in the past in attempts to protect TS/IP. This included patents, trademarks, copyright laws and identifying technology/information as a trade secret, as well as a mismatched collection of state and federal statutes. This section will conclude by addressing the risk/threats and vulnerabilities the U.S. Companies face regarding their TS/IP. They have to make decisions on the steps that are appropriate to protect their TS/IP. The tools offered by state and federal laws, the physical protection of locks, guards and control databases are all options available to them.

Patents/Trademarks/Copyright Laws

Patents are used to allow consumers and investors to see product designs. They also protect the producer from a competitor providing an identical product which can affect competitive markets. It limits the competitors from making something with the identical specifications unless the patent is removed or revoked. The challenges the original producing company faces is how much information to include in the application process. This is a public document that can be viewed by competitors. The process(es) described in the application could be used by the competitor that plans to enter foreign markets, where the patent laws of the U.S. are not always enforced and recognized. Therefore, the original producer must weigh the risks of receiving the patent against the possible loss of the technical information to a possible competitor (Priebe 2014). The lessoned learned here is that a conscious decision must be made if a patent is necessary, what to include in the applications and what impact will that information have to the market and the company's financial future.

Copyrights are used to protect written forms of expression, but not ideas. They cover written books, maps and charts, novels, motion pictures, music, instruction manuals, bookkeeping forms and computer programs. The last category has become more important in the last 20 years. Computer programs/source code are the vital information for anything computerized (Preibe 2014). Copyrights protect this type of technology/information. The lessons learned here include access control and a clear understanding of ownership. The company leadership must determine when the IP is copyright material and when it becomes a TS.

Trademarks are used to protect brands legally from competitor use. Companies will spend large sums of money to build a brand and to be recognized by just a symbol. A trademark is a work, symbol or name used to identify the origin of the product. This allows the companies to

maintain their rights in all markets (Priebe 2014). The lesson here is to ensure trademark licensing as soon as a new company is formed. The internet makes any delay in locking in a trademark critical to the branding of a new product. Information of a new or updated company is known instantly, one must ensure that trademark planning is done well in advance of a new company announcement.

Trade secrets are the manner in which companies classify their intellectual information in order to ensure that their intellectual/original ideas are protected. The full definition of a trade secret can be found of page 10 of this paper. By classifying an idea as a trade secret, it is protected from someone else taking it without permission. The categories that meet trade secret status have been explained in Section II of this paper and it is critical that the company take reasonable measures to protect their trade secrets (Priebe 2014). The lesson learned here is that U.S. companies be aware of their state statutes and the EEA 1996 so as to stay in compliance of the trade secret category.

Previous Legislation

Previous legislation over the last 60 years has evolved to the EEA 1996 and the DTSA of 2016 as the tools being used to assist companies and the government in attempting to deter and/or stop economic espionage. In the past, TS/IP were classified as property rights and were addressed in civil courts using tort laws. The states also used the Uniform Trade Secrets Act of 1979, the National Stolen Property Act, the World Trade Organization and the Trade-Related Aspects of Intellectual Property Rights Agreement. At the national level, the National Stolen Property Act of 1948 was used to prosecute people stealing TS/IP (Priebe 2014). More recently, the Epic civil trial saw the use of EEA 1996, computer related statues and also referenced Wisconsin state laws; 18 U.S.C. §1030 Computer Fraud and Abuse Act, Wis Stat. §943.70

Computer Crimes Act, Wis Stat. §134.90 Misappropriation of Trade Secrets, Brach of Contract, Breach of the Covenant of Good Faith and Fair Dealing, Fraud, Misrepresentation, Conversion, Common Law Unfair Competition, Unjust Enrichment, Wis Stat. § 895.446, Wis. Stat. . § 943.20 and Wis. Stat. V 895.446 (Epic v. Tata 2014).

In has been determined that the use of alternative legal theories will allow a broader coverage of the crime(s) committed. Listing not only the federal charges, but the state charges and any other business agreements will give the jury or Judge a full picture of the person's illegal conduct. This should include all phases; the planning, preparation, misappropriation, possible intended use or the actual use of the stolen TS/IP (Krotoski 2009). An example of this would also include consider charging conspiracy or attempt. The criminal federal statutes for economic espionage allows the use of these charges. These two charges do not require proof of the existence of an actual TS, but proof of the defendants' attempt or conspiracy with intent to steal a trade secret (Krotoski 2009).

It seems that companies might consider parallel trade secrets proceedings. The prosecution team can receive evidence from the civil case because there is little risk that a judge would find that the defendant's due process rights were violated. The prosecution should be cautious when a parallel trade secrets misappropriation proceeding is on-going. The following concerns should be considered when interacting with private litigants: is the criminal investigation known to the defendant in the civil action? Are the defendants in the civil action represented by counsel? Has the plaintiff made any misrepresentation to the defendants regarding its knowledge of a criminal case? Is the plaintiff willing to share the evidence collected and/or are they getting advice from the prosecutor on what evidence is needed for the criminal case? It remains unknown on how the court will address similar interactions between

prosecutors and private parties (Newby 2009). The lesson learned here is to ensure the victim company's legal team has an open dialogue with the prosecutor's office prior to and during civil action.

Risks/Threats/Vulnerabilities

Companies must always be aware of and measure the risk/threat of someone or company stealing its TS/IP. The risk is the chance that you as a company could become a victim of economic espionage. The types of risk can include organizational and/or reputational. The organizational risk is what level of damage the company will incur if their TS/IP is stolen. The reputational risk involves how the investors and clients will be affected by the loss of the TS/IP. The threats include a person, organization event or a condition that could harm a company, either man made or natural. The natural threat include damage as a result of bad weather, building damage giving access to sensitive information. The human threat includes external and internal. The loss of sensitive unrecoverable TS/IP could have devastating effects on the company. (Priebe 2014).

Once the threats and risks have been identified, the company must understand any vulnerabilities to better safeguard their TS/IP. Organizational weaknesses must be identified. It could be Human Resource policies and training, cyber policy, access policy, reporting procedures, general security and specific security to a certain area. Training and awareness are the key to ensuring that internal employees know the steps used to protect the company's TS/IP. The company also needs to realize that vulnerabilities could exist. These could include, but not limited to personnel and technical vulnerabilities. These are the weaknesses in the company's security procedures. The personnel concerns include hiring practices, training and managing procedures. Technical concerns include loophole(s) in cyber security, password strength,

computer backdoors and other weak points that hackers can exploit (Priebe 2014). The lessons learned here include a company's realization that some money and effort must be spent in security, not only physical security, but cyber security. These steps include a robust training program, an employee handbook with all the security procedures, a review of that handbook each year and signed every time it is reviewed. Computer screen warnings, a separate cyber security policy that is also reviewed and signed each year and an alert feature in the sensitive database(s) that tell cyber security when policies are being broken. The company's must consider the use of non-disclosure and non-compete agreements. The HR section must also be briefed and become sensitive to insider threat concerns. Disgruntled employees will display escalation in being upset at the company. This should be shared with managers and security. More details will be covered in best practices regarding threat assessment teams.

B. Best Practices

The federal authorities tried for many years to assist companies in protecting their TS/IP through the patent and copyright laws. The government saw that IP is another form of economic information, similar to trade secrets, that affects the well-being of America's economic success (H.Rept. 104-788). We saw in the lessons learned paragraphs that laws cannot be the only tools used to identify, stop and punish the people and companies that attempt to or have stolen another companies TS/IP. We will discuss the policies, practices and techniques that are suggested by legal experts as well as from the FBI.

