Journal of International Business and Law

Volume 15 | Issue 1 Article 4

1-1-2015

The Need for Modernization of the Economic Espionage Act of 1996

Lisa Capellupo

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/jibl

 Part of the Law Commons

Recommended Citation

Capellupo, Lisa (2015) "The Need for Modernization of the Economic Espionage Act of 1996," *Journal of International Business and Law*: Vol. 15: Iss. 1, Article 4.
Available at: https://scholarlycommons.law.hofstra.edu/jibl/vol15/iss1/4

This Notes & Student Works is brought to you for free and open access by Scholarship @ Hofstra Law. It has been accepted for inclusion in Journal of International Business and Law by an authorized editor of Scholarship @ Hofstra Law. For more information, please contact lawscholarlycommons@hofstra.edu.

THE NEED FOR MODERNIZATION OF THE ECONOMIC ESPIONAGE ACT OF 1996

*Lisa Capellupo**

I. INTRODUCTION

In September 2014, Senate investigators stated that Chinese state sponsored hackers had broken into the computer networks of private transportation companies in the U.S. twenty times in one year.[1] The hacked private transportation companies are responsible for moving military goods and troops across the globe.[2] The motivation behind this attack was an attempt by the Chinese to gain beneficial information. Similarly, in May 2014, the Department of Justice ("DOJ") released an indictment against five Chinese officers of the People's Liberation Army.[3] These defendants targeted makers of nuclear and solar technology in an attempt to gain confidential business information, sensitive trade secrets, and even various internal communications from these companies in order to gain a competitive advantage.[4] These two recent attacks on the United States demonstrate the modern day trend of espionage: economic espionage.

Economic espionage occurs when a foreign government sponsors, coordinates, or even assists in intelligence efforts directed at a domestic government or corporation.[5] Employing methods similar to those used in the retrieval of traditional espionage secrets, foreign "spies" are focused on obtaining trade secrets and intellectual property ("IP") from U.S. corporations. This is an increasingly substantial problem, as it has been estimated that U.S. IP, including trade secrets is valued at nearly half of the entire U.S. economy.[6] In an

---

* J.D. Candidate, Maurice A. Deane School of Law at Hofstra University, 2016. I would like to thank the staff of the *Journal of International Business & Law,* for giving me this opportunity and their excellent work in preparing this Note for publication. I would also like to thank my family, especially my sister Nicole Capellupo, for all your support and assistance during this process.

[1] Danny Yadron, *Chinese Hacked U.S. Military Contractors, Senate Panel Says*, WALL ST. JOURNAL (Sept. 18, 2014, 4:29 AM), http://www.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094.

[2] *Id.*

[3] *U.S. Files Economic Espionage Charges Against Chinese Military Hackers*, CBS NEWS (May 19, 2014, 8:25 AM), http://www.cbsnews.com/news/u-s-government-files-economic-espionage-charges-against-chinese-hackers-sources-say/ ("The DOJ specifically named "Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA),"...").

[4] *Id.*; *see also* Press Release, Dep't of Justice: Office of Pub. Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014) (stating the various techniques each individual used by the information which was obtained in these attacks).

[5] Darren S. Tucker, *The Federal Government's War on Economic Espionage*, 18 J. INT'L L. 1109, 1112 (2014); *Cf. Espionage Definition*, MERRIAM-WEBSTER, http:// www.merriam-webster.com/dictionary/espionage (last visited Feb. 15, 2015).

[6] Thomas A. Dye & T. Brooks Collins, TRADE SECRETS: CIVIL OR CRIMINAL ENFORCEMENT OF TRADE SECRET MISAPPROPRIATION, 2 Bloomberg Law Reports-Corporate Counsel (9th ed. 2011), *available at* http://www.cfjblaw.com/files/Publication/feb47d4d-58ba-4536-adf4-

Published by Scholarship @ Hofstra Law, 2015

effort to ward off this trend the United States Government enacted the Economic Espionage Act of 1996 ("EEA").[7] However, the results are not what the federal government imagined when the EEA was enacted in 1996.

This note will discuss all relevant aspects of the Economic Espionage Act of 1996, as well as the problems associated with the Act. Notable problems associated with the EEA include a lack of international law surrounding this field, international cooperation, training for federal prosecutors, and a severe punishment to deter future criminals. To remedy these issues, solutions should be adopted and implemented by the federal government to make this legislation as beneficial as originally intended. Solutions, which will be discussed in this note, include the adoption of a uniform international law to combat international economic espionage, the adoption of workplace solutions to combat internal economic espionage by foreign "spies," and the adoption of new legislation to cover the gaps of the EEA.

II. IMPORTANT TERMS DEFINED

A. Intellectual Property

Generally, intellectual property is a product of human thought and creativity.[8] IP is more widely known to cover literary images, designs, symbols and even names that are used in commerce.[9] More interestingly, IP is more valuable than real, tangible property due to the impact that it has on a corporation or business.[10] Specifically, as the assets of intellectual property can provide a significant competitive edge to their owner in their specific field.[11] The ramifications of losing such a competitive edge for a small or even medium sized business could be devastating to their business. This could result in not only a loss of money, but also a loss of stock, an increase in debt for the company, loss of investors, and eventually a complete shutdown.[12] To further illustrate this point, the misappropriation of intellectual property in general is $50 billion a year.[13]

5fd23cf80cbd/Preview/PublicationAttachment/8f30bf3e-90f3-4ad2-9904-61689aae7e7b/Bloomberg_article_civil_or_criminal_enforcement_of_trade_secret.pdf.

[7] *See generally* F.W. Rustmann, JR, *Legal Issues & The Economic Espionage Act Security World*, CTC Publications (Aug. 2000), http://www.ctcintl.com/Econ%20Espion%20Act.htm ("The economic espionage act was enacted to focus attention on the threat of foreign industrial spying, and to give the federal government a mechanism to prosecute offenders.").

[8] DEBORAH E. BOUCHOUX, PROTECTING YOUR COMPANY'S INTELLECTUAL PROPERTY 1 (Am. Mgmt. Ass'n ed., 2001).

[9] World Intellectual Property Organization [WIPO], *What is Intellectual Property?*, at 2, WIPO Pub. No. 450(E), http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.

[10] *See* BOUCHOUX, *supra* note 8, at 2.

[11] *Id.*

[12] Rick Newman, *10 Great Companies That Lost Their Edge*, U.S. NEWS: MONEY (Aug. 19, 2010, 10:39 AM), http://money.usnews.com/money/blogs/flowcharts/2010/08/19/10-great-companies-that-lost-their-edge.

[13] *Id.*

B. Trade Secret

IP is comprised of many different areas, one of which is trade secrets. A trade secret can be "all forms and types of financial, business, scientific, technical, economic, or engineering information."[14] In order for a trade secret to be a protected form of intellectual property, three requirements must be met. First, the original owner of the trade secret must have taken reasonable measures to protect the trade secret from others.[15] Second, the protected information must have some sort of economic value.[16] Finally, third, the protected information must be something, which cannot be easily obtained by the public.[17]

C. Economic Espionage

Economic espionage occurs when a foreign government sponsors, coordinates or even assists in intelligence efforts directed at a domestic government or corporation.[18] The foreign government is most often interested in targeting or acquiring trade secrets.[19] In recent years, the act of economic espionage has been steadily increasing against U.S. governments and corporations.[20] Most of the countries that have steadily been using their resources against the United States are France, Israel, China, Russia, Cuba and Iran.[21]

III. CURRENT TRENDS IN ECONOMIC ESPIONAGE

With the increasing popularity of the Internet in the last twenty years, persistent cyber espionage attacks on U.S. IP from foreign governments have occurred. These attacks threaten national security and the U.S. economy, resulting in unfair competitive advantages among domestic and foreign corporations.[22] Furthermore, recent studies have shown that misappropriation of trade secrets in relation to military technology has become increasingly popular.[23] Although many countries partake in economic espionage in general, and against the

---

[14] 18 U.S.C. § 1839 (2014).

[15] BOUCHOUX, *supra* note 8, at 193 (stating as long as the original owner of the trade secret is taking reasonable measures to protect the trade secret, then the secret will continue to be protected under intellectual property law); *See also* 18 U.S.C. § 1839.

[16] 18 U.S.C. § 1839.

[17] *Id.*

[18] Tucker, *supra* note 5, at 1112.

[19] *See id.* at 1111.

[20] *See id.* at 1115 (discussing a study conducted by the FBI showing the extent foreign governments and corporations have gone through to acquire U.S. trade secrets. Specifically how 100 countries out of 173 countries have spent money towards acquiring trade secrets, while 57 of those countries specifically have conducted covert operations to obtain these secrets).

[21] *Id.* at 1116 (describing the reasons why the U.S. is a highly sought after target for trade secret theft. This theft is largely due to the fact that the U.S. produces classified information/technology and products both in the realm of the government and private corporations, which holds a valuable economic value for other countries).

[22] H.R. REP. NO. 113-2281 (2013).

[23] Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 U.S. ATT'Y BULL. 2, 3 (2009).

