The *Michigan IT Lawyer* is pleased to present "*How Recent Attempts to Expand Economic Espionage Protection Will Likely Be Futile in Light of Trade Secret Protection Schemes Already Available to U.S. Companies*" by Shannon Murphy, the first-place winner of the 2013 Edward F. Langs Writing Award competition. Ms. Murphy has a B.S. in Neuroscience from the University of Michigan-Ann Arbor and graduated from the University of Detroit Mercy School of Law in December 2013. Ms. Murphy is a full-time intern with Reising Ethington, P.C., an intellectual property law firm in Troy, Michigan, and has accepted a position as an associate attorney with Reising Ethington pending the February 2014 bar examination results.

The statements made and opinions expressed in this essay are strictly those of the author, and not the State Bar of Michigan or the Information Technology Law Section. Comments regarding this article can be forwarded to the *Michigan IT Lawyer*, care of *michael@gallo.us.com*. Enjoy!

How Recent Attempts to Expand Economic Espionage Protection Will Likely Be Futile in Light of Trade Secret Protection Schemes Already Available to U.S. Companies

By Shannon Murphy

Introduction

The FBI estimates that billions of dollars are stolen from U.S. companies every year as a result of foreign and domestic organizations misappropriating trade secrets and other proprietary information.[1] For example, from the middle of February 2013 until the end of March 2013, a short six weeks, U.S. bank websites were offline for 249 hours, a much greater duration than usual.[2] National security officials suspect that the Iranian government may be promulgating these cyber attacks, which have been steadily assaulting U.S. financial institutions since the middle of 2012.[3] The threat to companies is even more pervasive given the amount of data and information that is now digitally stored and thus much more susceptible to cyber attack. In 2009, an estimated 81% of the market value of S&P 500 companies was derived from the value of their intangible assets, including trade secrets, proprietary data, marketing plans, business processes and source code.[4] Given the drastic increase in globalization that has occurred in the past few decades, it is possible for one cyber attack to impact a company's bottom line, share price, and customer confidence on an immense scale in a mere instant.[5]

The actual damage resulting from cyber attacks can be extremely challenging to evaluate, as demonstrated by the variable estimates of yearly losses resulting from such attacks, ranging anywhere between $2 billion to $400 billion or more a year.[6] This may be a result of the diverse wisdom and know-how that is represented in the stolen intellectual property. For example, it may be difficult to assess the value of the theft of business strategies that were discussed at a meeting. However, it may be easier to assess the value of certain other information, such as certain proprietary Valspar paint formulas that were valued at about $20 million, about one-eighth of Valspar's reported profits in 2009, which were misappropriated and almost divulged to a competing Chinese company.[7]

Shannon Murphy

Regardless of the various difficulties that may arise from regulating such an immense array of information, trade secret protection should be, and often is, a primary goal of U.S. and foreign companies.[8] Accordingly, on January 14, 2013, Congress enacted the Foreign and Economic Espionage Penalty Enhancement Act of 2012,[9] amending the Economic Espionage Act of 1996 to provide increased penalties for foreign and economic espionage.[10] The Executive Branch also took action on February 12, 2013 when President Obama signed an executive order titled "Improving Critical Infrastructure Cybersecurity" which seeks to establish a partnership between the government and private infrastructure operators "to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[11] This article will first provide a review of economic espionage related legislation and review recent jurisprudence under the Economic Espionage Act.[12] The article will then analyze the practical implications of the recent government action to stem the tide of economic espionage.

HOME BACK NEXT

I. Economic Espionage Legislation

Prior to the criminalization of trade secret misappropriation, the only recourse for companies was civil litigation.[13] Now, if a company's trade secrets are misappropriated the company may bring a civil cause of action under state law and/or report it to the FBI for investigation.[14] Companies should still take proper precautions to establish the proper infrastructure required to protect itself from trade secret misappropriation, such as the government purports to do under the recent directives of the executive order issued by President Obama.[15]

A. Trade Secret Misappropriation

In a purely economical sense, trade secrets can provide companies a way to protect the value of information.[16] State trade secret and unfair competition laws give companies a civil cause of action when their trade secrets are misappropriated.[17] A typical trade secret claim involves three basic elements: (1) the allegedly misappropriated information must be a trade secret, something not generally known to others in the same industry, and it must provide value to the entity that holds the secret; (2) the trade secret holder must have taken reasonable precautions to prevent disclosure; and (3) the trade secret holder must show that the defendant wrongfully acquired, or misappropriated, the trade secret.[18]

A trade secret is defined in the Uniform Trade Secrets Act, a model statutory scheme that serves as the basis of many states' trade secret legislation,[19] as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> > (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> >
> > (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[20]