Insider Threats

The sponsors of EEA 1996 saw the need to not only mention physical property as TS/IP, but to clearly spell out that intellectual property includes all manners of planning, developing and

production, to include even ideas. They even included the duplicating of information as well as the physical theft as a federal crime (H. Rept. 104-788). This is mainly focused on the trusted insider who has access to most, if not all of the company's TS/IP. This should be case by case access depending on position and responsibilities but is not always the situation. Once illegal conduct is detected, the most productive type of investigation would be the undercover investigation, this allows for the most productive technique for collecting evidence against the person/company attempting to have already taken the TS/IP. This type of investigation will allow investigators to determine the scope of the illegal activity, the number of people involved, their access and roles and possibly their motivations (Krotoski 2009).

The second type of investigation involving a trusted insider is the reactive investigation. This is the most common involving prosecutions under EEA 1996, where the company realizes the possible loss of TS/IP and notifies law enforcement. There is most likely a concern that the TS/IP is about to leave the U.S. or already has left the country. Federal law enforcement will conduct interviews, rely heavily on the company's cyber security to create a long history of the person's activity in and around the sensitive databases, collect evidence and work with the U.S. prosecutor to create a federal case against the person suspected of taking the TS/IP (Krotoski 2009).

These two types of investigations can also be used against the outside threat, but case studies have shown that at least 79.7% % of EEA 1996 18 USC 1832 criminal prosecutions involve the trusted insiders that were former or current employees. Prior to EEA 1996, cases during the 1950 to 2008 time frame involved someone that the owner of the TS/IP knew (Priebe 2014). Alternative charges have been used in trade secret and economic espionage cases to start the investigation/prosecution while the investigation continues to develop the trade secrets facts

(Krotoski 2009). The best practices recommendation here is for a company to realize that there are possibilities that the insider threat exist and to take the appropriate steps to identify and stop the theft of TS/IP.

Policies/Procedures

When using 18 U.S.C. §1832 to prosecute people/companies stealing TS/IP, the U.S. Attorney has established a checklist to assess initiating an economic or trade secret case in their U.S. Attorney's Manual. The steps in deciding to open an Economic Espionage case or Trade Secret case should include; scope and evidence of activity by a foreign government, foreign agent or foreign instrumentality is involved, the degree of the economic injury to the owner of the trade secret, the type of TS misappropriated, the effectiveness of available civil remedies and the potential deterrent value of the prosecution (Krotoski 2009). These are established and tested criteria to ensure that a successful prosecution is possible. A company that is concerned about possible theft of TS/IP or economic espionage must maintain a dialogue with the U.S. Attorney's office. This can be facilitated by the local federal law enforcement outreach program(s).

Prosecutions - Criminal and/or Civil

There are some reasons why economic espionage is not reported to federal and/or local authorities. There are other options available to the victim company that wants to keep the theft of the TS/IP as private as possible. They can conduct their own internal investigation, then fire the employee and file civil actions. We saw in the Epic, the historical IBM and AMSC cases that private firms and investigators were used. It is also possible that the amount of federal resources available to conduct the investigations is a limiting factor. These types of investigations can be

resource and time consuming (Priebe 2014). The lesson learned here is to research all available tools to use in either a criminal prosecution and/or civil court processes.

Some of the most common defense strategies used in trade secret and economic espionage cases will be reviewed in order to offer the victim company ways to prepare or defeat these past strategies. It is critical that the prosecutor or civil attorney for the plaintiff understand and evaluate the potential defenses early. Thomas Dougherty's Article, "Common Defense in Theft of Trade Secret Cases", provided the following common defenses published in the United States Attorney's Bulletin, November 2009; Tool kit defense, Knowledge of trade secret defense, Void for vagueness defense, Public disclosure defense, Reverse engineering defense and the Advice of counsel defense.

The Tool kit defense will involve the defense attorney trying to provide a plausible reason to explain why the person suspected of stealing the TS/IP removed the material and/or was in possession of the TS/IP. It must be proven beyond a reasonable doubt that the person who took the TS/IP intended to convert the TS/IP to economic benefit for someone other than the rightful owner. The following questions must be addressed in order for the tool kit defense to be possible; when did the employee access the TS/IP? Was the information taken related to the employee area of expertise? Did they have the authority to access the information while working at the company? Was the stolen TS/IP provided to another person at a new company of a possible new employer? What evidence supports the defendant's intent to convert the TS/IP and intent to injure the owner of the TS/IP?

The Knowledge of trade secret defense involves them claiming the defendant did not know that the information they took was a trade secret. However, the prosecutors do not have to prove they knew it was a trade secret but must prove that the defendant's actions were not

authorized by the owner of that information. If the defendant can prove that he had permission to take and use the TS/IP, then they would not be prosecuted.

The Void for vagueness defense attempts to prove that the wording in EEA 1996 and state statutes are too vague and not clearly explains the definition of a trade secret. They would also attempt to show that the term reasonable measures to protect the TS/IP was vague. It will be up to the prosecution team to show that the victim company is in compliance with both definitions. Defendants continue to challenge trade secret indictments as void for vagueness, however, the courts have consistently rejected these efforts.

The Public disclosure defense may argue that the TS/IP was already in the public domain or that the defendant believed it lawfully belonged to them. The prosecution will work closely with the victim company to show that the TS/IP was not publically known, such as in articles, public presentations, in a patent application or on the internet. There are instances when two parties have a legitimate dispute over who owns the TS/IP and are not typical of a criminal prosecution, but more suited for civil/private litigation.

The Reverse engineering defense relies heavily on the intent of the law makers responsible for EEA 1996 is as much as it states the intent is not to protect the owner of the TS/IP from discovery by fair and honest means. This can occur by independent invention, accidental disclosure or by so-called reverse engineering. However, the statutes do not protect the defendant if time consuming efforts, laboratory efforts and financial expense is not involved in the discovery of the TS/IP of the victim company. Therefore, this defense only is plausible if the TS/IP was readily attainable.

The Advice of counsel defense is only a plausible defense if the defendant can show that their legal counsel advised them that they could claim ownership of the TS/IP at issue. This will involve the defendant independently shows that they made full disclosure of all facts to their counsel before receiving advice. They could also show that they relied on good faith advice from the counsel that their conduct was legal (Doughtery 2009).

The following table will show how the companies can use these common defense strategies to plan their training and writing internal policies for an employee hand book to avoid these defenses being used.

The defense strategies will be listed and the three parts of trade secrets that address those will be listed as measures to ensure those strategies are not viable to the defendant. Trade secret under 18 U.S.C. § 1832 is defined as;

(1) Information (see page 7 for a full definition)

(2) Reasonable measures taken to protect the information and

(3) The TS derives independent economic value from not being publicly known (Priebe 2014).

Table 1 Lessons Learned for Common Defense Strategies

Possible Defense Strategy	Lessons Learned
Tool box	3 (It is made very clear that the TS/IP is the property of the company, no matter who created it.)
Knowledge of TS/IP	1, 3 (Clearly define the TS/IP in general terms and explain the need to protect it and what reasonable measures are in place.)
Void for vagueness	1, 2, 3 (The definition of a trade secret is clearly spelled out, what steps are in place to protect it and how they value of the TS/IP

	effect the economic wellbeing of the company is covered.)
Public disclosure	2 (Make it very clear on how the TS/IP is protected. Explain access and control measures in place.)
Reverse engineering	2 (Ensure that the reasonable measures are in place and that the employees understand the importance of protecting the TS/IP from accidental disclosure.)
Advice of counsel	1, 3 (Ensure that the definition of a trade secret is fully explained, that ownership of the TS/IP is by the owner.)

There are critical steps to consider when preventing the exposure of the TS/IP during either a criminal or civil court action. Use a general reference to the TS/IP in court documents that is protected by a previous court order. It might be possible to keep the victim company's name out of the court proceedings, using Company A or something else to mask the true company name, etc. (Krotoski 2009). Protective orders are also tools that can be used to protect the TS/IP. They are essential in the safeguarding the confidentiality of the TS/IP during every phase of a criminal case. There are three types of protective orders;

- A protective order may be needed before charges are filed in order to determine if a pre-indictment resolution of the case is possible.
- A protective order is filed after charges are filed, but before trial in order to restrict access to the TS solely to the defense attorneys defending the charges.
- A protective order is issued during the trial to control the use of the TS during the presentation of the case in a public forum.