U.S., the most active participant is China, while many other members of the World Trade Organization ("WTO") are following closely behind. [24]

There are many examples that illustrate current trends in economic espionage. In 2011, a Chinese national was sentenced to eighty-seven months in prison for committing two separate acts of economic espionage against the United States.[25] The criminal in this instance had stolen two distinct trade secrets and sold them to German and Chinese corporations and Chinese university students.[26] The act of selling this trade secret to university students grants China a substantial benefit. Research institutes are likely to easily replicate these trade secrets in a short amount of time and at a low cost, which would provide a large income when implemented by the government. This demonstrates a country using theft to their advantage. A separate incident involved Chinese military members who were indicted in Pennsylvania for hacking into numerous American businesses. This was an attempt to take beneficial trade secrets and implement them in China. These military members obtained unauthorized access to these companies' computers and took sensitive information regarding military strategies, with the hopes that the Chinese military would be able to use them to their advantage.[27]

Another notable cyber-attack was recently conducted by Russia. Over the past few years, Russian hackers launched a long-term cyber espionage attack on U.S. oil companies, entitled Energetic Bear.[28] This attack was primarily performed through the use of malware placed into oil companies' computers at the sites of power plants, energy grids, gas pipeline companies and industrial equipment makers.[29] Actions like this are what drastically impact the U.S. economy. If the hackers used this information to discover the reserves that one of those oil companies were planning on using, that foreign company could have the ability to beat the U.S. company to the punch and begin drilling in that location first. Such an action would be a major loss to both the oil company and the U.S. economy.

IV. ECONOMIC ESPIONAGE ACT

A. Statutes Used To Bring Economic Espionage Charges Under Prior to the EEA

Due to the lack of a uniform statute to bring economic espionage charges under prior to 1996, the federal government had used various other statutes to bring these charges against the accused. One of the acts, which was not ultimately effective, was the Computer Fraud and Abuse Act. The Computer Fraud and Abuse Act is primarily used when an individual intentionally accesses a computer without prior approval in order to obtain

---

[24] *Id.*; *See also* H.R. REP. NO. 113-2281.

[25] *Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets*, U.S. DEP'T OF JUSTICE (Dec. 21, 2011), http://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets [hereinafter *Chinese National*]

[26] *Id.*

[27] Ashley Fantz, *Chinese Hackers Infiltrated U.S. Companies, Attorney General Says*, CNN (May 19, 2014, 6:31 PM), http://www.cnn.com/2014/05/19/justice/china-hacking-charges/index.html?iid=EL.

[28] Jose Pagliery, *Russia Attacks U.S. Oil and Gas Companies in Massive Hack*, CNN (July 2, 2014), http://www.money.cnn.com/2014/07/02/technology/security/russian-hackers/?iid=EL.

[29] *Id.* (stating that such information that was obtained through the use of malware was sensitive information, primarily usernames and passwords to access oil companies' information).

confidential information.[30] However, the only information that is deemed protected under this act is information that was on a protected computer or a computer connected to the federal government.[31] Additionally, information that is used to injure the U.S. or give an advantage to a foreign nation can be prosecuted under this act, but only if it is obtained through a federal computer or in connection with one.[32]

The Computer Fraud and Abuse act on its own was not adequate to prosecute economic espionage. The main issue was that this act is only connected to protected information related to national defense. Information obtained from protected computers or federal computers could in fact contain trade secrets, which would be a connection to economic espionage. The overwhelming majority of thefts that occur are not actually related to the realm of national defense.[33] Accordingly, due to the narrow scope of this act, it was not a successful means of bringing economic espionage charges.

Prior to 1996, the Mail and Wire Fraud Statutes were also used to prosecute those who were charged with economic espionage. The Mail and Wire Fraud Statutes generally apply when one devises or intends to devise a scheme to fraudulently obtain money or property.[34] The activity must be done through the U.S. Post Office, private or commercial interstate carrier or means of wire, radio or television.[35] Nonetheless, this statute only has limited applicability. Mail fraud is only applicable when the mail was used to commit the criminal act, trade secret theft, while the fraud statutes require there be sufficient proof that a wire, radio or television was used to commit the actual criminal activity. [36]

Thus, only if trade secret theft occurred through these means could a charge be brought under this act. Due to the limited applicability of this statute, it is not pertinent to prosecute economic espionage in our modern age. A large reason as to why it is no longer applicable to modern day economic espionage is that it does not pertain to the methods "spies" use to perform economic espionage. The majority of economic espionage methods no longer use the U.S. Postal office, wire, radio or television. Instead, a large percentage occurs through cyber means. Therefore, to counter the issues associated with bringing charges under these various statutes, Congress passed the Economic Espionage Act of 1996.

B. Implementation of the Economic Espionage Act

The motive behind implementing the EEA was largely due to fear held by the federal government and Congress: fear that foreign governments and activity in general could irreparably damage the U.S. economy.[37] This damaging effect is largely illustrated and

---

[30] *See* 18 U.S.C. § 1030 (2012).

[31] 18 U.S.C. § 1030 (clarifying that information connected to the federal government is that which is obtained through a federal agency or department computer).

[32] 18 U.S.C. § 1030(a).

[33] The overwhelming majority of trade secret theft cases are narrowly related to the business realm. Yet, it is important to note that due to the increasing popularity of the Internet, there has been a spike in recent years connected to theft related to national defense.

[34] 18 U.S.C. § 1341 (2012).

[35] *Id.*

[36] Krotoski, *supra* note 23, at 4.

[37] Robin J. Effron, Note, *Secrets and Spies: Extraterritorial Application of the Economic Espionage Act and the TRIPS agreement,* 78 N.Y.U. L. REV. 1475, 1485 (2003) ("The drafters worried not only about foreign

supported by the Office of National Counterintelligence Executive who estimates the U.S. economy has lost tens or even hundreds of thousands of dollars due to economic espionage.[38] Despite this fear, there were other issues that lead to the implementation of this act; the predominant issue being the difficulty the U.S. government had prosecuting an economic espionage case. This difficulty was largely due to the lack of a specific statute to bring charges under. Instead, prosecutors brought such a case under multiple statutes.

C. Economic Espionage Act of 1996

In order for a party to be prosecuted domestically and also internationally, one must look to the Economic Espionage Act of 1996. In order to have committed a trade secret theft, one must intend or knowingly commit the act of economic espionage, while benefitting a foreign government, agent or instrumentality during the process.[39] [40] Yet, one must fall within one of the broad categories under the EEA in order to actually be prosecuted. More specifically, one must steal, duplicate, receive, or attempt to commit a crime or conspire to commit a trade secret theft to be liable for violating this act.[41] On the other hand, for one to be prosecuted internationally, one must intend to "convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce". [42] Similarly, there must be intent to benefit someone other than the owner of the trade secret, along with an intent to knowingly injure the owner of that said trade secret.[43] This can be accomplished in any of the same formats as those who are being prosecuted domestically.[44]

If one does commit trade secret theft the potential penalty they face if convicted is not enough to deter a party from committing the act.[45] The benefit of obtaining a trade secret and using it to obtain a significant financial gain is what drives most of these individuals to commit these crimes. Therefore, a fine or some jail time is not enough to stop their actions. Moreover, most of the individuals that partake in these actions are either wealthy or are backed by wealthy individuals who are capable of easily paying the fines.

Under the EEA, the President has a great deal of power. The president has the ability to submit a list of individuals believed to be responsible for economic espionage to a

---

entrepreneurs and organizations, but about foreign governments "trying to get advanced technologies from American Companies.").

[38] *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Comm. On the Judiciary Subcomm. On Crime and Terrorism*, 113th Cong. 1 (2014) [hereinafter *Hearing*] (statement of Randall C. Coleman, Assistant Dir., Counterintelligence Div. of Fed. Bureau of Investigation).

[39] 18 U.S.C. § 1831(a) (2012) (this portion of the Economic Espionage Act of 1996 does not apply only to individuals, but also to organizations who commit the act, and fulfill the elements of the crime); *See also* 18 U.S.C. § 1831(b).

[40] *See generally* 18 U.S.C. § 1839 (defining terms such as foreign agent and foreign instrumentality).

[41] 18 U.S.C. § 1831(a).

[42] 18 U.S.C. § 1832(a) (2012).

[43] *Id.*

[44] *See id.* at § 1832 (a)(1-4) (stating that one must steal, take or duplicate without authorization, receive stolen information or attempt to commit the act or conspire to commit the act of trade secret theft in order to be prosecuted under this portion of the EEA).

[45] *See generally id.* 18 U.S.C. § 1831 (stating the various portions of jail time and fines that could be incurred by one who commits trade secret theft either domestically or internationally).

congressional committee for investigation. [46] Usually, those individuals are not only determined by presidential discretion, but are often officials of a foreign government or persons acting on behalf of a foreign government.[47] Under the authority of the President and with notification of Congress, a list can be made confidential or an individual can be removed from a list.[48] The President also has the ability to freeze all assets of those who are accused of cyber espionage.[49]

D. Applicability of EEA Internationally

In modern times, the most important and relevant aspect of the EEA is that it is applicable to conduct which occurs outside of the United States. Yet, in order for this to occur one of two elements must be met. Either the one who committed the crime must be a citizen or permanent resident of the U.S., or the act must be committed in the U.S.[50] This portion of the EEA is most commonly used in recent times, due to the influx of economic espionage that is happening by foreign individuals in the United States or by citizens of the United States who are conducting these acts elsewhere.

E. Problems Associated With Economic Espionage Act

Since its adoption in 1996, there has been notable problems with the current version of the Economic Espionage Act of 1996, the most prevalent being the Internet[51]. When the EEA was implemented in 1996, the Internet was not as dominant as it is in our modern day culture. Since the Internet was not written into the statue, the Act is not designed to handle the issues currently occurring in this area of the law. Yet, this is predominantly how the trade secret thefts occur today. A simple solution that could fix this issue is to enact an amendment to this legislation that would include the Internet. Specifically, this amendment should refer to trade secret theft through digital means and associated issues.

Another issue is the lack of cases that have been brought under this statute. To be exact, only eight cases have been brought before the court under this statute since its

---

[46] H.R. REP. NO. 113-2281 (discussing the need for credible and reliable information for an individual to be placed on a congressional list).

[47] *Id.* Those individuals who are agents acting on behalf of a person in the manner of cyber espionage, which is what most often occurs in foreign economic espionage.

