Catholic University Law Review

Volume 62 | Issue 4 Article 1

2014

Amending the Economic Espionage Act to Require the Disclosure of National Security-Related Technology Thefts

David Orozco

Amending the Economic Espionage Act to Require the Disclosure of National Security-Related Technology Thefts

Cover Page Footnote
Assistant Professor of Legal Studies, The College of Business, Florida State University, dorozco@fsu.edu. The author appreciates the feedback received at the Florida State University's Center for Insurance Research, and the Academy of Legal Studies in Business 2012 Annual Conference.

AMENDING THE ECONOMIC ESPIONAGE ACT TO REQUIRE THE DISCLOSURE OF NATIONAL SECURITY-RELATED TECHNOLOGY THEFTS

David Orozco[+]

[+] Assistant Professor of Legal Studies, The College of Business, Florida State University, dorozco@fsu.edu. The author appreciates the feedback received at the Florida State University's Center for Insurance Research, and the Academy of Legal Studies in Business 2012 Annual Conference.

> Emerging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating. There appears to be multiple vectors of attack for persons and governments seeking to steal trade secrets. Foreign competitors of U.S. corporations, some with ties to foreign governments, have increased their efforts to steal trade secret information through the recruitment of current or former employees. Additionally, there are indications that U.S. companies, law firms, academia, and financial institutions are experiencing cyber intrusion activity against electronic repositories containing trade secret information. Trade secret theft threatens American businesses, undermines national security, and places the security of the U.S. economy in jeopardy. These acts also diminish U.S. export prospects around the globe and put American jobs at risk.
>
> As an Administration, we are committed to continuing to be vigilant in addressing threats—including corporate and state sponsored trade secret misappropriation—that jeopardize our status as the world's leader for innovation and creativity.[1]

The White House issued this statement regarding its strategy to combat trade secret theft in February of 2013.[2] This new strategy emphasizes the growing problem of foreign state-sponsored data breaches.[3] Recently, private companies and government agencies—ranging from Google to the U.S.

---

1. EXECUTIVE OFFICE OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 1-2 (2013) [hereinafter ADMINISTRATION STRATEGY], *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

2. *Id.* The White House issued this strategy report in tandem with a recent executive order promulgated on February 12, 2013. *See* Exec. Order No. 13636, 78 Fed. Reg. 11,739, 11,739-41 (Feb. 19, 2013) (envisioning greater protection of trade secrets from foreign and domestic theft by (1) mandating that federal agencies inform American companies of known cyber security threats, and (2) coordinating with the National Institutes of Standards and Technology to impose stricter standards and better procedures to protect companies from cyber attacks).

3. *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE i (2011) [hereinafter ONCIX REPORT], *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf ("Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security.").

Chamber of Commerce—have reported network breaches by overseas entities seeking to gain access to strategic information.[4]

The increasing vulnerability of domestic networks to state-sponsored groups underscores the related problem of trade secret theft committed by foreign actors.[5] Overseas-based trade secret theft poses increasing financial and security risks to the United States.[6] Although measuring specific loss is almost impossible, trade secret theft costs the United States between two and four hundred billion dollars annually.[7] Despite its financial significance, trade secret theft goes largely unnoticed because it is widely under-reported.[8] The various laws in place to protect trade secrets are ineffective due to the unavailability of a private cause of action, which impedes enforcement.[9]

---

4. *See* Siobhan Gorman, *China Hackers Hit U.S. Chamber*, WALL ST. J., (Dec. 21, 2011), http://online.wsj.com/article/SB10001424052970204058404577110541568535300.html (reporting a cyber attack on the U.S. Chamber of Commerce's computer network, resulting in the theft of "everything stored on its systems"); John Markoff, *Hackers Said to Breach Google Password System*, N.Y. TIMES, April 20, 2012, at A1, A3 (reporting that Chinese hackers stole Google's intellectual property and compromised the email accounts of two human rights activists in China). As a result of the breach of its password system, Google announced on its security blog that it would alert users if the company suspected that a cyber attack had compromised any of its users' Gmail accounts. Eric Grosse, *Security Warnings for Suspected State-Sponsored Attacks*, GOOGLE ONLINE SECURITY BLOG (June 5, 2012, 12:04 PM), http://google/onlinesecurity.blogspot.com/2012/06/security-warnings-for-suspected-state.html. According to Google's Vice President of Security Engineering,

> [w]e are constantly on the lookout for malicious activity on our systems, in particular attempts by third parties to log into users' accounts unauthorized. When we have specific intelligence—either directly from users or from our own monitoring efforts —we show clear warning signs and put in place extra roadblocks to thwart these bad actors.
>
> Today, we're taking that a step further for a subset of our users, who we believe may be the target of state-sponsored attacks. . . .
>
> You might ask how we know this activity is state-sponsored. We can't go into the details without giving away information that would be helpful to these bad actors, but our detailed analysis—as well as victim reports—strongly suggest the involvement of states or groups that are state-sponsored.