Threat Assessment Team(s)

The federal law enforcement entities that conduct regular outreach to industry/businesses strongly support the creation and use of a Threat Assessment Team (TAT). This team can be used for violent concerns and to identify possible insider threats to TS/IP. These teams are primarily comprised of company internal resources; legal, human resources, information technology, security/cyber security (if different from IT), a management team representative and if only invited by the company, a federal law enforcement representative. The individual team members will cover the following roles;

Legal – ensures compliance with all legal matters with the best interest of the company in mind. Liaison to state or federal prosecutors. Provides advice to the company management.

HR- has access to employment records for any history of performance issues, any records of challenges outside the company, i.e. divorce, loss of a family members, prolonged illness, etc. Any records of complaints from inside the company and limited scope background checks prior to hiring. Records of any training conducted and agreements on file.

IT – training records for access to the company's computer networks. History of equipment assigned, logs of use, what devices are connected to the company networks, etc.

Security/Cyber – logs of access to building(s), security camera access, any history of prior security concerns. Liaison to local law enforcement for any issues that carry over to the work place. Cyber security is specialized in access log reviews and will be needed to provide reports to prosecutors and civil firms if the company pursues civil or private litigation.

Management – supervisor level attendees, specific to one person or a section of the company. They can address performance issues, prior complaints, co-worker grievances, etc. Maintains the

records of initial training and refresher training. Will know what the employee's regular work pattern looks like, will know if overseas trips have been approved, etc.

Federal LE – provides resources outside the company and local law enforcement capabilities. Can contact overseas resources if needed. Has access to prior cases and can determine the scope of the effort by the suspected insider.

The TAT will review cases brought to their attention by management or through reports to any of the team member sections. The will look for patterns of, but not limited to;

-any unreported travel.

-financial hardships in the near past.

-history of not getting promoted, job dissatisfaction.

-unexplained visits to the office outside their normal routine.

-attempts to access areas they do not have a need to permission to access.

-unexplained contact with competitors and indications of job hunting.

-disregarding company policies on personal software and hardware, abusing remote access, downloading restricted material, etc.

- showing concerns about being investigated or monitored.

-excessive copying and use of faxes, that leave little to no trial of use.

The TAT will determine if any mitigation is necessary and devise a plan to contact the employee, monitor their activities and/or get federal law enforcement involved. The legal counselor will determine which avenue to pursue if charges are necessary or if civil litigation is

determined the best route (FBI.gov insider threat). Companies should consider networking their TATs to allow for early detection of insider threat across a specific industry. Federal law enforcement outreach coordinators can assist with this effort.

V. Summary

Governments are tasked and entrusted with the responsibility to protect the people and the country's interest as a whole. The committee that brought H. Rept. 104-788-Economic Espionage Act forward to become law saw the need to stop the economic losses due to the outright theft of U.S. trade secrets/intellectual property and the impact it was having on the victim companies and employees. It is known worldwide that the United States is a leader in research & development, production and manufacturing. Even though the Economic Espionage Act of 1996 had teeth that included heavy fines and jail time, it was seen as inadequate and the Foreign and Economic Espionage Penalty Enhancement Act 0f 2012 filled a need to increase punishment even more for the criminal statute (Priebe 2014). President Obama also felt it necessary to bolster efforts to protect TS/IP and signed The Defend Trade Secrets Act of 2016 allowing private parties (victim companies) to seek civil remedies. This act goes into details on how the victim company is protected, details on what is protected and the rights of the trade secret owners (Neifeld 2016).

However, foreign sponsored espionage directed at company secrets is still growing. This can be seen in the Sinovel and Huawei cases and there are reports stating that foreign government sponsored acts have increased significantly to approximately 21% of all breaches. The Chinese Intelligence Services are the worst, but not the only sponsors of this kind of larceny. The Russian Intelligence Services are quieter and more selective than the Chinese, but they too are in the business of stealing intellectual property for commercial purposes. Taken together, the

theft of trade secrets and economic espionage are assaults on national economies in which jobs and wealth depend on innovation and intellectual property protection. By 2010, intellectual property intensive businesses accounted for more than a third of U.S. GDP and directly or indirectly, for nearly 28% of all U.S. jobs (Brenner 2014). The drafters of EEA 1996 saw the need to not only seek to stop the theft of TS/IP, to punish the people and countries involved, it was insightful enough to put guidelines in place to protect the TS/IP from disclosure during the trial process. They included language to preserve confidentiality in both criminal and civil court proceedings. They included this extra step even though the Federal Rules of Criminal and Civil Procedure and the Federal Rules of Evidence were already in place. The law is very clear that protective orders be prepared and ready to stop the directing of the disclosure of any trade secrets, both in the criminal and civil courts (H.Rept. 104-788).

Federal law has attempted to protect IP for many years through patent and copyright laws. EEA 1996 extended vital federal protection to an additional form of proprietary information, the trade secrets. Then the U.S. government has bolstered the statutes, made publicly directed admonishments to foreign leaders and the U.S. is still losing over $300 billion dollars a year to economic espionage/theft of trade secrets. EEA 1996 is not intended to be used to prosecute employees that change employers or start their own companies using knowledge and skills while employed. The act is designed to stop the efforts of those that take the information of a specific process or procedure in order to duplicate them to produce products for themselves or new employers in order to complete with their prior employer (H.Rept. 104-788).

Mendelsohn's Theory and Schafer's Functional Responsibility Theory gave us insight into how victim company's assume some of the responsibility in the theft and loss of their TS/IP and the resulting economic damage to the company. Companies must be savvier in the

realization that there are insiders and external threats to their technology, techniques and procedures. They must understand the need to be proactive in protecting their TS/IP, but also leaning forward in recognizing the insider threat and taking steps to identify and mitigate it ahead of time. The requirements of the EEA 1996 statutes does take some of the burden off the victim if they meet the reasonableness of protecting the trade secret and that it has value. However, some blame/responsibility can be addressed by examining the security culture, management and the industry's competition. If/when a theft of TS/IP has occurred, the company's must use all resources available to them to stop and punish the people/companies responsible.

We saw in the case examples that IBM and EPIC have taken things into their own legal hands recently by civilly being awarded $920 million dollars and $940 million dollars respectively (TSI Brooklaw). The Huawei case example also involves decision makers in policy and the intelligence community. There are fears that some of China's largest companies, which are state sponsored, are targeting U.S. TS/IP. This is being conducted in an effort to bolster China's economy and their corporations/companies close ties to the Chinese government could bolster political goals also. The Huawei case involving T-Mobile is the first time Huawei has admitted it had stolen portions of software from a U.S. company (Benner et al 2019).

There are also examples of U.S. companies acting as good corporate citizens as seen in the Coca-Cola and Wyko case examples. One of the main competitors to Coke, PepsiCo notified Coke of the offer to sell TS/IP to Pepsi, which led to a successful federal investigation and prosecution. The Wyko IT manager identified illegal photographs of Goodyear equipment and notified them which also led to a successful investigation and prosecution. These are great

examples of how the need to protect U.S. IP is even more vital to protecting U.S. companies and economic growth (CNN 2007).

The motivations to commit theft or economic espionage does an excellent job of putting into perspective why people would consider the theft of TS/IP. The most common is greed, with a mix of disgruntled and revenge for a recipe for theft that can harm a company. We saw in the AMSC case how a disgruntled, greedy and vengeful employee assisted a Chinese company in the theft of trade secrets to avoid paying licensing fees. AMSC suffered a loss estimated at $800 million dollars, $100 million in fees and $700 million in future earnings with Sinovel (WSJ). The Human Resources person testified that she had to fire 600 people because of the loss, 80 of them in the Middleton, Wisconsin office. She ultimately resigned/fired herself (Yahoo finance). The effects on economic espionage on the U.S. economy can have effects down to the company and community level. Laws attempt to slow or stop the thefts, but victim companies and their employees are still being assaulted annually.