[48] *Id.* (In order for a list to become classified it must be a matter of national security, must be consistent with the act, and Congress must be given 15 days' notice of such a course of action. Yet, in order to be removed the president must determine such a action is appropriate. Once that is determined and credible information supports that conclusion, Congress must be notified within 15 days.).

[49] 50 U.S.C. §1701 (2014). (The president by freezing the assets of the accused will prohibit any transaction or interest of property).

[50] *See* 18 U.S.C. § 1837 (2014).

[51] *See generally* Dave Drab, *Economic Espionage and Trade Secret Theft: Defending Against the Pickpockets of the New Millennium*, XEROX.COM (2003), http://www.xerox.com/downloads/wpaper/x/xgs_business_insight_economic_espionage.pdf (discussing the various methods companies use to possess and store trade secrets) ("Between 1990 and 1995 alone, acts of economic espionage increased 300% as the result of the ease with which trade secret information can be misappropriated and disseminated over the Internet.").

creation.[52] Furthermore, only six cases have been brought under the portion of the statute that applies to international conduct.[53] Therefore, even if a foreign corporation, agent or instrumentality is brought up on charges under this act, it is very difficult for a case succeed.

On the other hand, even if a case is brought under this act, the charges are not enough to deter a party from committing the crime. If a party was found guilty of economic espionage a large fine is one of the possible results. Yet, this is not likely to deter the large majority of foreign governments/sponsors from committing economic espionage, as these governments/sponsors are able to pay fines without any issue. Even if prison was the result of a conviction, it is likely that a lesser sentence would be given, as seen in those cases where convictions have resulted. Hence, if a twenty-four month sentence is given to a defendant, it is likely when they get out of prison they would commit economic espionage again. Therefore, the benefits of committing economic espionage punishable under this act significantly outweigh the consequences.

F. Lack of International Cooperation and Law

Cooperation is an essential element in order for an international investigation and even prosecution to succeed.[54] When a foreign government either participates in the espionage or is asked to participate in an investigation, often cooperation does not result. This is largely due to the participating country's unwillingness to publically admit that they sponsored or partook in this activity. Additionally, a country is unlikely to give up their own citizens that allegedly committed economic espionage. Thus, it is often impossible to compel a foreign government to participate in an investigation, let alone a prosecution.[55]

Unlike the protections the United States has implemented, there is no international law specifically addressing the issue of economic espionage.[56] Furthermore, no foreign government considers cyber espionage to be a prohibited act.[57] It has been argued by many that the United States should attempt to use International Trade Law to fight foreign economic espionage.[58] The Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS") of the WTO is one of those laws. However this argument does not hold weight, specifically due to the fact that the agreement emphasizes and focuses more on trade

---

[52] *Chinese National, supra* note 25; *See also* Krotoski, *supra* note 23, at 7 (discussing the issues that are present with the lack of cases being brought under this statute).

[53] Krotoski, *supra* note 23, at 7.

[54] *See generally* Mark L. Krotoski, *Identifying and Using Electronic Evidence Early to Investigate and Prosecute Trade Secret and Economic Espionage Cases*, 57 ECON ESPIONAGE AND TRADE SECRETS, No. 5, 2009, at 43.

[55] The same concept can be extended to the concept of extradition or mutual legal assistance treaties. *See* David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies*, 17 AM. SOC'Y INT'L L. 1, 1 (2013) (discussing the ineffectiveness of international law in compelling foreign government participation).

[56] Katelynn Merkin, *Critical Analysis: Economic Espionage and International Law*, Denv. J. Int'l L. & Pol'y, (Dec. 26, 2013), http://djilp.org/4721/critical-analysis-economic-espionage-and-international-law/.

[57] Fidler, *supra* note 55 ("Other bodies of international law under which espionage issues arise, such as rules on armed conflict and on diplomatic relations in peacetime, do not prohibit or seriously constrain espionage or economic espionage.").

[58] *Id.*

secret theft than economic espionage.[59] This furthers the idea that TRIPS and the WTO is primarily concerned with the prevention of trade secret theft, instead of the prevention of economic espionage. Moreover, TRIPS is more concerned with the issues surrounding international trade, which rarely coincide with economic espionage.

V. PERFORMANCE OF ECONOMIC ESPIONAGE

When the EEA was adopted, the vast majority of trade secrets were stored in a paper format.[60] Today this is not the case, as almost all trade secrets are stored digitally.[61] Moreover, in recent decades, intangible assets have become increasingly more prosperous to companies and countries.[62] "This material is a prime target for theft precisely because it costs these countries so much to develop independently, is so valuable, and there are virtually no penalties for its theft."[63] In order to gain valuable information, foreign governments use a variety of methods to obtain trade secrets.

The more popular method used by foreign competitors is the targeting of employees.[64] Foreign competitors are known to have targeted and recruited insiders to assist them in trade secret theft, along with gathering intelligence through bribery of current employees.[65] These foreign corporations seek out employees who are fed up with a current employer and use this anger/frustration to their advantage.[66] There are even some competitors that have gone as far as establishing joint ventures with U.S. companies to purposely infiltrate them in order to obtain a desired trade secret.[67] Yet, this is not the only method used to obtain trade secrets.

In recent years the use of cyber espionage has been on the rise. This is usually completed through the use of hackers, malicious software or even proxies, all of which are backed by foreign entities.[68] One illustrative example that occurred this year involved cyber espionage conducted by North Korea upon the United States. Behind the cloak of secrecy that covers North Korea is an army of "Cyberwarriors".[69] It is these "Cyberwarriors" who are

---

[59] *See id.*

[60] *See generally* Drab, *supra* note 51 (discussing the various methods companies use to possess and store trade secrets).

[61] *Id.*

[62] H.R. REP. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023.

[63] *Id.*

[64] *Hearing, supra* note 38, at 2 (statement of Assistant Dir. Randall C. Coleman).

[65] *Id.*

[66] It is this frustration that makes these employees targets, as they are more likely to be less loyal to their employer. Therefore they would be more likely to betray their employer and assist in trade secret theft.

[67] *Hearing, supra* note 38, at 2 (statement of Assistant Dir. Randall C. Coleman).

[68] OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE (2011).

[69] Russell Brandom, *FBI Director Comey Reveals New Details on the Sony Hack*, VERGE (Jan. 7, 2015, 12:40 PM) http://www.theverge.com/2015/1/7/7507981/fbi-director-comey-reveals-new-details-on-the-sony-hack. (Indicating that a position for cyber espionage or even cyber warfare is a highly coveted position for the North Korean elite youth. The small portion of the youth which are selected to partake in this activity are thoroughly trained in other countries, such as Russia or China, and return once they have fully developed their craft. This position is highly sought after due to its ability to provide for a good quality of life for the hacker as well as allowing the individual to travel around the world.).

trained to commit economic espionage benefiting North Korea.[70] In December 2014, the United States concluded North Korea was responsible for a cyber-attack on Sony Pictures Entertainment.[71] The hacker here gained access to confidential Sony Pictures Entertainment information through the use of emails with Sony employees along with a malicious code, similar to a virus.[72] This attack cost the company millions of dollars and even prevented a film from going to theaters.[73] This is primarily how modern day cyber espionage occurs.

VI. PROTECTION AGAINST ECONOMIC ESPIONAGE

A. U.S. Protection Against Economic Espionage in General

The threat of economic espionage has been an issue for the government as early as 1992.[74] Even prior to the implementation of the Economic Espionage Act of 1996, the president was required to annually submit information to Congress pertaining to the threat of foreign economic espionage.[75] Yet, it was only after the implementation of the Economic Espionage Act that the United States government formed multiple taskforces to investigate, prosecute, and prevent economic espionage from occurring.

B. Federal Bureau of Investigation Protections

As many know, the FBI is the main investigative wing of the executive branch.[76] The FBI is the "Public voice for espionage, counterintelligence, counterterrorism, as well as for economic espionage and cyber and physical infrastructure protection..."[77] While all

---

[70] *Id.*

[71] *Id.*

[72] Jeyup S. Kwaak, *Sony Hack Shines Light on North Korea's Cyber Attackers,* WALL ST. J (Dec. 18, 2014), http://www.wsj.com/articles/sony-hack-shines-light-on-north-koreas-cyber-attackers-1418877740; *See also* Brandom, *supra* note 69 (North Korea is alleged to be the culprit behind this attack, due to the IP address used in the cyber-attack. The IP address is one that is exclusively used by North Koreans, for the minority that do have access to the Internet. Furthermore, the server was occasionally not masked during this attack, which also lead authorities to North Korea. Plus, the code that was used in this attack was a newer version of a previous attack by North Korea on another nation.); *See generally* Jon Fingas, *FBI Explains How It Linked North Korea To The Sony Pictures Hack,* ENGADGET (Jan. 7, 2015), http://www.engadget.com/2015/01/07/fbi-explains-north-korea-link-to-sony-hack/.

[73] Brandom, *supra* note 69.

[74] William T. Warner, *Economic Espionage: A Bad Idea*, NAT'L L. J., Apr. 12, 1993, at 13, 14.

[75] Nat'l Counterintelligence Ctr., *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage,* FED'N OF AM. SCIENTISTS, at 1 (last visited Feb. 13, 2015), http://www.fas.org/irp/ops/ci/docs/fecie_fy00.pdf; *See also* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359 § 809(b), 47 Stat. 1516 (1994).