Id.

5. Google, for example, alleged that Chinese government-sponsored agents were responsible for the 2010 attack on its network. *See* Gorman, *supra* note 4; Markoff, *supra* note 4, at A1.

6. ADMINISTRATION STRATEGY, *supra* note 1, at 1; ONCIX REPORT, *supra* note 3, at 1, 3.

7. ONCIX REPORT, *supra* note 3, at 3–4.

8. ONCIX REPORT, *supra* note 3, at 3 (noting that, even if a company is aware that its trade secrets have been stolen, it may choose not to report the theft because of concerns for its reputation).

9. Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 474 (2006) ("Trade secret protection is the only branch of intellectual property [for which] there is not a private cause of action based upon federal statute.").

To complicate matters, foreign, state-sponsored actors commit trade secret theft using increasingly sophisticated data collection techniques.[10] Some actors actively target technologies that directly affect national security.[11] Digital information, cultural attitudes favoring open access to information and transparency, use of the Internet and mobile devices to communicate sensitive information, and the outsourcing and globalization of business all contribute to the increase of both domestic and foreign trade secret theft.[12]

Given the serious risk and greater frequency of data breaches, policymakers have begun to take on a more active regulatory and oversight role. For example, U.S. Senator Joe Lieberman proposed legislation to protect critical infrastructure from a cyber warfare attack.[13] Similarly, Congress recently approved increased criminal penalties for trade secret theft.[14] Finally, in 2011, U.S. Senator Chris Coons and former U.S. Senator Herb Kohl proposed additional legislation to provide a federal private cause of action for companies harmed by trade secret theft.[15]

---

10. ONCIX REPORT, *supra* note 3, at 1, 5–6 (providing examples of China's and Russia's sophisticated data-hacking programs).

11. *See, e.g.*, Gorman, *supra* note 4 (explaining that Chamber of Commerce breach was the latest in a series of economic espionage originating from China and threatening national security).

12. *See* James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 178 (1997) ("Outsourcing, collaborative engineering, and the virtual corporation have substantially increased the risk of loss through both inadvertence and espionage"); Nicole Pelroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 10, 2012, at A1 (explaining that trade secret theft is no longer "the work of insiders or disgruntled employees" because "it has become easier to steal information because of the Internet, the proliferation of smartphones and the inclination of employees to plug their personal devices into workplace networks and cart proprietary information around").

13. *See* Cybersecurity Act of 2012, S.3414, 112th Cong. (2012). The Senate rejected the bill on August 2, 2012 after a failed vote for cloture. 158 CONG. REC. S5,919 (daily ed. Aug. 2, 2012). Senator Jay Rockefeller of West Virginia revived the effort by introducing the Cybersecurity Act of 2013 in July of 2013. *See* 159 CONG. REC. S5,909 (daily ed. July 24, 2013) (introducing the Cybersecurity Act of 2013, S.1353, 113th Cong. (2013)). The bill was referred to the Committee on Science, Commerce, and Transportation for consideration on July 24, 2013. 159 CONG. REC. S5,907 (daily ed. July 24, 2013).

14. *See* Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442 (increasing the monetary penalties under the Economic Espionage Act (EEA) from a maximum of $500,000 to a maximum of $5 million for individual offenders, and from a maximum of $10 million to a maximum of the "greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design" for an organizational offender).

15. *See* 157 CONG. REC. S6,229-30 (daily ed. Oct. 5, 2011) (introducing Senate Amendment 729, which would have amended the Currency Exchange Rate Oversight Reform Act of 2011 to provide for a private cause of action for trade secret theft); Press Release, Senator Coons Introduces Two Amendments to Currency Bill to Protect American Intellectual Property (Oct. 5, 2011), http://www.coons.senate.gov/newsroom/releases/release/senator-coons-introduces-two-amendments-to-currency-bill-to-protect-american-intellectual-property (describing legislation that would create "a single, uniform, nationwide cause of action" allowing private companies to

Furthermore, the Office of the National Counterintelligence Executive (ONCIX), which coordinates with several agencies and branches of government to track the impact of industrial espionage on American competitiveness and security,[16] reported to Congress that trade secret theft through cyber technology "represent[s] significant and growing threats to the nation's prosperity and security."[17] ONCIX's findings reinforce the government's interest in cyber security and emphasize the need for the recently proposed and enacted legislation.