Federal law enforcement has been conducting outreach for decades in efforts to inform and educate corporate America on what to look for regarding trusted insiders and others involved in stealing TS/IP. Besides understanding the motivations to conduct economic espionage, the following signs, behaviors and factors should also be considered. Working late hours outside their normal pattern, unnecessary copying of material, disregard for policies and directives, downloading confidential material and conduct unauthorized research and photography. Combine those early warning signs with the behaviors of unexplained short trips, life crisis spending and paranoia of being investigated should be indicators that trust is being violated. We saw some of these in the Wyko case example involving Goodyear's IP. The Wyko engineers

violated policies of no photography and the trusted access to steal and/or re-engineer a procedure needed for another contract (FBI. gov Economic Espionage).

The section on lessons learned and best practices explained that the U.S. government has taken steps over the years to high light the threat of economic espionage/theft of trade secrets. Laws have been passed, as well as, strong efforts by federal law enforcement to identify and stop those efforts to steal TS/IP. EEA 1996 ensures that tools are in place to allow the companies to seek punishment, send a message and attempt to recover monetary losses. EEA of 1996 offers some of those tools, the DTSA and the EEA penalty enhancements all can be used to reach this goal. However, it is up to the companies to decide which tools to use. It is recommended that U.S. companies put efforts into training and instilling the need to protect their TS/IP. Table 1 outlines teaching points that can be incorporated into employee handbook and policy agreements between the employees and the company. In the introduction examples of Valspar and Motorola, federal outreach had been conducted prior to the attempted theft and theft, respectfully. They chose to use 18 U.S.C. §1832 in criminal prosecutions. Those defendants were in the United States and were held accountable for their actions.

In the Epic and IBM cases using 18 U.S.C. §1836 and state statutes, the defendants were overseas and the foreign companies are not held accountable to repay or stop the criminal activity. They are outside the scope and jurisdiction of the U.S. court system and the authority of federal law enforcement. There are no records to date that the civil fines have been paid by either foreign company. The main take away from this research paper should be that U.S. companies work with federal agencies in designing and implementing TATs that their legal representation/departments maintain open dialog with the prosecutor's office and that industries strive to network regarding the identifying of threats to their technology.

VI. References

Benner, Mozur & Zhong 2019, Huawei Said to Be Under U.S. Investigation in Trade Secrets Case, New York Times. Retrieved on 05/26/2019 from https:///www.nytimes.com/2019/01/16/technology/huawei-investigation-trade-secrets.html

Burr 2013, Engineers Convicted for Theft of Trade Secrets, Blog Articles. Retrieved on 06/04/2019 from http://www.burr.com/2013/02/22/engineers-convicted-for-trade-secrets/

CNN, http://money.cn.com/2007/05/23/news/newsmaker/coke

Doughtery, T. (2009). Common Defense in Theft of Trade Secret Cases. *United States Attorneys' Bulletin, Economic Espionage and Trade Secrets, November 2009, Volume 57, Number 5*, 27-33.

Epic v. Tata, 10/31/2014, Case No. 14-CV-748, Demand for Jury Trial, Retrieved on 06/06/2019 from https://www.gallitanooconnor.com/file.asp?F=Epic%2DTata+Complaint%2Epdf&N=Epic%2DTata+Complaint%2Epdf&C=news

Farivar, January 19, 2018, Former IBM Developer Sentenced for Espionage, Theft of Trade Secrets. Retrieved on 5/27/2019 from https://www.voanews.com/a/ibm-chinese-developer-sentenced-for-economic-theft-of-trade-secrets/4215990.html

FBI Archives, March 2009, Former Paint Manufacturing Sentenced to 15 months in Prison for Stealing Trade Secrets Valued at $20 Million. Retrieved on 6/20/2019 from https://archives.fbi.gov/archives/chicago/press-release/20101cg090110-1.htm

FBI Counterintelligence, FBI.gov Brochures. Retrieved on 04/23/2018 from https://www.fbi.gov/investigate/counterintelligence

FBI Spotting Insider Threat, FBI.gov Brochures. Retrieved on 06/06/2019 from https://www.fbi.gov/file-repository/spotting-insider-threat_508.pdf.view

FBI The Insider Threat, FBI.gov Brochures. Retrieved on 06/06/2019 from https://fbi.gov/file-repository/insider_threat_brochure.pdf/view

FBI Economic Espionage, FBI.gov Brochures. Retrieved on 06/06/2019 from https://www.fbi.gov/file-repository/economic-espionage_508.pdf.view

FBI White Paper, April 2011, *Higher education and National Security: The Targeting of Sensitive, proprietary and Classified Information on Campuses of Higher Education*, http://FBI.gov/counterintelligence/strategicpartnership

H. Rept. 104-788. Retrieved on 03/12/2019 from https://www.congress.gov/congressional-report/104th-congress/house-report/788

Krotoski, M.L., 2009, Common Issues and Challenges in Prosecuting Trade Secrets and Economic Espionage Act Cases, United States Attorney Bulletin, November 2009, Volume 57, Number 5

NBCNews 2007, Third Defendant Gets Years in Coke Case, US Business, Retrieved on 06/05/2019 from http://www.nbcnews.com/id/19055773/ns/business-us_business/t/third-defendant-gets-years-coke-case/#.XPfMR2aWyUk

Neifeld 2016, Summary of the Defend Trade Secrets Act of 2016, Neifeld IP Law, Retrieved on 05/26/2019 from https://www.neifeld.com/pubs/Summary%20of%20the%20Trade%Secrets%20Acts%20of20201 6.pdf

Newby, T.G. (2009). Parallel Proceedings in Trade Secret and Economic Espionage Cases. *United States Attorneys' Bulletin, Economic Espionage and Trade Secrets, November 2009, Volume 57, Number 5,* 34-40.

Potts 1983, IBM Charges 2 Firms With Stealing Secrets, Washington Post, Retrieved on 05/29/2019 from https://www.washingtonpost.com/archive/business/1983/11/26/ibm-charges-2-firms-with-stealing-secrets/531c9098-4181-48e8-9794-97e05d88717e/?noredirect=on&utm_term=.02c9d2c8d180

Priebe,M.T., 2014, *The Economic Espionage Act of 1996: A 15 Year Review*, Grand Valley State University ScholarWork@GVSU

Reuters 2007, Ex-Coke aide gets 8 years in trade secrets case, Reuters Business News, Retrieved on 06/04/2019 from https://www.reuters.com/article/us-coke-tradesecrets/ex-coke-aide-gets-8-years-in-trade-secrets-case-idUSN2323386320070523

Tibbetts, S.G. & Hemmns, C., 2010, *Criminal Theory: A Text /Reader*, SAGE

Trelevon, E. (2018) "Jury: Sinovel guilty of stealing", *Wisconsin State Journal* 25 January 2018.