[76] *Awareness of National Security Issues and Response [ANSIR]*, FED'N OF AM. SCIENTISTS, http://fas.org/irp/ops/ci/ansir.htm (last visited Feb. 13, 2015) ("The FBI is the lead counterintelligence agency in the United States. It has the principle authority to conduct and coordinate counterintelligence and counterterrorism investigations and operations within the United States."); *see also* Michael J. Waguespack, Deputy Assistant Dir., Nat's Sec. Div., FBI, Testimony Before the House Comm. on Gov't Reform, Subcomm. on Nat't Sec., Veterans Affairs, and Int'l Relations (Apr. 03, 2011) (stating the Economic Espionage Act of 1996, has given the FBI primary jurisdiction in matters in connection with the act).

[77] *Awareness of National Security Issues and Response [ANSIR], supra* note 76.

national security issues are the primary concern of the Awareness of National Security Issues and Response Program ("ANSIR"). [78] Together this is the FBI's national security awareness program.[79] This program primarily focuses its attention on spreading awareness of potential espionage and counterintelligence issues for U.S. corporations, government agencies, and law enforcement agencies. [80] Today, ANSIR distributes unclassified awareness information through email to those who have signed up for their services. [81] Therefore, both U.S. corporations with their principal place of business in the United States or abroad are able to reap the benefits of the ANSIR services.

It is also important to note that the ANSIR program assists in protecting American interests from economic espionage. More specifically, this program attempts to reduce vulnerability of American interests by providing awareness and information on the techniques foreign intelligence services use to collect proprietary economic information.[82] ANSIR works closely with other government agencies on cyber threats and espionage.[83] Together these agencies provide alerts to subscribers on the latest cyber threats and virus's that could dramatically harm their business interests.[84] Thus, ANSIR is more of a preventive measure for subscribers to use. The information is given to all parties as a warning of threats capable of a happening within their infrastructure. Yet, it is important to note that the FBI does not conduct physical evaluations for the private sector.[85] It is only when the FBI has received a notification that a business may have been a target of foreign economic espionage that the FBI responds with the appropriate investigative activities to resolve the matter.[86]

Another agency assisting in the prevention of foreign economic espionage is the National Counterintelligence Center ("NACIC").[87] Similar to ANSIR, NACIC works with the U.S. Government to identify and counter foreign intelligence threats to both national and economic security interests.[88] This agency is solely responsible for producing the Annual Report to Congress on Foreign Economic and Industrial Espionage.[89] Furthermore, NACIC provides educational resources to American businesses to provide knowledge of how to spot

---

[78] *Id.*

[79] *Id.*

[80] Waguespack, *supra* note 76.

[81] *Id.* ("The number of ANSIR e-mails disseminated annually vary depending upon the threat environment. In calendar year 2000, a total of 63 advisories were disseminated. Because ANSIR Email has asked its subscribers what advisories within 17 infrastructures they desire to receive, not all advisories are received by every subscriber; however, the majority of subscribers ask to receive advisories from all 17 infrastructure categories.").

[82] *Id.*

[83] *Id.* (discussing how ANSIR works closely with the Department of Justice and FBI'S National Infrastructure Protection Center (NIPC)).

[84] *Id.* ("For private and public sector organizations which desire to share information about cyber intrusion incidents, computer system vulnerabilities and physical infrastructure threats, the NIPC's InfraGard initiative provides such a mechanism. There are currently 518 members in the 56 InfraGard Chapters nationwide.").

[85] *Id.*

[86] Waguespack, *supra* note 76. ("The procedure is simply to notify any FBI office in the United States or the FBI Legal Attache or U.S. State Department Regional Security Officer in American Embassies overseas.").

[87] NAT'L COUNTERINTELLIGENCE CTR., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE, *supra* note 68.

[88] *Id.*

[89] *Id.*

and prevent economic espionage. This is primarily accomplished through an industry outreach program.[90]

The FBI Counterintelligence Division is also a major player in the prevention of foreign economic and cyber espionage. This agency is charged with exposing, preventing, and investigating these activities, along with protecting critical national secrets and assets.[91] Yet, to handle the influx of trade secret thefts that occurred and were anticipated, the Counterintelligence Division created the Economic Espionage Unit in 2010.[92] This unit is solely responsible for countering threats of economic espionage. This is done in a variety of ways: "developing training and outreach materials; participating in conferences; visiting private industry; working with the law enforcement and intelligence community on requirement issues; and providing classified and unclassified presentations."[93] This unit is charged with prosecuting cases that arise under the EEA, along with working with private sector employees/firms to investigate and prosecute trade secret theft.[94]

However, these are not the only FBI programs that assist in combatting foreign espionage. The Counterintelligence Strategic Partnership Program is also a part of the FBI that participates in this area. This program is charged with not only determining, but also safeguarding technology, which if compromised, would result in a drastic loss to national security.[95] This program is often "the first line of defense inside facilities where research and development occurs and where intelligence services are focused."[96] This is accomplished by mitigating risks posed by foreign actors obtaining sensitive or classified information.[97]

C. Department of Justice Protections of American Interests

The FBI is not the only segment of the federal government to assist in the prevention of economic espionage. The DOJ also formed a taskforce to assist with trade secret theft: The Intellectual Property Task Force. This Task Force is chaired by the Deputy Attorney General, and is part of a department-wide initiative to confront the growing number of both domestic and international IP crimes, including trade secret theft.[98] This Task Force works to identify and implement various strategies with both federal and international

---

[90] *Id.* ("The NACIC outreach mission provides industry with threat awareness materials (literature, posters, videotapes, and briefings), and it sponsors regional awareness seminars and security fairs.")

[91] *FBI-Counterintelligence*, FBI.COM, http://www.fbi.gov/about-us/investigate/counterintelligence (last visited Feb. 13, 2015).

[92] *Hearing, supra* note 38, at 1 (statement of Assistant Dir. Randall C. Coleman).

[93] *Economic Espionage: Protecting America's Trade Secrets*, DEP'T OF JUSTICE, http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage-1 (last visited Feb. 13, 2015).

[94] *Id.* The workload of this unit has steadily been increasing through the years.

[95] *FBI-Strategic Partnerships*, FBI.COM, http://www.fbi.gov/about-us/investigate/counterintelligence/strategic-partnerships (last visited Feb. 13, 2015).

[96] *Id.*

[97] *Id.*

[98] Office of the Deputy Att'y Gen., *Intellectual Property Task Force*, Dep't of Justice, DEP'T OF JUSTICE, http://www.justice.gov/dag/intellectual-property-task-force (last visited Feb. 13, 2015); *See also Hearing, supra* note 38, at 2 (statement of Assistant Dir. Randall C. Coleman) (the Intellectual Property Task Force works in conjunction with the U.S. Intellectual Property Enforcement Coordinator, and the National Intellectual Property Rights Coordination Center).

partners to combat these crimes.[99] This Task Force has an increased focus on international aspects of IP enforcement, specifically seeking to reinforce relationships with key foreign partners and industry leaders to combat this threat.[100] Since the creation of this task force, it has successfully investigated various cases, which has even lead to convictions under the EEA.[101] Yet more importantly, this Task Force is also known for assisting the Office of the Intellectual Property Enforcement Coordinator ("IPEC") in recommending intellectual property enforcement measures.[102]

D. International Protection Against Economic Espionage

It is well known that there is no law on point in the international realm that directly deals with economic espionage. Yet, there are laws and agreements that focus on trade, which are known to be used in an attempt to combat the theft of trade secrets. The predominant agreement used in this context is Article 39 of the TRIPS Agreement of the WTO. This Article requires that members of the agreement protect undisclosed information, which constitutes a trade secret.[103] The member should prevent the information from being disclosed, acquired by or even used by another without their consent in any manner that is not honest commercial practice.[104] Under this agreement it is important to understand that the obligation to protect trade secrets is only imposed on the member nations' territory and does not impose duties on those nations outside of the agreement.[105]

---

[99] Office of the Deputy Att'y Gen., *supra* note 98; *See also Hearing, supra* note 38, at 2 (statement of Assistant Dir. Randall C. Coleman) (more importantly, they exchange pertinent information with various parties in the federal government to ensure they can assist with their investigation. This taskforce also provides law enforcement officials with training of how to deal with intellectual property theft).

[100] Office of the Deputy Att'y Gen., *supra* note 98; *See also Hearing, supra* note 38, at 3 (statement of Assistant Dir. Randall C. Coleman) (discussing the international policing efforts this task force performs to assist in international economic espionage); *Chinese National, supra* note 25.

[101] Z Scott & Elizabeth Pozolo, *The Common Denominators of Trade Secret Theft and Corporate Espionage*, INSIDE COUNSEL (Apr. 22, 2014), http://www.insidecounsel.com/2014/04/22/the-common-denominators-of-trade-secret-theft-and.

[102] *Intellectual Property Task Force*, *supra* note 98.

[103] Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 39, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS AGREEMENT].

[104] *Id.* ("The information which should be protected must be: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.").

[105] Fidler, *supra* note 55.

VII. ILLUSTRATIVE CASES

A. U.S. v. Okamoto & Serizawa

i. Background

Takashi Okamoto was employed at the Lerner Research Institute ("LRI") of the Cleveland Clinic Foundation ("CCF") between the January 1997 and July 26, 1999.[106] Okamoto was employed as a research scientist conducting research on Alzheimer's.[107] His main task was to study the causes of early on-set Alzheimer's, which led to the development of the "reagents".[108] However, during the course of his employment with CCF, Okamoto had met with a representative of the Institute of Physical and Chemical Research ("Riken"), a corporation located in Saitama-ken, Japan.[109] Riken, like CCF, conducts research surrounding the causes and treatment of Alzheimer's.[110] Ultimately, while still employed at CCF, Okamoto accepted a position with Riken, which would begin in the fall of 1999.[111]

In July 1999, Okamoto and Dr. A misappropriated DNA in reagents and sabotaged the remaining reagents.[112] Following this incident, Okamoto transferred the stolen DNA from the home of another co-conspirator, Dr. B, and then to Serizawa in Kansas City.[113] On July 26, 1999, Okamoto ceased employment with CCF.[114] In August 1999, he began his employment with the Japanese corporation Riken.[115] Shortly after beginning employment with Riken, Okamoto visited Serizawa to obtain the misappropriated DNA, and returned to Japan with it.[116]

Soon after Okamoto received the boxes from Serizawa, the FBI arrested Serizawa.[117] Both Okamoto and Serizawa were charged with violating 18 U.S.C. § 1831.[118] It

---

[106] *Reported Criminal Arrests and Convictions Under the Economic Espionage Act of 1996*, BEOWULF, 29, http://b-e-o-w-u-l-f.com/texts/Reported_Criminal_Arrests.pdf (last visited Feb. 13, 2015) [hereinafter *Reported Criminal Arrests*] (It should also be noted that Hiroaki Serizwa had befriended Okamoto during this time period. Yet, Serizawa did not work with Okamoto, as he was employed by the Kansas University Medical Center in Kansas City, Kansas).