Defense-related technologies are a prime target for trade secret theft. For example, the Department of Defense (DOD) conducts approximately $400 billion in business with private defense contractors annually, which provides access to and allows contractors to collect and maintain sensitive information and intellectual property.[18] Consequently, the DOD requires contractors to file suspicious contact reports whenever they encounter activity that signals a possible threat.[19] However, although private contractors working with the DOD are frequently targeted, only ten percent of contractors actually file reports when they detect suspicious activity.[20] This scenario is troubling because if trade secret theft victims fail to report the crime, regulatory laws will not be enforced and harmful activity will not be deterred.[21]

To ameliorate the harmful effects of the under-enforcement of trade-secret theft penalties and network vulnerabilities, this Article proposes an amendment to the Economic Espionage Act of 1996 (EEA), a federal statute that criminalizes industrial espionage and trade secret theft.[22] The proposed

---

"sue for trade-secret theft in federal court"). The amendment was tabled. 157 CONG. REC. S6,227 (daily ed. Oct. 5, 2011).

16. ONCIX REPORT, *supra* note 3, at iii–iv (noting that, to create the report, ONCIX collaborated with "the Air Force Office of Special Investigations (AFOSI), Army Counterintelligence Center (ACIC), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Defense Security Service (DSS), Department of Energy (DoE), Department of Health and Human Services (HHS), Department of State (DoS), Federal Bureau of Investigation (FBI), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency, and Naval Criminal Investigative Service (NCIS)," among others).

17. *Id.* at i (indicating that the use of "[c]yberspace" in business "amplifies these threats by making it possible for malicious actors, whether they are corrupted insiders or foreign intelligence services (FIS), to quickly steal and transfer massive quantities of stat while remaining anonymous and hard to detect.").

18. *Id.* at A-1.

19. *Id.*

20. *Id.* (observing that defense contractors generally do not report trade secret theft unless the theft affects a contract with the Pentagon, largely because "reporting procedures are often cumbersome and redundant").

21. *See* George Stigler, *The Optimum Enforcement of Laws*, 78 J. POL. ECON. 526, 530–31 (1970) (arguing that, in order to achieve the optimal number of offenses, "rational [law] enforcement" must have "expected penalties increasing with expected gains so there is no marginal net gain from larger offenses").

22. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. §§ 1831–39 (2006 & Supp. 2012)). A prior work proposed amending the EEA to mandate

amendment to the EEA seeks to make two changes to the existing law. First, the proposed amendment imposes both civil and criminal penalties for the failure to report trade secret theft involving technology restricted by export control laws. Second, the proposed amendment establishes a whistleblower defense to encourage parties to report suspected trade secret thefts or violations of the duty to disclose.

Part I of the Article discusses the federal and state laws that protect trade secrets and the nexus between trade secrets and national security. Part II demonstrates that the existing laws are largely unsuccessful in preventing, deterring, or remedying trade secret theft against U.S. companies. Part II also examines the tension between the duty to preserve confidential information under agency law and the immunity granted to officers and directors under the fiduciary oversight doctrine developed by the Delaware courts. Part III discusses the policy justifications for amending the EEA to impose an affirmative duty to report suspected trade secret thefts. Finally, Part IV discusses the proposed amendment to the EEA and the expected positive impact that this change will have on trade secret management practices.

I. TRADE SECRET LAW AND THE RELATIONSHIP BETWEEN TRADE SECRETS AND NATIONAL SECURITY

Trade secrets are a form of intellectual property[23] that dates to the Middle Ages.[24] The term "trade secret" encompasses a broad spectrum of information that can include customer lists,[25] technical data,[26] recipes,[27] and methods of

---

affirmative disclosures as a measure to preserve national security. Aaron J. Burstein, *Trade Secrecy as an Instrument of National Security? Rethinking the Foundations of Economic Espionage*, 41 ARIZ. ST. L.J. 933 (2009). Burstein's article, in contrast to the instant work, does not address the specific changes to the EEA and the enforcement mechanics required to safeguard national security. *Id.* at 982 ("For example, policymakers would need to decide upon triggers for breach reporting, the appropriate recipient(s) of reports, penalties for failing to comply with reporting requirements, and an agenda for using breach reports. Discussing these details is beyond the scope of this Article.").

23. Trade secrets are quasi-property in the sense that the law punishes misappropriation of the trade secret, but it does not provide relief in cases involving the independent derivation of the secret—such as by reverse engineering—if the information was not misappropriated. *C.f.* 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 2.01[2], 2–11 (2001) (explaining that "the possessor of a trade secret has a property right in [the information] that permits the possessor to restrict use and disclosure of it in many situations.").