TSI Brookslaw 2013, http://tsi.brooklaw.edu/cases/united-states-america-v-clark-alan-roberts-and-sean-edward

USA v. Jin, Trade Secrets Institute, Court Imposes Four-Year Prison Sentence on Ex-Motorola Employee Caught with trade Secrets and a One-Way Ticket to China, Retrieved on 05/28/2019 from http://tsi.brooklaw.edu/category/legal-basis-trade-secret-claims/economic-espioange-act

US Attorney News Release, "Sinovel Corporation and Three Individuals charged in Wisconsin with Theft of AMSC Trade Secrets", June 27, 2013, FBI.gov archives

Wallace, H. & Roberson, C., 2015, *Victimology: Legal, Psychological and Social Perspectives*, Pearson Education Inc., Prentice Hall

Wikipedia-motivations, Retrieved 04/20/2018 from https://en.wikipedia.org/wiki/Motives_for_spying

Yahoo Finance 2018, Epic Systems wins $940 Million, Yahoo Finance's Morning Brief Newsletter. Reteived on 2/23/2018 from https://finance.yahoo.com/news/epic-systems-wins-940-million-032159510.html

Annex A

104TH CONGRESS REPORT
***2d Session* "HOUSE OF REPRESENTATIVES! 104–788**
ECONOMIC ESPIONAGE ACT OF 1996
SEPTEMBER 16, 1996.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed
Mr. MCCOLLUM, from the Committee on the Judiciary, submitted the following

R E P O R T

[To accompany H.R. 3723]
[Including cost estimate of the Congressional Budget Office]
The Committee on the Judiciary, to whom was referred the bill (H.R. 3723) to amend title 18, United States Code, to protect proprietary economic information, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:
Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.
This Act may be cited as the ''Economic Espionage Act of 1996''.

SEC. 2. PROTECTION OF TRADE SECRETS.
(a) IN GENERAL.—Chapter 31 of title 18, United States Code, is amended by adding at the end the following:
''§ 670. Protection of trade secrets
''(a) OFFENSE.—Whoever—

‘‘(1) with the intent to, or with reason to believe that the offense will, benefit any foreign government, foreign instrumentality, or foreign agent; or ‘‘(2) with the intent to divert a trade secret, that is related to or is included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and with the intent to, or with reason to believe that the offense will, disadvantage any owner of that trade secret; wrongfully copies or otherwise controls a trade secret, or attempts or conspires to do so shall be punished as provided in subsection (b).

‘‘(b) PUNISHMENT.—

‘‘(1) GENERALLY. — The punishment for an offense under this section is—
‘‘(A) in the case of an offense under subsection (a) (1), a fine under this title or imprisonment for not more than 25 years, or both; and
‘‘(B) in the case of an offense under subsection (a)(2), a fine under this title or imprisonment for not more than 15 years.
‘‘(2) INCREASED MAXIMUM FINE FOR ORGANIZATIONS.—If an organization commits an offense—
‘‘(A) under subsection (a) (1), the maximum fine, if not otherwise larger, that may be imposed is $10,000,000; and
‘‘(B) under subsection (a) (2), the maximum fine, if not otherwise larger, that may be imposed is $5,000,000.
‘‘(c) DEFINITIONS. — As used in this section—
‘‘(1) the term ‘foreign instrumentality’ means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government; ‘‘(2) the term ‘foreign agent’ means any officer, employee, proxy, servant, delegate, or representative of a foreign government;
‘‘(3) the term ‘trade secret’ means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
‘‘(A) the owner thereof has taken reasonable measures to keep such information secret; and
‘‘(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and
‘‘(4) the term ‘owner’, with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.
‘‘(d) CRIMINAL FORFEITURE.—
‘‘(1) Notwithstanding any other provision of State law, any person convicted of a violation under this section shall forfeit to the United States—
‘‘(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
‘‘(B) any of the person’s property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

‘‘(2) The court, in imposing sentence on such person, shall order, in addition to any other sentence imposed pursuant to this section, that the person forfeit to the United States all property described in this section.
‘‘(3) 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 the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections
(d) and (j) of such section, which shall not apply to forfeitures under this section.
‘‘(e) ORDERS TO PRESERVE CONFIDENTIALITY.—In any prosecution or other proceeding under this section, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.
‘‘(f) CIVIL PROCEEDINGS TO ENJOIN VIOLATIONS.—

‘‘(1) GENERALLY.—The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.
‘‘(2) EXCLUSIVE JURISDICTION. — The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.
‘‘(g) TERRITORIAL APPLICATION.—
‘‘(1) This section applies to conduct occurring within the United States.
‘‘(2) This section also applies to conduct occurring outside the United States
if—
‘‘(A) the offender is—
‘‘(i) a United States citizen or permanent resident alien; or
‘‘(ii) an organization substantially owned or controlled by United
States citizens or permanent resident aliens, or incorporated in the
United States; or
‘‘(B) an act in furtherance of the offense was committed in the United
States.
‘‘(h) NONPREEMPTION OF OTHER REMEDIES. — This section shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret
‘‘(i) EXCEPTIONS TO PROHIBITION.—
‘‘(1) This section does not prohibit and shall not impair any otherwise lawful activity conducted by an agency or instrumentality of the United States, a
State, or a political subdivision of a State.
‘‘(2) This section does not prohibit the reporting of any suspected criminal activity to any law enforcement agency or instrumentality of the United States, a State, or a political subdivision of a State, to any intelligence agency of the United States, or to Congress.’’.
(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 31, United States Code, is amended by adding at the end the following new item:
‘‘670. Protection of trade secrets.’’.

SEC. 3. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF
ORAL COMMUNICATIONS.

Section 2516(1)(c) of title 18, United States Code, is amended by inserting ''section 670 (relating to economic espionage),'' after ''(bribery in sporting contests),''.

PURPOSE AND SUMMARY

H.R. 3723, the Economic Espionage Act of l996, creates a new crime of wrongfully copying or otherwise controlling trade secrets, if done with the intent either to (1) benefit a foreign government, instrumentality, or agent, or (2) disadvantage the rightful owner of the trade secret and for the purpose of benefitting another person.

The term ''trade secret'' is defined in the bill to include all types of financial, business, scientific, technical, economic, or engineering information, whether tangible or intangible, and regardless of the means by which the information is stored, compiled, or memorialized.

The definition of the term trade secret also requires both that the owner of the information have taken some reasonable measures to keep the information secret and that the information derives independent economic value from not being generally known to the public and not being readily ascertainable through legal means. This new crime applies to conduct occurring in the United States and also to conduct occurring outside the United States provided, in the latter instance, that the offender is either a United States person or resident alien, an organization substantially owned or controlled by a United States citizen or permanent resident, or an organization incorporated in the United States; or that an act in furtherance of the offense was committed in the United States.

The bill provides for punishments consisting of a fine, imprisonment, or both. The maximum term of imprisonment is 25 years if the criminal act was done with the intent to benefit a foreign government and 15 years in all other cases. The bill also provides for a significantly increased maximum fine if the crime is committed by an organization. If the intent of the organization was to benefit a foreign government, the maximum fine that may be imposed under the bill is $10 million. In all other cases the maximum fine that may be imposed on an organization committing this crime is $5 million. The bill requires courts hearing cases brought under the statute to enter such orders as may be necessary to protect the confidentiality of the information involved in the case. The bill also empowers the Attorney General to file a civil action, in advance of the commencement of the criminal case, in order to obtain appropriate injunctive relief against a violation of the new criminal section. The bill provides for criminal forfeiture of the proceeds of the crime and limited forfeiture of the property used to commit the crime. Finally, the bill amends the wiretap statute to authorize the interception of communications in furtherance of the new crime when such interceptions are approved by a federal court.

BACKGROUND AND NEED FOR THE LEGISLATION

INTRODUCTION

For many years federal law has protected intellectual property through the patent and copyright laws. With this legislation, Congress will extend vital federal protection to another form of proprietary economic information—trade secrets. There can be no question that the development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interests.

GROWING IMPORTANCE OF PROPRIETARY ECONOMIC INFORMATION

The United States produces the vast majority of the intellectual property in the world. This category of property includes patented inventions, copyrighted material, and proprietary economic information. Trade secrets, in contrast with copyrighted material and patented inventions, are information as to which owners take steps to keep confidential. The value of the information is almost entirely dependent on it being closely held. It includes, but is not limited to, information such as production processes, bid estimates, production schedules, computer software, and technology schematics. 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 l992, they represented only 38 percent of the market value. As the 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 easier to steal. 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 companies or line their own pockets. In other instances, outsiders target a company, systematically infiltrate it, and then steal its vital information. More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies. The term economic or industrial espionage is appropriate in these circumstances. 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 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. The phrase industrial espionage includes 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, or 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 problems. Each will be punished under this bill.