[107] *Id.*

[108] *Id.*

[109] *See id.* (stating Riken receives 94% of its funding from the Japanese Ministry of Science and Technology, which is part of the government of Japan.)

[110] *Id.* (noting Riken had formed the Brain Sciences Institute (BSI) to research this important area).

[111] *Id.*

[112] *Reported Criminal Arrests*, *supra* note 106.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.* (In order to prevent CCF from realizing what Okamoto had done, Okamoto and Serizawa devised a plan. "On or about August 16, 1999, defendants Okamoto and Serizawa filled small laboratory vials with tap water and made meaningless markings on the labels of the vials, and defendant Okamoto instructed defendant Serizawa to provide the worthless vials to officials of the CCF in the event that they came looking for the missing DNA and cell line reagents.").

[117] *Id.; see also* DAVE DRAB, PROTECTION UNDER LAW: UNDERSTANDING THE ECONOMIC ESPIONAGE ACT OF 1996 6-7 (2003), *available at* http://www.xerox.com/download/security/white-paper/1272102-35448-49fa772c96a40/cert_WP2_EE96_red.pdf (once the CCF had realized that the DNA was missing from the

was alleged that both parties "knowingly and with the intent to benefit RIKEN, an instrumentality of the government of Japan, without authorization, did steal, appropriate, take, carry away, conceal, and obtain by fraud, artifice and deception, certain trade secrets that were the property of CCF...."[119] Ultimately, the charges against Serizawa were dropped as the part of a plea bargain.[120] Unlike Serizawa, the charges against Okamoto remained.[121] However, federal prosecutors had to seek his extradition from Japan in order to charge him under the EEA.[122]

It has been estimated that the material stolen from the CCF cost about $2 million.[123] Furthermore, due to the acts of Okamoto and Serizawa, the loss of this trade secret completely ended Alzheimer's research at CCF.[124] Okamoto, if extradited from Japan, could have faced a maximum penalty of fifteen years in prison and a $500,000 fine.[125] Unfortunately, a conviction never resulted from this case against Okamoto.[126] After seeking extradition of the defendant for over three years, the Tokyo High Court issued a ruling in May 2004 that they would not permit the extradition of Okamoto to the United States.[127] Not only is this the first time Japan has denied the U.S. an extradition request, but also Okamoto is able to remain in

---

laboratory, an internal investigation was launched. Once CCF determined criminal activity was responsible for the missing DNA, the FBI was notified and ultimately resulted in Serizawa's arrest).

[118] Drab, *supra* note 117, at 7.

[119] *Reported Criminal Arrests*, *supra* note 106, at 30.

[120] *Court Rejects U.S. Request for Extradition in Industrial Spy Case*, JAPAN TIMES (Mar. 30, 2004), http://www.japantimes.co.jp/news/2004/03/30/national/court-rejects-u-s-request-for-extradition-in-industrial-spy-case/#.VNFsMlq4kfE [hereinafter *Court Rejects U.S. Request*] (The terms of the plea bargain only required that Serizawa plead guilty to perjury and all charges under the EEA would therefore be dropped. This was done to assist the FBI in a case against Okamoto.); *See also Reported Criminal Arrests, supra* note 106, at 30 ("Hiroaki Serizawa (age 40), a researcher at the University of Kansas Medical Center, plead guilty to providing false information to the FBI in September 1999 about his relationship with Takashi Okamoto. Mr Serizawa admitted that he lied when he denied knowing that Okamoto has taken a position with Riken, a Japanese government-sponsored research facility. Mr Serizawa also "underestimated the number of vials that were taken. The plea agreement eliminates the more serious charges under the Economic Espionage Act."); *See also* Lexicon Communications Corp., *Economic Espionage Updates*, Economic Espionage (last updated Mar. 2004), http://www.economicespionage.com/UpdateClevelandClinic.htm [hereinafter *Economic Espionage Updates*] (stating that Serizawa was sentenced to three years of probation, a $500 fine and a 150 hours of community service, as opposed to the maximum penalty that he could have faced of five years in prison and a $250,000 fine.).

[121] Liz Howard, *Criminal Penalties for Theft of Biological Materials*, BIOPHARM (June 2002), http://images.alfresco.advanstar.com/alfresco_images/pharma/2014/08/22/0937424b-b819-4034-9dce-b12586e55447/article-22987.pdf.

[122] *Reported Criminal Arrests, supra* note 106, at 30; Drab, *supra* note 117, at 7; John Mangels, *Scientist Gets Probation in Clinic Espionage Case*, ECONOMICESPIONAGE.COM (May 29, 2003), http://www.economicespionage.com/Cleveland%20Plain%20Dealer%20Clinic%20Story.htm.

[123] *Reported Criminal Arrests*, *supra* note 106, at 29.

[124] Drab, *supra* note 117, at 7.

[125] *Lawyer Says Alleged Stolen DNA from Industrial Espionage Case Not in Japan*, EUBIOS (Feb. 6, 2001), http://www.eubios.info/DAILY/EEID27.HTM [hereinafter *Lawyer Says*].

[126] *Economic Espionage Updates, supra* note 120; Natalie Obiko Pearson, *Tokyo Rejects Extradition of Alleged Spy,* ECONOMIC ESPIONAGE (Mar. 29, 2004, 12:38 AM), http://www.economicespionage.com/tokyo_rejects_extradition_of_all.htm.

[127] Pearson, *supra* note 126 ("Judge Masaru Suda, however, ruled that Okamoto had not violated U.S. economic espionage laws because he had not acted with the intention of profiting from the research materials, reported the Yomiuri Shimbun, a major daily newspaper, on its Web site after Monday's verdict.").

Japan without any punishment for his crimes in the U.S.[128] Ultimately, a conviction is highly unlike to ever result from this case, unless Okamoto voluntarily returns to the United States in the future.[129]

ii. Conclusions

U.S. v. Okamoto & Serizawa, at its formative stages, was considered a vital case in proving the benefits of the Economic Espionage Act. Unfortunately, this case did not result as intended. Despite being the first case to bring charges under 18 U.S.C. § 1831, this case ultimately fell short of its intended purpose. Today this case is one of the many that demonstrate the lack of protection the Economic Espionage Act of 1996 provides to domestic corporations and businesses. Instead, this case illustrates the lack of training for prosecutors, the lack of international cooperation in this area and the need for stricter punishment.

iii. Lack of Training for Prosecutors

As mentioned above, very early on in *U.S. v. Okamoto & Serizawa* federal prosecutors provided Serizawa with a plea deal[130]. The government's intent with this plea deal was to ensure Serizawa's compliance with the investigation and a future trial.[131] However, in this process the United States ensured that the only individual who was capable of being convicted in connection with this economic espionage would not be punished accordingly. This plea deal not only removed any economic espionage charge against Serizawa, but also reduced the charges against him to perjury.[132] Accordingly, the possible sentences he could have faced also dramatically decreased.[133]

Upon review of this case, it seems that federal prosecutors were more concerned with the compliance of Serizawa than with obtaining the necessary convictions under this act. This is demonstrated with the completion of this plea deal prior to the United States even beginning the extradition process for Okamoto. If federal prosecutors had more guidance and training under this relatively new act they could have sought the extradition of Okamoto prior to obtaining a plea deal. Then, if Japan denied their request, the United States would still be able to accurately punish Serizawa, providing a conviction under the EEA.[134]

---

[128] *Id.* (Japan will only extradite those individuals who are accused of acts which are also illegal in Japan. Here this is not the case, as Japan does not have any economic espionage laws. The closest act that it could be compared to in Japan is theft and destruction of property).

[129] Mangels, *supra* note 122.

[130] *Court Rejects U.S. Request*, *supra* note 120; *Reported Criminal Arrests, supra* note 120, at 30; *Economic Espionage Updates, supra* note 120.

[131] *See Researcher Gets Probation, Fine Economic Espionage Charges Dismissed in Plea Deal*, RECORD-COURIER (May 29, 2003, 12:00 AM), http://www.recordpub.com/local%20news/2003/05/29/researcher-gets-probation-fine-economic-espionage-charges-dismissed-in-plea-deal [hereinafter *Researcher Gets Probation*] (stating the compliance they sought included supervised phone calls with Okamoto).