24. *See* Robert P. Merges, From Medieval Guilds to Open Source Software: Informal Norms, Appropriability Institutions, and Innovation 5 (Nov. 13, 2004) (working paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract-id=661543 (noting that medieval guilds "protected investments in training new members . . . which is a human capital formation function typically associated with modern 'trade secret' law").

25. *See, e.g.*, COLO. REV. STAT. § 7-74-102(4) (2012) (defining a "trade secret" to include a "listing of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value").

26. *See, e.g.*, UNIF. TRADE SECRETS ACT § 1(4) (1986) (defining a "trade secret" to include a "program").

conducting business.[28] Trade secrets can be critical intangible assets in a knowledge-based economy.[29] Companies expend considerable resources to generate and protect trade secrets,[30] especially information that is valuable, rare, inimitable, and non-substitutable (VRIN).[31] A VRIN resource has the potential to generate long-term and sustainable competitive advantage for companies.[32]

Theft of a company's trade secrets can occur in two ways: (1) inbound trade secret theft, and (2) outbound trade secret theft.[33] Inbound trade secret theft occurs when trade secrets are brought into a company, with or without the company's knowledge.[34] Outbound trade secret theft, conversely, occurs when a company's own trade secrets leave the company without its consent.[35] This Article is primarily concerned with imposing an affirmative duty to disclose outbound trade secret theft.

---

27. *See, e.g.*, *id.* (defining a "trade secret" to include a "formula," "method," or "process"); William Neuman, *A Man With Muffin Secrets, But No Job to Go With Them*, N.Y. TIMES, Aug. 7, 2010, at A1, A3 (describing the trade secret claim Bimbo Bakeries USA—the owner of Thomas' English muffins—filed against a former employee, which alleged that the employee stole the company's secret "nooks and crannies" recipe).

28. *See, e.g.*, UNIF. TRADE SECRETS ACT § 1(4) (defining a "trade secret" to include a "method" or "process"); Complaint para. 81, Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp., No. 09 Civ. 2862 (SCR) (S.D.N.Y. June 16, 2010), 2009 WL 1025597 (alleging trade secret misappropriation by former employees of Starwood Hotels who stole several business materials, including Strategic Plans, "Brand Bibles," and "'Property Improvement Plans,'" or templates "for how to create the 'the Ultimate W Experience' in conversion properties, providing step-by-step details for how to convert a hotel property to a W branded hotel.") *Starwood Hotels* survived a motion to dismiss. Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp., No. 09 Civ. 2862 (SCR), 2010 U.S. Dist. LEXIS 71436, at *26 (S.D.N.Y. June 16, 2010).

29. David J. Teece, Gary Pisano & Amy Shuen, *Dynamic Capabilities and Strategic Management*, 18 STRATEGIC MGMT. J. 509, 516–17 (1997).

30. *See, e.g.*, Complaint, *supra* note 28, at paras. 46–51 (describing the measure Starwood Hotels took to protect its business methods and processes, such as requiring employees to sign confidentiality agreements and certify compliance with the terms annually, securing networks and computers, allowing remote access to the company's information only through a password protected system, and marking confidential documents).

31. *See* Norman D. Bishara & David Orozco, *Using the Resource-Based Theory To Determine Covenant Not To Compete Legitimacy*, 87 IND. L.J. 979, 1009 (2012) (describing how businesses establish a legitimate business interest in non-compete cases through the ownership of a knowledge-based asset with VRIN properties); *see also* Jay Barney, *Firm Resources and Sustained Competitive Advantage*, 17 J. MGMT. 99, 105–07 (1991) (considered the seminal work on the resource-based theory of business strategy).

32. Barney, *supra* note 31.

33. *See* James Pooley & Katherine Nolan-Stevaux, *Trade Secrets and Corporate Governance: Best Practices*, IPO LAW JOURNAL—TRADE SECRETS SECTION (Nov. 10, 2005), at 1-2, http://www.ipo.org/wp-content/uploads/2013/04/TS_CorporateGovernance.pdf.

34. *See id.* at 2.