At hearings before the Subcommittee, Louis Freeh, the Director of the Federal Bureau of Investigation, testified that the FBI is currently investigating reports and allegations of economic espionage activities conducted against the United States by individuals or organizations from 23 different countries. Some of these governments are ideological and military adversaries which continue to target U.S. economic and technological information as an extension of the concerted

intelligence assault on the United States conducted throughout the cold war. Other governments targeting U.S. economic and technological information are longtime political and military allies of the United States or have been traditionally neutral. These countries target the United States despite their friendly relations with our government and, in some cases, take advantage of their considerable legitimate access to U.S. information to collect sensitive information more easily than our traditional adversaries. Some of these countries find no contradiction in maintaining a military alliance with the United States while at the same time using their intelligence services to target U.S. technologies. Incidents of economic espionage are not limited to foreign governments or foreign companies.

A recent survey by the American Society for Industrial Security International noted that foreign nationals had been identified in 21% of incidents involving intellectual property loss where the nationality of the perpetrators was known. In cases not involving a foreign government or a company, the perpetrator of the theft of intellectual property was an individual with a trusted relationship with the company, often an employee or former employee, retiree, contractor, vendor supplier, consultant or business partner. The survey noted that there has been a 323% increase in reported incidents since a survey four years ago. That study estimates the potential losses for all American industry could amount to $63 billion annually.

NEED FOR LEGISLATION

At the hearing before the Subcommittee, Director Freeh testified that the FBI has experienced difficulties in prosecuting cases of economic espionage. While the FBI attempts to use various criminal statutes currently in force to investigate and prosecute this crime, these laws do not specifically cover the theft or improper transfer of proprietary information and, in the opinion of Director Freeh, are insufficient to protect this type of information. He testified further that in some instances, the FBI has conducted investigations only to have federal prosecutors decline the FBI's request to use further investigative procedures or to actually prosecute the case itself out of a concern over the lack of statutory criminal authority to do so.

The principal problem appears to be that there is no federal statute directly addressing economic espionage or which otherwise protects proprietary information in a thorough, systematic manner. The statute that federal prosecutors principally rely upon to combat this type of crime, the Interstate Transportation of Stolen Property Act (18 U.S.C. § 2314), was passed in the 1930s in an effort to prevent the movement of stolen property across State lines by criminals attempting to evade the jurisdiction of State and local law enforcement officials. That statute relates to ''goods, wares, or merchandise.'' Consequently, prosecutors have found it not particularly well suited to deal with situations involving ''intellectual property,'' property which by its nature is not physically transported from place to place. Courts have been reluctant to extend the reach of this law to this new type of property. One court has held that ''the element of physical 'goods, wares, or merchandise' in sections 2314 and 2315 is critical. The limitation which this places on the reach of the Interstate Transportation of Stolen Property Act is imposed by the statute itself and must be observed.'' *United States* v. *Brown,* 925 F.2d 1301 (10th Cir. 1991). Other statutes on which the government relies to prosecute this type of crime, such as the mail fraud statute or the fraud by wire statute, have also proved limited in their use. The mail fraud statute is only applicable when the mails are used to commit the criminal act and the fraud by wire statute requires proof that wire, radio, or television technology was used to commit the crime.

State laws also do not fill the gaps left by federal law. While the majority of States have some form of civil remedy for the theft of proprietary economic information, either by recognizing a tort for the misappropriation of the information or by enforcing contracts governing the use of the information, these civil remedies often are insufficient. Many companies choose to forego civil litigation because of the difficulties in enforcing a monetary judgment against some defendants which may have few assets or foreign governments with few assets in the United States or because companies do not have the resources or time to bring the civil action. Additionally, private individuals and companies lack the investigative resources necessary to prove that a defendant has in fact misappropriated the proprietary economic information in question. Only a few States have any form of criminal law dealing with the theft of this type of information and most of those laws are misdemeanors, rarely used by State prosecutors.

These problems underscore the importance of developing a systematic approach to the problem of economic espionage. The Committee believes that such a scheme will serve as a powerful deterrent to this type of crime. Additionally, a comprehensive federal criminal statute will better facilitate the investigation and prosecution of this crime.

GENERAL INTENTIONS OF THE COMMITTEE

This legislation is not intended to apply to innocent innovators or to individuals who seek to capitalize on the personal knowledge, skill, or abilities they may have developed. The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed. It is the intent of Congress, however, to make criminal the act of employees who leave their employment and use their knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer.

H.R. 3723 has been drafted so as to minimize the risk that the statute will be used to prosecute persons who use generic business knowledge to compete with former employers. For example, under the new offense the government is required to prove that the defendant has wrongfully copied or otherwise exerted control over a ''trade secret.'' The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it. It is important to note, however, that an owner of this type of information need only take ''reasonable'' measures to protect this information. While it will be up to the court in each case to determine whether the owner's efforts to protect the information in question were reasonable under the circumstances, it is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation. The new statute also requires that the government prove that the defendant wrongfully copied or otherwise controlled a trade secret. It is the Committee's intent that the phrase ''copies or otherwise controls'' be read broadly to include virtually any means by which information can be recorded, altered, or otherwise manipulated. This phrase includes both the taking of physical possession of the medium on which the information is stored, recorded, or otherwise memorialized as well as situations where the information has been copied, duplicated, photographed, drawn, or otherwise reproduced in some form from the original and where the

original information continues to remain in the possession of the owner. This concept of control also includes situations in which the information has been transmitted from one place to another (regardless of whether by electronic means, through the mails, or by person), even if in transmitting the information it continues to remain in the possession of its rightful owner. The concept of control also includes the mere possession of the information, regardless of the manner by which the non-owner gained possession of the information.

HEARINGS

The Committee's Subcommittee on Crime held one day of hearings on H.R. 3723 on May 9, 1996. Testimony was received from Louis Freeh, Director of the Federal Bureau of Investigation; Tom Brunner, U.S. Chamber of Commerce; Dr. James P. Chandler, George Washington University; Dr. Raymond Damadian, President, Fonar Corp.; Richard J. Heffernan, American Society of Industrial Security; Pete McCloskey, President, Electronic Industries Association; John Melton, Vice President SDL, Inc.; David Shannon, Senior Counsel, Intel Corporation; Dan Whiteman, Director of Security, General Motors; with additional material submitted by Hughes Corporation.

COMMITTEE CONSIDERATION

On July 10, 1996, the Subcommittee on Crime met in open session and ordered reported the bill H.R. 3723, by a voice vote, a quorum being present. On September 11, 1996, the Committee met in open session and ordered reported favorably the bill H.R. 3732 with one amendment in the nature of a substitute by voice vote, a quorum being present.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 2(l)(3)(A) of rule XI of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT FINDINGS

No findings or recommendations of the Committee on Government Reform and Oversight were received as referred to in clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 2(l)(3)(B) of House rule XI is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 2(l)(C)(3) of rule XI of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 3723, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 403 of the Congressional Budget Act of 1974: U.S. CONGRESS, CONGRESSIONAL BUDGET OFFICE, *Washington, DC, September 16, 1996.* Hon. HENRY J. HYDE, *Chairman, Committee on the Judiciary, House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has reviewed

H.R. 3723, the Economic Espionage Act of 1996, as ordered reported by the House Committee on the Judiciary on September 11, 1996. CBO estimates that enacting the bill would result in additional discretionary spending of about $3 million over the 1997–2002 period, subject to the availability of appropriated funds. Enacting H.R. 3723 would affect direct spending and receipts by increasing the amount of forfeiture receipts and penalties collected and spent by the government. We estimate that the collection of such receipts would total about $10 million through fiscal year 1998 and the spending of such receipts would total about $5 million over the same period. Because enacting the bill would affect direct spending and receipts, it would be subject to pay-as-you-go procedures. However, we expect that the forfeiture and penalty provisions would have no significant net effect 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 H.R. 3723 would make the misappropriation of a trade secret a federal crime. Under current law, cases involving the theft of trade secrets are prosecuted under various statutes; however, none is broad enough to accommodate most cases involving the unauthorized use of such material. Under this bill, trade secrets 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. In addition, this bill would enable the Attorney General to obtain court injunctions as relief against any violations of this bill and would enable the federal government to investigate offenses under this bill through the use of authorized wire, oral, or electronic intercepts.