Put simply, "a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business."[21] Trade secrets more at risk for economic espionage include technical information relating to military technologies, particularly marine systems and aerospace/aeronautics; information and communications technology; clean energy-generating technologies; as well as healthcare, agricultural, and advanced materials and manufacturing techniques.[22]

Besides showing the existence of a trade secret, plaintiffs alleging trade secret misappropriation must ultimately prove that they took reasonable efforts to maintain the secret.[23] "If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished."[24] To determine whether such efforts are reasonable, the trade secret owner should consider the following guidelines: "(1) the efforts to maintain secrecy need not prevent improper means of discovery; (2) the efforts must be actual; (3) the trade secret must be treated as a secret; and (4) the efforts must be directed at the trade secrets."[25] The reasonable effort involved in maintaining trade secrets will grow exceedingly as the interconnectedness of people, organizations, the nation, and the world sprawls. A Cisco Systems study estimated that the number of wireless devices in the world is expected to increase from 12.5 billion in 2010 to 25 billion in 2015.[26] Each link in that chain provides a point of susceptibility for trade secret information, particularly in an age when employers are expecting their employees to be instantly accessible.[27]

Finally, the trade secret holder must show that the defendant wrongfully acquired, or misappropriated, the trade secret.[28] According to the Uniform Trade Secrets Act, "misappropriation" means:

> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
>
> (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
>
> > (A) used improper means to acquire knowledge of the trade secret; or
> >
> > (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was
> >
> > > (I) derived from or through a person who has utilized improper means to acquire it;
> > >
> > > (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
> > >
> > > (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

> (C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.[29]

The underlying theme of trade secret misappropriation is acquisition by "improper means."[30] A trade secret owner can establish a prima facie misappropriation case if the owner "has evidence that the employee acted willfully and knew that the taking of the trade secret was improper."[31] Without such evidence, the trade secret owner must show "that the employee should have known she had a duty not to disclose the trade secret to others" by proffering evidence that the employee was on reasonable notice that the information (1) was a trade secret and (2) that the employee had a duty to keep the information confidential.[32] Common methods of misappropriation involved in economic espionage cases involve employees taking information from an employer[33] and the interception of confidential or proprietary information by third parties such as hackers.[34]

B. The Economic Espionage Act

1. Enactment of the Economic Espionage Act

The Economic Espionage Act was passed in 1996 in response to difficulties that the FBI was experiencing in prosecuting economic espionage cases.[35] According to the FBI Director at the time, Louis Freesh, existing legislation did not "specifically cover the theft or improper transfer of proprietary information and . . . [was] insufficient to protect this type of information."[36] Furthermore, many companies failed to bring civil trade secret suits against alleged misappropriators because of the difficulties involved in enforcing a monetary judgment.[37] The Economic Espionage Act, providing criminal liability for economic espionage, was designed to "fill the gaps" left by state and federal laws.[38]

The Economic Espionage Act of 1996 provides for extraterritorial jurisdictional reach, applying to conduct outside of the U.S. if the offender is a citizen or permanent resident alien in the U.S. or a U.S. organization, or if "an act in furtherance of the offense was committed in the United States."[39] The Court of Appeals for the Federal Circuit recognized Congress' concerns about the application of the Economic Espionage Act to extraterritorial based conduct, emphasizing "that it is appropriate to remedy that overseas misappropriation when it has a domestic nexus."[40]

The Act consists of two main causes of action.[41] First, under 18 U.S.C. § 1831, a defendant will be subject to criminal liability if he or she knowingly misappropriates a trade secret "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."[42] This cause of action "is designed to apply only when there is 'evidence of foreign government sponsored or coordinated intelligence activity.'"[43] A second cause of action is available under 18 U.S.C. § 1832, and is broader in the sense that a defendant need not intend for the misappropriation to benefit a foreign entity.[44] However, the trade secret must be "related to a product or service used in or intended for use in interstate or foreign government" and the defendant must intend or know "that the offense will, injure any owner of that trade secret."[45] In response to a very narrow judicial construction of a trade secret that is "related to a product or service used in or intended for use in interstate or foreign government,"[46] Congress amended the Economic Espionage Act,[47] as will be discussed further in Section I. B. 3., *infra*.