[132] *Id.*

[133] *Id.*

[134] It would have been far easier for the United States to score a conviction related to Serizawa. Not only was he present in the United States, but also it would have been easier for prosecutors to prove his connection to economic espionage.

iv. Lack of International Cooperation

Due to the lack of a uniform international law or treaty in place to directly address economic espionage, the U.S. was forced in this case to rely on the cooperation with Japan. Thus, once Okamoto left the United States to take up his new employment in Japan, the U.S. was forced to rely on Japan to ensure the success of this prosecution. This entailed filing countless extradition requests with the Japanese government to see if they would comply with releasing Okamoto to the U.S. Unfortunately for the U.S., after years of seeking extradition of Okamoto, Japan refused to extradite him.[135]

From the start of the extradition process, it should have been clear to federal prosecutors that Japan would not cooperate with their requests. According to Japan's extradition treaty with the United States, they will only agree to extradite an individual for prosecution in another country if that crime is also acknowledged in Japan.[136] Mutual recognition of a crime is not present in this case, as Japan does not have any criminal law in place addressing economic espionage.[137] Therefore, Japan was not mandated to comply with the United States. Japan was free to use their discretion in deciding to comply with these requests, which were ultimately denied.

Japan stated that they would not voluntarily extradite Okamoto because they do not believe that he actually committed the crime.[138] More specifically, Japan claimed there was no evidence to support the claim that Riken would have benefited from this theft.[139] Yet, there was actual evidence that resulted from the internal investigation of CCF to show that Okamoto did in fact plan on continuing his work at Riken.[140] Hence, Riken and the Japanese government would have benefited from the work stolen from CCF. Accordingly, there was information present to provide to Japan to ensure their cooperation in this matter. Instead, Japan decided they would rather not partake in this matter. Due to the lack of cooperation between Japan and the United States, now the only viable option the United States has is the possible voluntary return of Okamoto.[141]

This case clearly sends the wrong message to criminals. It demonstrates not only that the United States is at the mercy of other countries to assist in combating international economic espionage, but also that criminals are capable of escaping prosecution for their crimes due to extradition formalities. In order to prevent this crushing blow from occurring again, the United States should seek to modify or update extradition agreements with countries that consistently partake in economic espionage. This would ensure that this dilemma would not occur again.

---

[135] Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389, 439 (2006).

[136] *Court Rejects U.S. Request*, *supra* note 120.

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] Drab, *supra* note 117, at 6.

[141] Since Japan has denied the extradition requests of the United States, the only other possibility for the U.S. to obtain Okamoto is his return to the U.S. There still remains a warrant in place for his arrest, which can only be acted upon if this were to occur. Therefore, if he ever did in fact return to the U.S. federal prosecutors would be able to then arrest him, pursuant to the existing arrest warrant.

v. The Need for Stricter Punishment

At the time the theft of the CCF regents occurred, the maximum sentence both Okamoto and Serizawa could have faced was fifteen years in prison and a fine of $500,000.[142] Yet, neither individual faced anything remotely close to this. Serizawa, as previously mentioned, accepted a plea deal, which allowed for him to escape from being charged with economic espionage. Instead, Serizawa was charged with perjury. Accordingly, Serizawa was sentenced to three years of probation, a $500 fine, and 150 hours of community service.[143]

This plea deal is a fairly light punishment as compared to the maximum that Serizawa could have otherwise faced. The primary motive for this lighter sentence was Serizawa's cooperation with the FBI's investigation. Yet, this was not the only factor in bringing about this deal. Serizawa's criminal record also played a part.[144] More specifically, since Serizawa had no existing criminal record and would allow for the FBI to monitor phone calls with Okamoto, this plea deal emerged.[145]

This plea deal serves as a clear illustration of the lack of consequences present surrounding the area of economic espionage. A criminal could clearly commit an act such as Okamoto's (obtaining a trade secret from a domestic corporation or business, and easily profit from that secret). The profit an individual stands to make from these secrets could easily be in the millions of dollars. Yet, when actually charged and convicted under the act, the punishment received is barely a consequence when compared to the potential benefit obtained. If an individual is willing to comply with a potential investigation and they're remorseful, or even a "model citizen", it is likely the government would be easier on them than a repeat offender. How could the United States government believe that anyone would actually stop committing these acts when there is no hard penalty to deter them?

A. U.S. v. Meng

i. Background

Xiadong Sheldon Meng is a former Chinese national, raised in Beijing and currently holding Canadian citizenship while living in the United States.[146] At the time the offense was committed, Meng resided in California as a software engineer for Quantum3D.[147]

---

[142] *Lawyer Says*, *supra* note 125.

[143] *Economic Espionage Updates, supra* note 120.

[144] *Researcher Gets Probation, supra* note 131.

[145] *Id.*

[146] Jordan Robertson, *Engineer is First Sentenced For Economic Espionage*, USA TODAY (Jun. 18, 2008, 6:17 PM), http://usatoday30.usatoday.com/tech/products/2008-06-18-4083753379_x.htm; Catherine Elsworth, *Chinese Spy Jailed For 24 Months,* TELEGRAPH (June 18, 2008, 7:55 PM), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/2152976/Chinese-spy-jailed-for-24-years.html.

[147] Chris Brook, *Xiaodong Sheldon Meng (Quantum3D),* Threatpost (Jan. 5, 2011, 6:05PM), http://threatpost.com/xiaodong-sheldon-meng-quantum3d/91787 ("...Quantum3D, a defense contractor that makes visual simulation software used for military training and other purposes"); *see* Janet Siegel, *Federal Court in California Imposes Maximum Sentence Under Plea Deal in First Ever Sentencing Under the Economic Espionage Act of 1996* (Jun. 10, 2008),

Quantum3D primarily designs software and various other products intended for military purpose, ranging from combat simulation to day and night infrared technology.[148] At the time Meng accepted a position with Quantum3D, the company required him to sign an "Employee Proprietary Information Agreement".[149] This agreement stated his obligation to return any and all Quantum3D information, documents, or property at the end of his employment with the company.[150]

During his time with Quantum3D, Meng came to acquire company trade secrets "Mantis" and "viXsen"; both products were software connected to military training.[151] Soon after obtaining these trade secrets, Meng terminated his relationship with Quantum3D and began working with Orad, a direct competitor in China.[152] It is alleged that Meng took these trade secrets from Quantum3D and pitched them to Asian military officials upon ending his relationship with Quantum3D.[153] More specifically, it was alleged that Meng had pitched these technologies in various meetings with the People's Republic of China, Malaysian Air Force, and the Thailand Air Force.[154]

It is further alleged that Meng illegally installed a copy of the Quantum3D software "Mantis" at a Chinese Naval site following these sales pitches.[155] When this software was installed at the Chinese naval site, Meng changed the source code for the software to make it appear to a potential buyer that the software was from his new employer Orad.[156] However, these actions were not fruitful. Consequently, the U.S. Government charged Meng with misappropriating Quantum3D's trade secrets and attempting to export them to a foreign nation, China, in violation of EEA.[157]

---

http://www.tradesecretslaw.com/2008/06/articles/trade-secrets/federal-court-in-california-imposes-maximum-sentence-under-plea-deal-in-first-ever-sentencing-under-the-economic-espionage-act-of-1996/ (stating the various positions Meng has been employed in within Quantum3D ranging from systems engineer to analysis to consultant for the company.); *see also* Elsworth, *Chinese Spy Jailed For 24 Months, supra* note 142 (stating Meng had been employed by Quantum3D from 2000-2003).

[148] *Former Quantum3D Employee Charged With Espionage*, SILICON VALLEY BUS. J. (Dec. 14, 2006, 2:23PM), http://www.bizjournals.com/sanjose/stories/2006/12/11/daily49.html.

[149] Siegel, *supra* note 147.

[150] *Id.*

[151] *Id.* ("Among the products to which Meng had access were "Mantis," a product used to visually simulate motions and three-dimensional scenes for training and other purposes, and "viXsen," a visual simulation software program using for training military fighter pilots using thermal imaging (night vision) equipment."); *see also* Brook, *Xiaodong Sheldon Meng (Quantum3D), supra* note 143 (stating Meng the massive amount of military training software that was stolen from Quantum3D).

[152] Siegel, *supra* note 147.

[153] Elsworth, *supra* note 146.

[154] *Former Quantum3D Employee Charged with Espionage, supra* note 148.

[155] *Inside the Ring*, WASH. TIMES (Aug. 10, 2007), http://www.washingtontimes.com/news/2007/aug/10/inside-the-ring-97219344/.

[156] *Id.*

[157] Siegal, *supra* note 147 ("The United States government charged Meng with misappropriating Quantum3D's trade secrets without authorization and attempting to export them from the United States to China in violation of various federal laws including, among others, the Economic Espionage Act (18 U.S.C. § 1831), the Trade Secrets Act (18 U.S.C. § 1832), and the Arms Export Control Act (22 U.S.C. § 2778)."). *See also Inside the Ring, supra* note 155 (stating Meng had violated the Arms Export Control Law by selling "viXsen" to China).

ii. Conclusions

Following this federal indictment, Meng accepted a plea deal in this case. [158] As a result, his punishment was significantly reduced from a maximum of twenty-five years in prison to twenty-four months in prison. [159] Moreover, in order to accept this plea deal, Meng was required to plead guilty to only two of the thirty-six offenses cited in the indictment against him. [160] This significant reduction in sentencing was largely due to Meng's lack of a criminal record. [161] Just as in *U.S. v. Okamoto & Serizawa,* federal prosecutors preferred to go easy on a new criminal instead of giving out a sentence that sends a message to others who intend to misappropriate trade secrets in the future.

The punishments distributed by the federal government under this act should be equal to the damage that was done to the U.S., in this case U.S. national security. The software stolen from Quantum3D by Meng was a program of high value to the U.S. [162] It was also part of a campaign launched by the Chinese military in an effort to possess leading U.S. technology to build up their military force. [163] If the United States did not discover the sale of Quantum3D's trade secrets, who knows what the ramifications could have been in the international arena. This case "Demonstrates the importance of safeguarding sensitive U.S. military technology as well as trade secrets. It should also serve as a warning to others who would compromise our national security for profit."[164] Yet, this is not 100% a true statement. Yes, this and many other economic espionage cases demonstrate the need for protection of U.S. military technology and various other trade secrets, but they do not send a warning to those who seek to compromise our national security.