Federal Budgetary Impact. — Based on information from the Federal Bureau of Investigation (FBI), CBO expects that the agency's caseload would increase as a result of enacting H.R. 3723. We estimate that, over the next six years, the government would most likely investigate and prosecute a total of about 50 cases covered by this legislation. While pursuing investigations would consume staff time and other resources of the federal government, CBO estimates that the Department of Justice and the FBI would not need significant additional resources to enforce the provisions of the bill over the next two years. However, after fiscal year 1999, resource needs could exceed $1 million each year to support the increasing caseload. CBO estimates that resource needs could total about $3 million from fiscal year 1999 through fiscal year 2002. 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 its provisions. Criminal fines and receipts from the sale of forfeited property would be deposited in the Crime Victims Fund and spent in the following year. CBO estimates that the government would collect additional fines and receipts from the sale of forfeited property of about $10 million through fiscal year 1998. Based on information from the FBI, we estimate that additional receipts paid into the Crime Victims Fund after fiscal year 1998 could exceed $10 million a year. Spending from the fund would increase by the same amounts, but with a one-year lag. CBO does not expect any significant increase in prison costs as a result of this bill. The following table summarizes the pay-as-you-go effects of enacting this bill

.

[By fiscal year, in millions of dollars]

	1996	1997	1998
Change in outlays	0	0	5

Change in receipts ----------055

Mandate Statement.—H.R. 3723 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 contact is Susanne S. Mehlman. Sincerely, JUNE E. O'NEILL, *Director.*

INFLATIONARY IMPACT STATEMENT
Pursuant to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the Committee estimates that H.R. 3723 will have no significant inflationary impact on prices and costs in the national economy.

SECTION-BY-SECTION ANALYSIS
Section 1. TITLE.—Section 1 states the short title of the bill as the ''Economic Espionage Act of 1996.''
Section 2. PROTECTION OF TRADE SECRETS. This section adds a new section to Chapter 31 of Title 18 of the United States Code. The new section, section 670, creates the crime of wrongfully copying or otherwise controlling a trade secret.

Section 670(a)—OFFENSE.—Subsection (a) of new section 670 creates the criminal offense involving the misappropriation of trade secrets. The offense provides that anyone who ''wrongfully copies or otherwise controls'' a trade secret, or attempts or conspires to do so, shall be punished in accordance with subsection (b) of that section. In order for a violation of the statute to be proven, the government must also prove that the defendant committed the offense either

(1) with the intent to, or with reason to believe that the offense would, benefit any foreign government, foreign instrumentality, or foreign agent, or (2) with the intent to divert a trade secret related to, or included in, a product that is produced for, or placed in, interstate or foreign commerce, to the use or benefit of anyone other than the owner of the trade secret and with the further intent to, or with reason to believe that the offense would, disadvantage the owner of that trade secret.

This section punishes the theft, unauthorized appropriation or conversion, duplication, alteration, or destruction of a trade secret. This section is intended to cover both traditional instances of theft, where the object of the crime is removed from the rightful owner's control, as well as non-traditional methods of misappropriation or destruction that involve duplication or alteration. When these nontraditional methods are used the original property never leaves the control of the rightful owner, but the unauthorized duplication or misappropriation effectively destroys the value of what is left with the rightful owner. Given the increased use of electronic information systems, information can now be stolen and the original usually remains intact. The intent of this statute, therefore, is to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished.

This section requires that the government prove that the person charged with the crime acted with the intent to accomplish one of two goals. One, a person will be guilty under this section if

they wrongfully copied or otherwise controlled a trade secret with the intent to benefit any foreign government, foreign instrumentality or foreign agent. In this instance, ''benefit'' is intended to be interpreted broadly. The defendant did not have to intend to confer an economic benefit to the foreign government, instrumentality, or agent, to himself, or to any third person. Rather, the government need only prove that the actor intended that his actions in copying or otherwise controlling the trade secret would benefit the foreign government, instrumentality, or agent in any way. Therefore, in this circumstance, benefit means not only an economic benefit but also reputational, strategic, or tactical benefit. Alternatively, the government may prove that the defendant intended the misappropriated trade secret to be used for the economic benefit of a person other than the rightful owner (which can be the defendant or some other person or entity). In this situation (i.e., when the defendant does not act with the intent to benefit a foreign government, instrumentality, or agent) the government must prove that the defendant intended to confer an economic benefit, not an abstract benefit or reputational enhancement, through his actions. Therefore, a person who discloses a trade secret but who does not intend to gain economically from it or intends that some other person economically gain from trade secret, cannot be prosecuted under this section. Additionally, when the defendant does not act with the intent to benefit a foreign government, instrumentality, or agent, the government must also show that the defendant intended to disadvantage the rightful owner of the information.

This additional provision does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner. While the term ''wrongfully'' is not defined in the statute specifically, the use of the term in this section involves the defendant's knowledge that his or her actions in copying or otherwise exerting control over the information in question was inappropriate. It is not necessary that the government prove that the defendant knew his or her actions were illegal, rather the government must prove that the defendant's actions were not authorized by the nature of his or her relationship to the owner of the property and that the defendant knew or should have known that fact.

Section 670(b)—PUNISHMENT. — The bill provides for several types of punishment, including fines, imprisonment, or both. The maximum term of incarceration varies depending upon the intent of the person convicted of the crime. If the defendant's intent was to benefit a foreign government, foreign instrumentality, or foreign agent the maximum term of imprisonment is 25 years. In all other cases, the maximum term of imprisonment is 15 years. If an organization commits an offense under the section, the maximum fine amount is substantially increased from that otherwise provided under title 18. If an organization commits an offense involving an intent to benefit a foreign government, foreign instrumentality, or foreign agent the maximum fine which may be imposed is $10 million. In all other circumstances, the maximum fine which may be imposed on an organization violating section 670 is $5 million.

Subsection (c)—DEFINITIONS.—Subsection (c) of new section 670 provides for definitions of some of the key terms used in the section. The definition of the term ''trade secret'' is based largely on the definition of that term in the Uniform Trade Secrets Act. As defined in H.R. 3723, ''trade secret'' means all forms and types of financial, business, scientific, technical, economic, or engineering information'' if certain conditions exist, as discussed below. This information

includes patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether such properties are tangible or intangible, and regardless of the means by which such property is stored or compiled, or memorialized physically, electronically, graphically, photographically, or in writing. These general categories of information are included in the definition of trade secret for illustrative purposes and should not be read to limit the definition of trade secret. It is the Committee's intent that this definition be read broadly.

As defined in the bill, however, in order for information to meet the definition of trade secret, two conditions must be proven to have existed at the time the defendant copied or otherwise exerted control over the information. First, the owner of the information must have taken reasonable measures to keep such information secret. Secret in this context means that the information was not generally known to the public or to the business, scientific, or educational community in which the owner might seek to use the information. The bill requires the owner to take only ''reasonable measures'' to keep such information secret. The fact that the owner did not exhaust every conceivable means by which the information could be kept secure does not mean that the information does not satisfy this requirement. Rather, a determination of the ''reasonableness'' of the steps taken by the owner to keep the information secret will vary from case to case and be dependent upon the nature of the information in question.