2. Judicial Interpretation of the Economic Espionage Act

The following Section is not intended to be a comprehensive review of past adjudications under Section 1830 *et seq*. Rather, this Section is meant to give a jurisprudential overview and provide the reader with the proper foundation for understanding key ways the statutory scheme has been interpreted, particularly by various Circuit courts, and how these interpretations may have prompted Congress to take action to amend the Economic Espionage Act.

a. Prosecutions under 18 U.S.C. §§ 1831 and 1832

Under 18 U.S.C. § 1831, if the alleged misappropriator intends or knows "that the offense will benefit any foreign government, foreign instrumentality, or foreign agent,"[48] he or she may be found guilty of economic espionage. The statute also provides for attempt and conspiracy charges.[49] During the course of one economic espionage investigation,[50] federal agents came across the name of Dongfan "Greg" Chung, an employee of Boeing since the 1960s.[51] In 2006, federal agents discovered approximately 300,000 Boeing documents at Chung's house, 6 pages of which had information pertaining to classified trade secrets relating to the U.S. military's Delta IV space shuttle.[52] The U.S. government was able to prove that Chung had been in contact numerous times with the China Aviation Corporation, owned by the Chinese government, and thus guilty of conspiracy and intending to benefit China under Section 1831.[53]

Under Section 1832, a defendant need not intend to benefit a foreign agent or government.[54] In *U.S. v. Krumrei*, for example, the defendant employee approached a com-

petitor telling them he would be a consultant for them in the development of a similar product.[55] The competitor contacted the defendant's employer and told them of the defendant's plan.[56] The defendant ended up selling trade secret information to a private investigator posed as an agent for the competitor and was accordingly found guilty under Section 1832 of the Economic Espionage Act.[57]

b. Defenses to Economic Espionage

The most common defenses include (1) that there were no trade secrets and (2) that the government failed to proffer sufficient evidence to support a conviction.[58] Some circuits have failed to recognize an impossibility defense to attempt or conspiracy under Section 1832.[59] Entrapment was also not recognized as a defense to the Economic Espionage Act, particularly in circumstances where the government establishes a controlled setting for offering the trade secret information to the alleged defendant.[60] Finally, Section 1832 has survived many challenges that it is unconstitutionally vague.[61]

c. Valuation of Trade Secrets and Adequate Sentencing

In *U.S. v. Howley*, two employees of a Goodyear supplier were convicted by a jury of misappropriating Goodyear's trade secrets under 18 U.S.C. § 1832.[62] The District Court sentenced each defendant to four months of home confinement, 150 hours of community service, and four years of probation.[63] On appeal, the Sixth Circuit upheld their conviction, but vacated and remanded the case for resentencing.[64] The court noted the difficulties in the valuation of trade secret information, but emphasized that even the lowest estimate that the government proffered, $305,000, would have resulted in a guidelines range of 37 to 46 months in prison.[65]

d. Limiting Constructions of the Statutory Provisions

Perhaps the most controversial holding under the Economic Espionage Act is the Second Circuit's opinion in *U.S. v. Aleynikov*.[66] The defendant was a computer programmer for Goldman Sachs from May 2007 to June 2009, developing source code for a proprietary high-frequency trading system.[67] He then accepted a position as the executive vice president of a startup company, Teza Technologies, which sought to develop its own high-frequency trading system.[68] On his last night of work at Goldman Sachs, right before heading down to his going away party, the defendant encrypted and uploaded more than 500,000 lines of source code from Goldman's system to a server in Germany.[69] He later downloaded the code to his home computer and was carrying it on a thumb drive and laptop while at meetings with Teza Technologies.[70]

In district court, the defendant was convicted by a jury of violating the Economic Espionage Act.[71] The Second Circuit reversed on principles of statutory construction, holding that the source code was not "related to a product or service used in or intended for use in interstate or foreign commerce" and thus was not a protectable trade secret under the statute.[72] The court claimed that the proprietary source code was not sufficiently related to a product used in interstate or foreign commerce because "Goldman had no intention of selling its HFT system or licensing it to anyone."[73] Following the decision, concern arose among Wall Street and the technology industry that such a narrow statutory construction would encourage misappropriation of valuable trade secret information.[74]

3. Foreign and Economic Espionage Penalty Enhancement Act of 2012

The concurring opinion in *U.S. v. Aleynikov* closes with a plea "that Congress will return to the issue and state, in appropriate language, what I believe they meant to make criminal in the EEA."[75] Congress undertook the challenge, amending the Economic Espionage Act of 1996 through the Foreign and Economic Espionage Penalty Enhancement Act of 2012. The legislation was promulgated in response "to reports of increased foreign predatory action and of 'sensitive US economic information and technology ... targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.'"[76]

Despite the pleas for clarity, Congress did not suggest any resolution to the narrow construction issues that arose in *U.S. v. Aleynikov*, but rather was focused on addressing some of the sentencing problems that the court dealt with in *U.S. v. Howley*.[77] Instead of delineating clearer boundaries for the law's application, the Foreign and Economic Espionage Penalty Enhancement Act merely increases the penalties for individuals from $500,000 to $5 million and from $10 million for organizations to the greater of $10 million or 3 times the value of the stolen trade secret.[78] The Act also provides that the United States Sentencing Commission will review punishment sentences issued under the statute.[79]