Since there is a high demand by less developed militaries for such technology, there is likely to be a large amount of money to be made off of the sale of trade secrets. Once again, the benefits of committing these acts against the U.S. far outweigh the consequences, which are barely carried out in convictions under the EEA. In order to combat this, the federal government should begin to seek the maximum sentence under the EEA. Additionally, federal prosecutors should stop offering plea deals to those individuals with a clean criminal record. It will only be possible for individuals to understand that the U.S. will no longer sit by and let the country's most precious trade secrets walk out, if these actions are taken.

---

[158] *Inside The Ring, supra* note 155 (stating Meng accepted a plea deal sentencing him to 24 months in prison, as well as serving 3 years of supervised release once he is out of prison, a $10,000 fine and forfeit all computer equipment which was seized in connection with the case).

[159] *Id.* (stating Meng accepted a plea deal sentencing him to 24 months in prison, as well as serving 3 years of supervised release once he is out of prison, a $10,000 fine and forfeit all computer equipment which was seized in connection with the case); Jonathan Pollard, *Chinese Spy Meng Sentenced to 24 Months* (June 18, 2008), http://www.jonathanpollard.org/2008/061808a.htm (This maximum sentence would have been for violating the EEA and the Arms Export Control Act. Additionally, Meng is required to pay a $10,000 fine in connection with his sentence).

[160] *Id.*

[161] Robertson, *supra* note 146.

[162] *Chinese Spy Meng Sentenced to 24 Months, supra* note 159.

[163] *Inside The Ring, supra* note 155.

[164] *Id*

C. U.S. v. Ye and Zhong

i. Background

On November 23, 2001, Fei Ye and Ming Zhong were arrested and charged with two counts of economic espionage.[165] Both individuals were arrested at San Francisco International Airport, possessing stolen trade secrets from multiple California based companies while attempting to board a flight for China.[166] These trade secrets were primarily obtained from Sun Microsystems, INC., where Ye had worked, and Transmeta Corporation, where both parties had previously been employed.[167] Ye and Zhong, both originally from China, planned to use these misappropriated trade secrets to benefit China. This would be accomplished by using the stolen technology to start a microprocessor company, Supervision INC.[168]

After establishing Supervision INC, the parties obtained direct assistance and funding from the Chinese government.[169] These individuals also promised China they would assist in the development of a "super-integrated circuit design, and form a powerful capability to compete with worldwide leaders in the field of integrated circuit design."[170] However, this is not the only benefit that Ye and Zhong provided to China. The City of Hangzhou and the Province of Zhejiang in China, which was also funding Supervision, INC., would have benefitted by receiving a portion of the profits from the creation and manufacturing of this microprocessor.[171]

ii. Conclusions

Following a federal indictment, Ye and Zhong were sentenced to only a year in jail, compared to the maximum sentence of thirty years in prison that they could have received.[172] Just as in the preceding two cases, there was a significant difference between the maximum sentence that could have been obtained, and the sentence received. A plea deal was to blame

---

[165] U.S. DEP'T OF JUSTICE, PRESS RELEASE: TWO MEN PLEAD GUILTY TO STEALING TRADE SECRETS FROM SILICON VALLEY COMPANIES TO BENEFIT CHINA (Dec. 14, 2006) *available at* http://www.justice.gov/criminal/cybercrime/press-releases/2006/yePlea.htm.

[166] *Id.*; *See also* Jordan Robertson, *Engineers Sentenced to 1 Year for Espionage Case*, FOX NEWS (Nov. 21, 2008), http://www.foxnews.com/printer_friendly_wires/2008Nov21/0,4675,TECEconomicEspionage,00.html (stating inside the luggage was sensitive documents all pertaining to chip designs from four different technology companies both Ye and Zhang had worked for.); Dan Verton, *Beijing's Red Spider's Web,* ASIA TIMES (Jul. 22, 2008), http://www.atimes.com/atimes/China/JG22Ad01.html (stating the trade secrets possessed by Ye and Zhong included microchip blueprints and computer-aided design scripts from Sun Microsystems Inc, NEC Electronics Corp, Transmeta Corp and Trident.

[167] Verton, *supra* note 166.

[168] *See id.*; Robertson, *supra* note 166

[169] Verton, *supra* note 166.

[170] *Id.*

[171] *Id.* (stating Supervision, INC also applied for funding from the National High Technology Research and Development Program of China); Robertson, *supra* note 166.

[172] Jordan Robertson, *2 Chinese Engineers Sentenced in Chip Espionage*, SF GATE (Nov. 22, 2008, 4:00 AM), http://www.sfgate.com/business/article/2-Chinese-engineers-sentenced-in-chip-espionage-3184508.php.

in all of these cases. [173] Moreover, in exchange for a reduced sentence, both defendants agreed to cooperate with a federal investigation. [174] Once again, there is no punishment resulting from this case sufficient to actually deter another employee of a U.S. corporation from committing a similar act in the future.

VIII. SOLUTIONS

A. Obama Administration New Strategy to Combat Economic Espionage

In 2013, the Obama Administration announced their new plans to combat international economic espionage and trade secret theft. [175] This new plan seeks to "improve legal frameworks, stronger enforcement of existing laws and strong and efficient remedies for trade secret owners". [176] The first prong of this new strategy consists of increasing diplomatic pressure on other countries. [177] This would consist of the U.S. government sending consistent and coordinated messages from the appropriate agencies to the foreign governments who regularly conduct economic espionage. [178] To ensure that these measures are effective, the State Department will schedule meetings between senior administration officials and members of the corresponding foreign governments where these activities continuously occur. [179]

Under this new strategy, intellectual property attachés are going to push the need to incorporate more trade secret protection into their current intellectual property agendas. [180] Furthermore, various federal agencies will begin to use existing programs to educate foreign government officials on the need to increase awareness and enforcement of trade secret theft. [181] Additionally, there would be a push for increased cross-border diplomatic cooperation with law enforcement. [182] This is one aspect of the new strategy that is greatly needed to deter economic espionage. If there was more cooperation between countries, it

---

[173] Dan Levine, *DOJ's Economic-Spy Strategy Emerges*, INVESTORVILLAGE (May 5, 2008), http://www.investorvillage.com/mbthread.asp?mb=329&tid=4703584&showall=1.

[174] Jordan Robertson, *2 Chinese Engineers Sentenced in Chip Espionage*, SF Gate (Nov. 22, 2008, 4:00AM), http://www.sfgate.com/business/article/2-Chinese-engineers-sentenced-in-chip-espionage-3184508.php.

[175] *See generally* EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS, (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter ADMINISTRATION STRATEGY ON MITIGATING THE THEFT] (discussing the five specific actions the plan attempts to use: focusing on diplomatic efforts to protect trade secrets overseas; promoting voluntary practices by private industry to protect trade secret; enhancing domestic law enforcement operation; improving domestic legislation and promoting public awareness and stakeholder outreach).

[176] Fidler, *supra* note 55 (It is important to note that this plan does in fact predominately focus on a more national and domestic level, while avoiding the international issues associated with this problem.).

[177] *See Id.*; *See generally* EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, *supra* note 175.

[178] ADMINISTRATION STRATEGY ON MITIGATING THE THEFT, *supra* note 175, at 3 (The relevant federal agencies which would send these communications to foreign governments include "the Departments of Commerce, Defense, Justice, Homeland Security, State, Treasury and the U.S. Trade Representative").

[179] *Id.*

[180] *Id.*

[181] *Id.*

[182] *Id.*

would make it more likely that foreign governments participate in an investigation and even prosecution of economic espionage.

The second prong of Obama's new strategy includes promoting voluntary practices by private industry to protect trade secrets.[183] Essentially, this strategy would consist of U.S. companies sharing practices with each other that have and can be used to mitigate the risk of trade secret theft.[184] It is important to note that these are merely suggestions for the businesses to use in an attempt to safeguard their IP. The third goal this new plan seeks to enhance is domestic law enforcement.[185] This includes the expansion of the FBI's "efforts to fight computer intrusions that involve the theft of trade secrets by individual, corporate, and nation-state cyber hackers."[186] Furthermore, The DOJ and FBI will be continuing to train both prosecutors and investigators under the Economic Espionage Act.[187]

The fourth item of Obama's strategy directly addresses domestic legislation on economic espionage. The administration has recommended that congress increase the penalty for those who are convicted of economic espionage.[188] The current form of the Economic Espionage Act calls for a maximum of fifteen years in prison if convicted.[189] The Obama Administration plans to increase that maximum to at least twenty years.[190] Once again, this shows how the current penalty for the economic espionage act is not truly a penalty. It is not enough to deter an individual from committing the crime. Thus, increasing that penalty to twenty years in prison might actually be the starting point of deterrence.

B. The Need for New International Law Addressing Economic Espionage

As it is known, there is no current law on point in the international arena that directly addresses the issue of economic espionage. Despite this, many countries prohibit the act under their own national laws.[191] Thus, even though one country's laws shun the act from occurring, the international realm does not have any protection. Therefore, there is a need for some sort of international law that will directly address this issue. More specifically, some legislation other than the TRIPS Agreement should be used.

The TRIPS Agreement should no longer be used due to the fact that it predominantly focuses on issues connected to trade. Only protected information, trade secrets, which are relevant to trade are to be protected under this law. However, in the world of trade

---

[183] ADMINISTRATION STRATEGY ON MITIGATING THE THEFT, *supra* note 175, at 6.

[184] *Id.*

[185] *Id.* at 7.