The definition of trade secret also requires that the information in question derive independent economic value, whether actual or potential, from the fact that the information is not generally known to, and not readily ascertainable through proper means by, the public. Therefore, information which is generally known to the public, or which the public can readily ascertain through proper means, does not satisfy the definition of trade secret under this section. The term ''owner'' is defined to include the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret in reposed. In this case, owner includes both natural persons as well as organizations (such as corporations and partnerships) entitled to own property. It also includes federal, state, and local government organizations, as well as foreign government organizations.

Subsection (d)—CRIMINAL FORFEITURE. — This section is designed to permit forfeiture of both the proceeds and assets used to facilitate the commission of the offense described in the bill. This section requires that any person convicted of a violation of section 670 shall forfeit all property constituting, or derived from, any proceeds the person obtained as the result of such violation, regardless of whether the proceeds were obtained directly or indirectly from the criminal conduct. This section also requires that the person convicted of violating section 670 forfeit any of the person's property used, or intended to be used, to commit or facilitate the crime. But this section further provides, however, that in determining the extent of the property to be forfeited, the court may take into consideration the nature, scope, and proportionality of the use of the property in the offense. The intent of this proviso is to minimize the number of instances in which the property forfeited is disproportionate to the harm caused by the defendant's conduct.

The forfeiture provision supplements, and is in addition to, the authorized punishments in the bill. The subsection incorporates existing law that sets forth procedures to be used in the detention, seizure, forfeiture, and ultimate disposition of property forfeited under this subsection.

Subsection (e)—ORDERS TO PRESERVE CONFIDENTIALITY.—This subsection authorizes the court to preserve the confidentiality of alleged trade secrets during legal proceedings consistent with existing rules of criminal procedure, civil procedure, and evidence, and other applicable laws. The intent of this section is to preserve the confidential nature of the information and, hence, its value. Without such a provision, owners may be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth.

Subsection (f)—CIVIL PROCEEDINGS TO ENJOIN VIOLATIONS.—
This section empowers the Attorney General to commence a civil action in the United States District Courts to obtain injunctive relief against a violation of new section 670. The standards for obtaining such injunctive relief are to be those provided for under the Federal Rules of Civil Procedure. The district courts shall have exclusive jurisdiction over actions brought under this subsection. This subsection is neither intended to create a general civil cause of action nor does it authorize persons other than the Attorney General to commence a civil action to enjoin a violation of section 670.

Subsection (g)—TERRITORIAL APPLICATION .— To rebut the general presumption against the extraterritoriality of U.S. criminal laws, this subsection makes it clear that the Act is meant to apply to the specified conduct occurring beyond U.S. borders. To ensure that there is some nexus between the ascertaining of such jurisdiction and the offense, however, extraterritorial jurisdiction exists only if the offender is a United States citizen or permanent resident alien, an organization substantially owned or controlled by United States citizens or permanent resident aliens or is incorporated in the United States. Alternatively, extraterritorial jurisdiction will exist if an act in furtherance of the offense was committed in the United States.

Subsection (h)—NON-PREEMPTION OF OTHER REMEDIES. — This subsection makes it clear that the act does not preempt non-federal remedies, whether civil or criminal, for dealing with the theft or misapplication of trade secrets. In particular, the fact that the Attorney General is authorized (under subsection (f) of section 670) to commence civil proceedings in order to enjoin further conduct which would violate section 670 is not to be interpreted to mean that other persons and entities may not also seek injunctive relief that may be available in other civil actions (using state law tort or contract claims) in order to prevent the further misuse of a trade secret.

Subsection (i)—EXCEPTIONS TO PROHIBITION.—The Act does not prohibit, and is not to be deemed to impair, any otherwise lawful activity conducted by an agency or instrumentality of the United States, a State, or political subdivision of a State. This subsection is intended to make it clear that the act does not prohibit any lawfully authorized investigative, protective, or intelligence activity by one of those government entities. This subsection also makes it clear that it is not a violation of section 670 to report suspected criminal activity to a law enforcement

agency or instrumentality of the United States, a State, or political subdivision of a State, to any intelligence agency of the United States, or to Congress.

Section 3. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS. — This section adds new section 670 to the list of offenses which may be investigated through the use of authorized, wire, oral, or electronic intercepts. This section does not alter the existing standard or procedures for obtaining the authorization to conduct such intercepts.

AGENCY VIEWS
Agency views were submitted to the Committee with respect to H.R. 3723.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED
In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE
PART I—CRIMES
* * * * * * *
CHAPTER 31—EMBEZZLEMENT AND THEFT
Sec.
641. Public money, property or records.
* * * * * * *
670. Protection of trade secrets.
* * * * * * *
§ 670. Protection of trade secrets
(a) OFFENSE.—Whoever—
(1) with the intent to, or with reason to believe that the offense will, benefit any foreign government, foreign instrumentality, or foreign agent; or
(2) with the intent to divert a trade secret, that is related to or is included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and with the intent to, or with reason to believe that the offense will, disadvantage any owner of that trade secret; wrongfully copies or otherwise controls a trade secret, or attempts or conspires to do so shall be punished as provided in subsection (b).
(b) PUNISHMENT.—
(1) GENERALLY — The punishment for an offense under this section is—
(A) in the case of an offense under subsection (a)(1), a fine under this title or imprisonment for not more than 25 years, or both; and
(B) in the case of an offense under subsection (a)(2), a fine under this title or imprisonment for not more than 15 years.
(2) INCREASED MAXIMUM FINE FOR ORGANIZATIONS. — If an organization commits an offense—

(A) under subsection (a)(1), the maximum fine, if not otherwise larger, that may be imposed is $10,000,000; and
(B) under subsection (a)(2), the maximum fine, if not otherwise larger, that may be imposed is $5,000,000.
(c) DEFINITIONS .— As used in this section—
(1) the term ‘‘foreign instrumentality’’ means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;
(2) the term ‘‘foreign agent’’ means any officer, employee, proxy, servant, delegate, or representative of a foreign government;
(3) the term ‘‘trade secret’’ means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
(A) the owner thereof has taken reasonable measures to keep such information secret; and
(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and
(4) the term ‘‘owner’’, with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.
(d) CRIMINAL FORFEITURE.—
(1) Notwithstanding any other provision of State law, any person convicted of a violation under this section shall forfeit to the United States—
(A) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
(B) any of the person’s property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.
(2) The court, in imposing sentence on such person, shall order, in addition to any other sentence imposed pursuant to this section, that the person forfeit to the United States all property described in this section.
(3) 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 the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.
(e) ORDERS TO PRESERVE CONFIDENTIALITY. — In any prosecution or other proceeding under this section, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.
17

(f) CIVIL PROCEEDINGS TO ENJOIN VIOLATIONS.—
(1) GENERALLY.—The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.
(2) EXCLUSIVE JURISDICTION. — The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.
(g) TERRITORIAL APPLICATION.—
(1) This section applies to conduct occurring within the United States.
(2) This section also applies to conduct occurring outside the United States if—
(A) the offender is—
(i) a United States citizen or permanent resident alien; or
(ii) an organization substantially owned or controlled by United States citizens or permanent resident aliens, or incorporated in the United States; or
(B) an act in furtherance of the offense was committed in the United States.
(h) NONPREEMPTION OF OTHER REMEDIES. — This section shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret
(i) EXCEPTIONS TO PROHIBITION.—
(1) This section does not prohibit and shall not impair any otherwise lawful activity conducted by an agency or instrumentality of the United States, a State, or a political subdivision of a State.
(2) This section does not prohibit the reporting of any suspected criminal activity to any law enforcement agency or instrumentality of the United States, a State, or a political subdivision of a State, to any intelligence agency of the United States, or to Congress.

* * * * * * *

CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS 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 or acting 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—
(a) * * *
* * * * * * *
(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224

(bribery in sporting contests), *section 670 (relating to economic espionage)*, subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), and section 1341 (relating to mail fraud), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), or section 1992 (relating to wrecking trains);

* * * * * * *

®