C. Executive Order

On February 12, 2013, President Obama signed an executive order titled "Improving Critical Infrastructure Cybersecurity"[80] which he emphasized in his State of the

Union Address.[81] One of the goals of the order is to prevent cyber attacks, "through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."[82] The order calls for the development of a "Cybersecurity Framework" for the development of "standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks,"[83] with provisions to have a final version published by February 12, 2014.[84] After another two years, the Department of Homeland Security, the Office of Management and Budget and the National Security Agency, along with the owners and operators of critical infrastructure must report "any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements."[85]

Supporters of the President's order tout the government's efforts to work toward increased protection against cybersecurity, particularly in light of the congressional failure to enact more comprehensive cybersecurity legislation.[86] Critics of the order tend to focus on privacy concerns and have even described the order as a "'negligence bar for cybersecurity'" because allowing voluntary participation in the sharing of cybersecurity regulation may lead to "'quasi-mandatory'" standards and "'companies that don't meet them could face lawsuits after suffering a breach.'"[87] The U.S. Chamber of Commerce criticized the order, believing "'that the executive action is unnecessary and opposes the expansion or creation of new regulatory regimes.'"[88]

The President's actions, along with the Congressional amendments to the Economic Espionage Act, make up a legislative regime that may be better classified as information gathering instead of providing substantive protection to U.S. companies' trade secrets, as will be discussed further below.

II. Practical Implications of Economic Espionage Legislation

The federal government's plan to develop a "comprehensive framework" may be a mere gesture and result in a body of law that is years behind technological development. This is not meant to impart in any way on the importance of the assembly of cybercrime-related data and the dissemination of knowledge resulting therefrom. The government's role in this particular realm may be better for merely assembling information and not enacting laws that seem superficially sufficient yet are practically inadequate. Corporate managers must take it on themselves to adequately protect their valuable trade secret information. As such, the remainder of the section addresses potential risk factors for cyber-related economic espionage and ways those risks may be abated.

A. Susceptibly to Economic Espionage

There are three main ways in which criminals obtain economic intelligence.[89] First, criminals accomplish espionage through the aggressive targeting and recruitment of insiders at U.S. companies and research institutions, often who are of the same national background.[90] Second, they conduct operations such as "bribery, cyber intrusions, theft, dumpster diving (in search of discarded intellectual property or prototypes), and wiretapping."[91] Finally, criminals may "establish seemingly innocent business relationships between foreign companies and U.S. industries to gather economic intelligence."[92] For example, in light of increased cooperation with China, including the employment of Chinese national experts at U.S. research facilities and the rapid increase in the past few years of off-shoring U.S. production and R&D operations to Chinese facilities, it is expected that Chinese government agencies and business will have more opportunities to obtain sensitive U.S. economic trade secret information.[93] It has also been reported that Russia's increased economic involvement in American markets will likely increase the number of Russian companies affiliated with the intelligence services, and that many Russian immigrants with advanced technical skills will be heavily targeted by the Russian intelligence services.[94]

B. Abating the Risk of Economic Espionage

1. Implementing Procedures to Protect Trade Secret Information

As described above, to maintain a trade secret, a company must make reasonable efforts to maintain its secrecy.[95] These efforts must be reasonable under the circumstances and "do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage."[96] Reasonable measures typically include standard security measures "such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as confidentiality agreements and document labeling, are often considered reasonable measures."[97] More generally, reasonable efforts are usually sufficient if employees are advised as to the existence of a trade secret, keeping access to the trade secret limited to a "need to know basis," and controlling access to operating facilities.[98]

2. Promoting a Widespread Dissemination of Information Regarding Already Available Tools

Promulgating information about the potential ways companies can protect trade secret information helps in the development of corporate policies that can (1) adequately stand up to a court challenge that reasonable efforts were not

employed to maintain the trade secret as a secret, and (2) provide employees with a disincentive to misappropriate, possibly quashing potential misappropriation before it occurs.

Companies may not be aware of the criminal penalties available for trade secret misappropriation, and may fail to report an incident or an attempted incident. Because of the naturally more sympathetic nature of a crime victim, as opposed to a "greedy corporation" going after a "poor ex-employee" in a civil action, courts may be more likely to protect the secret nature of the proprietary information, for example by issuing an order to preserve confidentiality.[99] Even broader protection may be available in the Third Circuit, where the Economic Espionage Act charge of attempt was held to apply in circumstances where a trade secret is not necessarily even involved, but rather in circumstances where "the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such."[100]

Certain procedural advantages may be more accessible now as well. For the first five years after the Economic Espionage Act was passed, prosecution of economic espionage and trade secret violations required approval from senior Justice Department officials; now, prosecutors must still gain approval for economic espionage charges, but approval is not required for a theft of trade secrets claim under 18 U.S.C. § 1832.[101] Furthermore, no disclosure of trade secret may be required if the defendant is charged with attempt or conspiracy.[102] And even where the trade secret information must be presented to a court, a trial court must preserve the confidentiality of the trade secret pursuant to 18 U.S.C. § 1835.[103] This section "further encourages enforcement actions by protecting owners who might otherwise 'be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth.'"[104]

If companies were aware of the previously described mechanisms by which trade secret information may be protected, it is more likely that suspected trade secret theft would be reported. And even further, with an increase in reporting, there would be a corresponding increase in available data that could be used to develop more targeted means of stopping cyber crime before it happens.