[186] *EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (Feb. 2013), http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter ADMINISTRATION STRATEGY ON MITIGATING THE THEFT].*

[187] ADMINISTRATION STRATEGY ON MITIGATING THE THEFT, *supra* note 175 ("These training events will target domestic law enforcement officers, prosecutors, and international partners. These events will include both a trade secret specific curriculum as well as broader intellectual property rights...").

[188] *Id.*

[189] *See* 18 U.S.C. § 1831 (2012).

[190] ADMINISTRATION STRATEGY ON MITIGATING THE THEFT, *supra* note 175, at 32.

[191] Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies, supra* note 55.

secret theft and economic espionage this does not cover a large portion of the crime. In actuality, a large portion of trade secret theft and economic espionage targets businesses not participating in trade. Hence, there is a need for a more universal law that is more relevant to the business realm than to the trading world.

Additionally, the TRIPS Agreement is only relevant to those countries that are participants under it.[192] If one country steals or acquires a trade secret from another country which is not a member to this agreement, there is no protection.[193] This is particularly important, as there are many countries that continually partake in economic espionage who do not recognize the TRIPS Agreement. Hence, a more universal law that would be accepted by those countries that partake in economic espionage is needed.

C. The Adoption of New Legislation

i. Deter Cyber Theft Act of 2014

The Deter Cyber Theft Act of 2014 was introduced to the United States Senate on May 22, 2014.[194] This proposed legislation would require the president to provide yearly reports to Congress, identifying foreign countries partaking in economic espionage, targeted technologies, items produced through misappropriated trade secrets and methods used to obtain such information.[195] Additionally, this act will provide the president with the power to identify specific foreign countries that engage in economic espionage of U.S. trade secrets.[196] If a country is mentioned in the reports, the President would have the ability to issue sanctions on them.[197] If adopted, the President would be given the ability to block all transactions, either interest based or property based, that occur by a foreign persons in the United States.[198]

This legislation aims to send a message to foreign companies; the United States has had enough of cyber espionage.[199] Senator Levin, who sponsored this act, has said "We need

---

[192] *See* TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), *available at* https://www.wto.org/english/docs_e/legal_e/27-trips.pdf.

[193] The relevant countries that have accepted TRIPS Agreement include: China, Japan, United States and Republic of Korea. *See generally* World Intell. Prop. Org., *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (Total Contracting Parties: 161)* (last visited October 1, 2015), http://www.wipo.int/wipolex/en/other_treaties/parties/.jsp?treaty_id=231&group_id=22.

[194] Deter Cyber Theft Act of 2014, S. 2384, 113th Cong. (2014).

[195] *See generally id.* at § 2(a)(1). This source further describes the requirements the President's report must have including: describing the espionage tactics engaged in by foreign countries, the actions the President has taken to decrease economic espionage and the progress made using those actions. *Id.*

[196] *Id.* at §2(a)(1)(A)(i) (The President must specifically cite those foreign countries which either personally engage in economic espionage, or facilitate, support, fail to prosecute or allow economic espionage to continue in their country.).

[197] *Id.* at §2(b)((1).

[198] *Id.* at §2(a)(2)(b) (Sanctioning must only be on those interests which are in the United States, are under control of a U.S. resident or come in contact with U.S. interests, but the President will not have the ability to sanction the importation of goods from a country that is placed on the watch list.).

[199] Samuel Rubenfeld, *Senator Proposes Sanctions to Fight Cybertheft,* WALL ST. J, (May 23, 2014, 5:30AM), http://blogs.wsj.com/riskandcompliance/2014/05/23/senator-proposes-sanctions-to-fight-cyber-theft/.

to call out those who are responsible for cyber theft and empower the president to hit the thieves where it hurts the most- in their wallet..."[200] If this act is adopted by Congress, it would deter the persistent use of economic espionage of U.S. trade secrets. This would be accomplished through the use of sanctions. The countries that partake in economic espionage of U.S. trade secrets most likely have a large amount of either property or interests in the United States. If one of these countries is placed on the priority watch list they could face the possibility of these sanctions.

Sanctions, in general, are implemented to force a change in behavior.[201] They can be imposed in a variety of ways, ranging from tariffs to asset freezes or seizures.[202] Sanctions placed by one country upon another can be risky, but also very effective if implemented by an economically powerful country.[203] This is directly demonstrated in the proposed act. The United States is not only an economically powerful country, but also more likely to be successful in deterring the behavior of economic espionage participants. Thus, the U.S. would have the ability not only to implement these sanctions, but also to ensure that they continue until the other country stops the use of economic espionage. Hence, the adoption of the Deter Cyber Theft Act of 2014 would deter the continuation of foreign economic espionage of U.S. trade secrets.

D. Workplace Solutions

It is no secret that the majority of economic espionage targets businesses. Today there are two specific categories that have emerged in connection with trade secret theft and businesses: those companies that have been a victim of economic espionage and those who don't know they have been invaded yet.[204] Despite all the legislation that has been implemented and proposed surrounding this area of law, additional measures are still needed. It is no secret that those within the company conduct the majority of economic espionage that targets businesses.[205] Thus, it is time to cut off trade secret theft from the source. Guidelines should be implemented by American businesses to prevent the likelihood of trade secret theft.

One guideline that could be implemented by businesses is to prevent the use of external devices by employees.[206] This would eliminate the possibility of an employee directly copying data files from the business, which contain a trade secret, and using the files for their own gain. If direct elimination is not possible, a limitation should be placed upon the employees.[207] A corporation could make it so that only one individual is capable of using

---

[200] *Senate Introduces Cyber-espionage Bill,* INFOSECURITY MAG. (May 8, 2013), http://www.infosecurity-magazine.com/news/senate-introduces-cyber-espionage-bill/ (This would be accomplished through the use of sanctions on those countries who are benefiting from economic espionage of U.S. companies.).

[201] Brent Radcliffe, *Sanctions Between Countries Pack a Bigger Punch Than You Might Think,* INVESTOPEDIA, http://www.investopedia.com/articles/economics/10/economic-sanctions.asp (last visited Feb. 13, 2015).

[202] *Id.* (listing examples of sanctions and defining them as well).

[203] *Id.*

[204] Scott & Pozolo, *supra* note 101.

[205] *Hearing, supra* note 38 (statement of Assistant Dir. Randall C. Coleman).

[206] Z Scott & Pozolo, *supra* note 101 (specifying external drives as thumb drives, USB and DVD ports).

[207] Z Scott & Pozolo, *Corporate Trade Secret Theft: How to Prevent it (and How to Respond if it Happens Anyway),* INSIDE COUNSEL (May 20, 2014), http://www.insidecounsel.com/2014/05/20/corporate-trade-secret-theft-how-to-prevent-it-and.

external drives to copy and store files. Thus, if any information is stolen from the corporation, it is easy to pinpoint who misappropriated that information. Additionally, IT could also be upgraded at businesses.[208] This could include requiring multiple passwords to access company files or the company network, or to even download files within the company.[209]

Another solution to workplace economic espionage is to educate company employees. This would range from classes dedicated to educating employees about what constitutes a trade secret, the company's policy toward theft and reporting suspicious behavior, and even educating employees on the EEA.[210] An education program will ensure that all employees understand the importance of reporting a potential theft and how they could be prosecuted under the EEA if need be. Additionally, an anonymous hotline could be set up for employees to report suspicious activities occurring within the business.[211] The implementation of a hotline would make employees more likely to comply with these new guidelines, as there would be no repercussions in the workplace.

Furthermore, employers should exercise caution when hiring new employees. Under the EEA employers are liable for prosecution for stolen trade secrets misappropriated by new employees.[212] Thus, a corporation can be held liable for the misappropriation of a trade secret that occurred at another business or by a potential new employee. Accordingly, corporations should implement guidelines/procedures to limit those new employees that come from a competing business.[213] This would limit the likelihood that a corporation would be liable under the EEA for an act that occurred outside their business. Conversely, employers should interview employees who are leaving their corporation.[214] This interview would allow for the company to determine if the individual has any information, such as a trade secret. If an employer determines the individual possesses a trade secret, measures should be taken to ensure that they do not use that information to their benefit and the company's detriment.[215]

IX. CONCLUSION

Economic espionage costs American businesses billions of dollars a year.[216] Not only has this figure dramatically increased since the creation of the EEA, but it continues to rise. Similarly, there has been an increase in foreign economic espionage in recent years. Thus, the EEA was intended to prevent this from occurring, but is not capable of doing the job. Changes must be adopted in order to prevent such a hit to the American economy.

---

[208] *Id.*

[209] *Id.*

[210] *Id.* ("In addition to taking steps to tighten IT security, companies must also prioritize compliance and training programs that educate employees' possibilities of compromise from foreign governments, the existence of the EEA, and its penalties.").

[211] *Id.*

[212] *Id.* ("The EEA allows for the prosecution of a company that "receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained or converted without authorization.").

[213] Z Scott & Pozolo, *supra* note 207.

[214] *Id.*

[215] *Id.* (citing this information in an exit interview could be used later on down the road if that employee ends up working with a competitor, and a civil or criminal trial ensues.).

[216] BOUCHOUX, *supra* note 8, at 2.

THE NEED FOR MODERNIZATION OF THE EEA OF 1996

The EEA was adopted in 1996 and is clearly not capable of handling the advanced technology that is present in this age. Not only is the act not written to cover acts performed in the cyber realm, but also it does not even cover present technology at all. This needs to be changed in order for the EEA to work as it was intended. The modernization of the EEA is not the only thing needed to cure this problem. A uniform international law should be implemented to cover international economic espionage. Additionally, stricter punishment should be implemented with the modernization of this act, to deter criminals from continuing these actions. While on a smaller scale, businesses should take steps to protect themselves from employees committing economic espionage right beneath their noses.