3. Encouraging Congress to Enact a More Definite Anti-Cybercrime Statute Instead of Settling for Congress's Misplaced Reliance on an Overly Deterrence Focused Amendment to the Economic Espionage Act.

The punitively focused amendments to the Economic Espionage Act clearly stem from underlying roots of deterrence theory, "a fundamentally Utilitarian approach to controlling forbidden acts, as it accepts the suffering inflicted on the convicted person as the price for the prevention of future forbidden acts for the greater general benefit of society."[105] Professor Fellmeth eloquently describes the conflicting approaches to underlying criminal theory, "that the intentional design of a legal system to achieve general deterrence offends Kantian ethics by treating human beings as mere means to achieve social goals of preventing undesirable behavior." Due to the admonition of human dignity and liberty of the alleged criminal under a purely Utilitarian scheme, one innocent individual that is wrongfully subjected to punishment could result in an "ethical tragedy."[106]

Employees run the risk of being charged with trade secret misappropriation should they use information that they obtained from their previous employers at new jobs, particularly at competing companies. Some cases involving such a factual scenario clearly fall within the bounds of the law.[107] However, if a software engineer leaves his job to start his own company, developing source code on his own initiative without the assistance of any proprietary information obtained from his old job, he may be criminally sanctioned if he unknowingly is in possession of a flash drive, for example, that contained a part of his old employer's proprietary source code. Despite the Kantian-offensive nature of subjecting the arguably innocent software engineer to months or years of federal imprisonment,[108] supporters of the Economic Espionage Act amendments continue to praise this Congressional strategy of abating cyber-attacks and trade secret theft through increased punishment. [109]

It must be recognized "that the liberal democratic adherence to a generally Kantian-type morality mingles with a contrary Utilitarian strain of thought in the United States."[110] And accordingly, Congress should be more focused on adequately defining the scope of the law and clarifying the statutory language so as to avoid a purely Utilitarian approach to controlling cyber-related trade secret misappropriation. With a more definite body of law and jurisprudence, we could be better placed to avoid anti-Kantian potential "ethical tragedies," especially in light of the heavy-handed statutory sentencing recommendations. If the Senate revives reconsideration of the Cyber Intelligence Sharing and Protection Act (CISPA) or drafts substantively related legislation,[111] they should take particular care to adequately balance Utilitarian goals with the promotion of Kantian-type morality by ensuring the statutory language is as clear and unambiguous as possible in order to avoid potential judicial interpretations such as the Second Circuit's opinion in *U.S. v. Aleynikov*.[112] It is not a shock that courts may narrowly construe a statutory

requirement in order to avoid the infliction of an overly harsh punishment. Therefore, the balance between these competing goals is key, and despite enactment of legislation that leans too far one way or the other, which will likely be the result, one can only hope that societal and moral tendencies will force the practical application of the policy to a more balanced medium.

Conclusion

The government's role in the encouragement of trade secret protection is omnipresent; however, the practical effect of recent attempts to amend economic espionage legislation may be futile. A company must, and should, take it upon itself to adequately protect its trade secret information even in light of the recent government action. A more practical method of increasing trade secret protection would result if Congress promoted the dissemination of information relating to the current trade secret enforcement regime and drafted more comprehensive conduct-focused economic espionage legislation. ▪

Endnotes

1 FBI, Economic Espionage, *http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage* (last visited May 3, 2013).

2 Bob Sullivan, *Bank Website Attacks Reach New High: 249 Hours Offline in Past Six Weeks*, NBC News (Apr. 3, 2013), *http://redtape.nbcnews.com/_news/2013/04/03/17575854-bank-website-attacks-reach-new-high-249-hours-offline-in-past-six-weeks?lite*.

3 *Id.*

4 H.R. Rep. No. 112-610, at 4 (July 19, 2012) (citing Nick Akerman et al., *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, McAffee, at 6 (Mar. 28, 2011), *http://www.mcafee.com/us/resources/ reports/rp-underground-economies.pdf*).

5 Nick Akerman et al., *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, McAffee, at 28 (Mar. 28, 2011), *http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf*; *see also* Andrew F. Popper, *Beneficiaries of Misconduct: A Direct Approach to IT Theft*, 17 Marq. Intell. Prop. L. Rev. 27, 60 (Winter 2013) ("The theft of IT or other non-tangible assets by upstream producers has a pernicious effect on fair market pricing, violates a most fundamental policy of intellectual property (protection of those who create and invent such property), and violates clear ethical norms regarding the sale of goods that benefitted from stolen IT or trade secrets.").

6 Office of the National Counterintelligence Executive, Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, at 4 (Oct. 2011), *http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf*.

7 *Id.* at 3.

8 John R. Thomas, *The Role of Trade Secrets in Innovation Policy*, Congressional Research Service, at 1 (Aug. 31, 2010), *http://www.fas.org/sgp/crs/secrecy/R41391.pdf*.

9 P.L. 112-269; H.R. No. 6029 (Jan. 14, 2013).

10 18 U.S.C. §§ 1831-1839 (2006).

11 Exec. Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739, 11739 (Feb. 19, 2013).

12 *See e.g.*, U.S. v. Chung, 659 F.3d 815 (9th Cir. 2011), *cert. denied*, No. 11-1141, 2012 WL 929750 (U.S. Apr. 16, 2012); U.S. v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

13 *See e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) (applying Ohio law).

14 *See* 18 U.S.C. § 1832(a).

15 *See* Exec. Order 13636 at 11739.

16 Michael Risch, *Why Do We Have Trade Secrets?*, 11 Marq. Intell. Prop. L. Rev. 1, 26 (Winter 2007).

17 *See e.g.*, M.C.L. §§ 445.1901-1910 (1998) (Michigan); 765 I.L.C.S. §§ 1065/1-9 (1988) (Illinois); 6 Del. C. §§ 2001-2009 (2002) (Delaware); Cal. Civ. Code §§ 3426.1-9 (1984) (California); *but see* Michael J. Hutter, *The Case for Adoption of a Uniform Trade Secrets Act in New York*, 10 Alb. L.J. Sci. & Tech. 1, 6 (1999) (New York and New Jersey have not enacted comprehensive trade secrets statutes, instead relying upon common law.).

18 Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 Stan. L. Rev. 311, 317 (Nov. 2008).

19 TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1327-28 (Fed. Cir. 2011) (citing 18 U.S.C. § 1839(3); H.R. Rep. No. 104–788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4031) ("Fortunately, trade secret law varies little from state to state and is generally governed by widely recognized authorities such as the Restatement of Unfair Competition and the Uniform Trade Secrets Act. Moreover, the federal criminal statute governing theft of trade secrets bases its definition of trade secrets on the Uniform Trade Secrets Act, so there is no indication of congressional intent to depart from the general law in that regard.").

20 Uniform Trade Secrets Act (U.T.S.A.) § 1(4) (1985). The Economic Espionage Act of 1996, as amended, has a similar, and arguably more expansive, definition of "trade secret"; *see* 18 U.S.C. § 1839(3) ("[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.").

21 Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) (applying Ohio law).

22 Office of the National Counterintelligence Executive, *supra* note 6, at 8-9.

23 *See* Risch, *supra* note 16, at 26; U.T.S.A. § 1(4).

24 Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) (citing Harrington v. National Outdoor Advertising Co., 355 Mo. 524, 532, 196 S.W.2d 786, 791 (Mo. 1946); 1 R. Milgrim, Trade Secrets § 1.01[2]).

25 David W. Slaby et al., *Trade Secret Protection: An Analysis of the Concept "Efforts Reasonable Under the Circumstances to Maintain Secrecy"*, 5 Santa Clara Computer & High Tech. L. J. 321, 326 (1989).

26 Office of the National Counterintelligence Executive, *supra* note 6, at 6.

27 *See id.*

28 Lemley, *supra* note 18, at 317.

29 U.T.S.A. § 1(2).

30 *See id.*

31 Derek P. Martin, *An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation*, 1993 B.Y.U. L. Rev. 949, 958 (Jan. 1993).

32 *Id.*

33 *See, e.g.*, U.S. v. Chung, 659 F.3d 815, 819 (9th Cir. 2011) (A Chinese national who worked for Boeing for over 40 years was found guilty of misappropriating trade secret information and providing it to agents of the Chinese government.); U.S. v. Hanjuan Jin, 833 F. Supp. 2d 977, 980 (N.D. Ill. 2012) (Former Motorola employee was charged under the Economic Espionage Act of attempting to provide Motorola's trade secret information to a telecommunications company in China that does work for the Chinese military.).

34 *See, e.g.*, U.S. v. Genovese, 409 F. Supp. 2d 253, 254-55 (S.D.N.Y. 2005) (Defendant was charged under the Economic Espionage Act with hacking proprietary portions of Microsoft's source code and posting it on the internet.).

35 H.R. Rep. No. 3723 (Sept. 16, 1996).

36 *Id.*

37 *Id.*

38 *Id.*

39 18 U.S.C. § 1837.

40 TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1330 n.4 (Fed. Cir. 2011).

41 *See* 18 U.S.C. §§ 1831-1839.

42 *Id.* at § 1831(a).

43 U.S. v. Hsu, 155 F.3d 189, 195 (3d Cir. 1998) (quoting 142 Cong. Rec. S12, 212 (daily ed. Oct. 2, 1996) (Managers' Statement for H.R. No. 3723)).

44 *See* 18 U.S.C. § 1832.

45 *Id.* at § 1832(a).

46 *See* U.S. v. Aleynikov, 676 F.3d 71, 82 (2d Cir. 2012).

47 P.L. 112-269; H.R. No. 6029 (Jan. 14, 2013).

48 18 U.S.C. § 1831(a).

49 *Id.* at § 1831(a)(4)-(5).

50 U.S. v. Chung, 659 F.3d 815, 819 n. 2 (9th Cir. 2011) (Federal agents were investigating a naval defense contractor Chi Mak, who was convicted in 2007 of, *inter alia*, acting as an unregistered foreign agent.).

51 *Id.* at 819.

52 *Id.* at 824.

53 *Id.* at 829-30. ("The government presented ample evidence that, during the 1980s, Defendant intended to benefit China by providing technical information responsive to requests from Chinese officials and by delivering presentations to Chinese engineers. Defendant also delivered a presentation on the space shuttle to Chinese engineers in 2001.").

54 See 18 U.S.C. § 1832(a).

55 U.S. v. Krumrei, 258 F.3d 535, 537 (6th Cir. 2001).

56 *Id.*

57 *Id.* at 539.

58 *See, e.g.*, U.S. v. Chung, 659 F.3d 815, 824 (9th Cir. 2011).

59 *See* U.S. v. Yang, 281 F.3d 534, 544 (6th Cir. 2002) (no impossibility defense for attempt or conspiracy); U.S. v. Hsu, 155 F.3d 189, 202 (3d Cir. 1998) (no impossibility defense for attempt).

60 U.S. v. Yang, 74 F. Supp. 2d 724, 737 (N.D. Ohio 1999) (By offering the defendants the opportunity to steal a patent application, "the Government did nothing more than present individuals who were already pre-disposed to commit economic espionage with the opportunity to do so.").

61 *See* U.S. v. Howley, 707 F.3d 575, 581 (6th Cir. 2013); *Yang*, 281 F.3d at 544 n.2; *Krumrei*, 258 F.3d at 539.

62 *Howley*, 707 F.3d at 579.

63 *Id.* at 582.

64 *Id.* at 583.

65 *Id.* at 582.

66 *See* U.S. v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

67 *Id.* at 73.

68 *Id.* at 74.

69 *Id.*

70 *Id.*

71 U.S. v. Aleynikov, 785 F. Supp. 2d 46, 83 (S.D.N.Y. 2011).

72 *See Aleynikov*, 676 F.3d at 82 ("The conduct found by the jury is conduct that Aleynikov should have known was in breach of his confidentiality obligations to Goldman, and was dishonest in ways that would subject him to sanctions; but he could not have known that it would offend this criminal law or this particular sovereign.").

73 *Id.*

74 Adam Cohen, *Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act after United States v. Aleynikov*, 30 Yale J. on Reg. 189, 190-91 (Winter 2013).

75 *Aleynikov*, 676 F.3d at 83.

76 Charles Doyle, *Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832*, Congressional Research Service, at 14 (Jan. 28, 2013), *http://www.fas.org/sgp/crs/secrecy/R42681.pdf* (quoting H.R. Rept. No.

112-610, at 2 (2012); Office of the National Counterintelligence Executive, Foreign Spies, Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, at i (Oct. 2011)).

77 *See generally* H.R. No. 6029 (Jan. 14, 2013).

78 *Id.* at 1.

79 *Id.* at 1-2.

80 Exec. Order 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11739, 11739 (Feb. 19, 2013).

81 Remarks by the President in the State of the Union Address (Feb. 12, 2013), *http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address*.

82 Exec. Order 13636, 78 Fed. Reg. at 11739.

83 *Id.* at 11741.

84 *Id.*

85 *Id.* at 11743.

86 Alexei Alexis, *President Obama Signs Executive Order On Cybersecurity, Seeks Voluntary Standards*, Bloomberg BNA (Feb. 18, 2013) ("The announcement came after months of White House deliberations in the wake of failed attempts in the previous Congress to enact cybersecurity legislation (11 PVLR 1435, 9/24/12 [the Cyber Intelligence Sharing and Protection Act (CISPA)]). Senate Majority Leader Harry Reid (D-Nev.) praised the president for taking 'decisive action' to protect the nation from cyber-attacks.").

87 *Id.* (quoting Edward R. McNicholas, Partner, Sidley Austin LLP, Washington statement Feb. 14, 2013).

88 *Id.* (quoting Ann Beauchesne, U.S. Chamber of Commerce Vice President of National Security and Emergency Preparedness, statement Feb. 13, 2013).

89 FBI, *supra* note 1.

90 *Id.*; *see also* U.S. v. Chung, 659 F.3d 815 (9th Cir. 2011) (Chinese-national employee of Boeing found guilty of intending to benefit the Chinese government under the Economic Espionage Act).

91 FBI, *supra* note 1.

92 FBI, *supra* note 1.

93 Office of the National Counterintelligence Executive, *supra* note 6, at 7-8.

94 *Id.*

95 *See* Section I. A., *supra*, at 3; U.T.S.A. § 1(4).

96 U.T.S.A. § 1 cmt. (citing E.I. du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), *cert. denied*, 401 U.S. 967 (1971)).

97 U.S. v. Chung, 659 F.3d 815, 825 (9th Cir. 2011).

98 *Id.* (quoting U.T.S.A. § 1 cmt.).

99 Douglas Nemec & Kristen Voorhees, *Recent Amendment to the Economic Espionage Act Extends Protection Against Misappropriation*, Thompson Reuters News & Insight (Feb. 13, 2013), *http://newsandinsight.thomsonreuters.com/Legal/Insight/2013/02__February/Recent_amendment_to_the_Economic_Espionage_Act_extends_protection_against_misappropriation/* (citing 18 U.S.C. § 1835 (Orders to Preserve Confidentiality)).

100 U.S. v. Hsu, 155 F.3d 189, 203 (3d Cir. 1998).

101 Doyle, *supra* note 76, at 12; *see also* U.S. Department of Justice, Criminal Resource Manual §1122 ("Prior to passage of the EEA, the Attorney General assured Congress in writing that for a period of five years, the Department of Justice would require that all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General to the Criminal Division. (See October 1, 1996 letter from Attorney General Janet Reno to Chairman Orrin Hatch, Criminal Resource Manual at 1123). This requirement expired on October 11, 2001. Subsequently, the Attorney General renewed the prior requirement for initiating prosecutions under 18 U.S.C. §1831.... The requirement was not extended for cases under 18 U.S.C. §1832...").

102 *See* U.S. v. Yang, 281 F.3d 534, 544 (6th Cir. 2002).

103 18 U.S.C. § 1835 ("[T]he court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws.").

104 U.S. v. Hsu, 155 F.3d 189, 197 (3d Cir. 1998) (quoting H.R. Rep. No. 104-788, at 13, 1996 U.S.C.C.A.N. at 4032).

105 Aaron Xavier Fellmeth, *Civil and Criminal Sanctions in the Constitution and Courts*, 94 Geo. L.J. 1, 26-27 (Nov. 2005).

106 *Id.* at 26.

107 *See, e.g.*, U.S. v. Suibin Zhang, 2012 WL 1932843, No. Cr-05-00812 (N.D. Cal. May 29, 2012) (While the defendant was still employed as an engineer with Netgear, Inc. but after he accepted a job offer from Broadcom Corp., he misappropriated trade secrets belonging to Marvell Semiconductor, Inc., a supplier of semiconductor chips to Netgear and was convicted under 18 U.S.C. § 1832.).

108 I use the phrase "arguably innocent" a bit loose here. I use the phrase to qualify the engineer's moral culpability. I do not mean to imply that he would not be found guilty if prosecuted under a trade secret statute. He very well could be found liable under a particular state law. The government or his prior employer may be able to prove that he disclosed or used a trade secret, assuming it was similar to his newly developed program, without express or implied consent "before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake." U.T.S.A. § 1(2)(ii)(C).

109 *See, e.g.*, Nemec & Voorhees, *supra* note 99 ("Finally, the EEA can also provide a stronger deterrent than corresponding civil remedies. Former employees, for example, may be less willing to risk 10 years in federal prison than a few years' injunction against working with a competitor.").

110 Fellmeth, *supra* note 105, at 26.

111 *See* Jason Koebler, *ACLU: CISPA Is Dead (For Now)*, U.S. News and World Report, *http://www.usnews.com/news/articles/2013/04/25/aclu-cispa-is-dead-for-now* (Apr. 25, 2013) (reporting that "the Senate committee is 'working toward separate bills' to improve cybersecurity, which are currently being drafted. But don't expect these bills soon . . . it'll be at least three months before the Senate takes a vote on any cybersecurity legislation.").

112 *See* U.S. v. Aleynikov, 676 F.3d 71, 82 (2d Cir. 2012).