35. *See id.*

A. Regulation of Trade Secrets and Protection Against Trade Secret Misappropriation

1. Federal Law

a. The Economic Espionage Act

The EEA was enacted in 1996 as a response to the rising economic value of information, the lack of adequate federal criminal sanctions, and the inability of state criminal laws to deter trade secret theft.[36] The EEA was also meant to address the rise in post-Cold War, state-sponsored industrial espionage.[37] The Federal Bureau of Investigation (FBI) estimated that, at the time the EEA was enacted, nearly twenty-five countries had developed methods by which to illegally acquire the United States' industrial secrets.[38]

Under the EEA, a "trade secret" encompasses "all forms and types of financial, business, scientific, technical, economic, or engineering information."[39] This type of information includes "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, graphically, photographically, or in writing."[40] This information only qualifies as a trade secret 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."[41]

The EEA criminalizes misappropriation of information that meets the statutory criteria of a trade secret.[42] The EEA prohibits both the theft of trade secrets, undertaken by either domestic or foreign actors,[43] as well as industrial espionage committed for the benefit of foreign state actors.[44] Although the EEA authorizes the Department of Justice (DOJ) to initiate civil proceedings to enjoin violations of the Act, it does not create a private cause of action for the aggrieved parties.[45] Consequently, victims of misappropriation must work with the U.S. Attorney's Office to obtain relief. Penalties for misappropriating

---

36. Pooley, Lemley & Toren, *supra* note 12, at 179–80.

37. See *id.* at 179 (explaining that one of the dual purposes of the EEA was to address "the apparent threat of industrial espionage sponsored by foreign states").

38. *Id.* at 178–79.

39. 18 U.S.C. § 1839(3) (2006).

40. *Id.*

41. *Id.*

42. 18 U.S.C. §§ 1831, 1832 (2006).

43. 18 U.S.C. § 1832 (criminalizing the "[t]heft of trade secrets").

44. 18 U.S.C. § 1831 (criminalizing "[e]conomic espionage").

45. *See* 18 U.S.C. § 1836 (2006) (providing for a civil cause of action and exclusive federal jurisdiction, but making no mention of a private cause of action).

trade secretes include imprisonment and fines assessed against the offending individuals and organizations.[46] Congress recently amended the EEA to increase its monetary penalties for misappropriation.[47]

b. The International Trade Commission and Section 337 of the Tariff Act of 1930

Under Section 337 of the Tariff Act of 1930, the International Trade Commission (ITC) has the authority to consider unfair trade practices, including trade secret misappropriation involving imported products.[48] In *TianRui Group Co. v. International Trade Commission*, the Federal Circuit Court of Appeals affirmed the ITC's authority under Section 337 to apply domestic law to trade secret misappropriation occurring outside of the United States if the products related to those trade secrets were imported into the United States.[49] Commentators largely agree that the ITC is a more attractive, expedient, and powerful regulator of foreign trade secret theft, particularly for larger companies that can shoulder the litigation expenses.[50] Indeed, if the ITC rules in favor of the trade secret owner, it may issue an "exclusionary order" that prevents the defendant from shipping the implicated goods into the United States.[51] However, the ITC is not likely to play an adjudicatory role in cases affecting national security, which involve information that will benefit a

46. 18 U.S.C. §§ 1831, 1832. For example, in 2010 scientist Kexue Huang was charged with stealing trade secrets from his former employer, Dow Agrosciences. Press Release, Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets (Dec. 21, 2011), *available at* http://www.justice.gov/opa/pr/2011/December/11-crm-1696.html. He was accused of using those secrets to conduct research that would benefit Chinese universities. *Id.* Huang ultimately pleaded guilty and was sentenced to eighty-seven months in prison. *Id.*

47. *See supra* note 14 (describing the penalty increases imposed by the Foreign and Economic Espionage Penalty Enhancement Act of 2012).

48. Tariff Act of 1930, Pub. L. No. 71-361, § 337, 46 Stat. 590, 703–04 (codified at 19 U.S.C. § 1337 (2006)) (creating the ITC and authorizing it to investigate and adjudicate cases involving imports that allegedly infringe intellectual property rights and injure domestic industry).

49. 661 F.3d 1322, 1332–34 (Fed. Cir. 2011).

50. *See* Ernest P. Shriver, *Separate But Equal: Intellectual Property Importation and the Recent Amendments to Section 337*, 5 MINN. J. GLOBAL TRADE 441, 463–64 (1996).

51. 19 U.S.C. § 1337(d)(1) ("If the Commission determines, as a result of an investigation under this section, that there is a violation of this section, it shall direct that the articles concerned, imported by any person violating the provision of this section, be excluded from entry into the United States, unless, after considering the effect of such exclusion upon the public health and welfare, competitive conditions in the United States economy, the production of like or directly competitive articles in the United States, and United States consumers, it finds that such articles should not be excluded from entry."); *see also* Colleen V. Chien & Mark A. Lemley, *Patent Holdup, The ITC, and the Public Interest* 105, 122 (Stanford Law School, Working Paper No. 2022168, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2022168 (arguing that the ITC should apply economic and public policy analyses to its exclusion order decisions).

foreign state rather than information that can be used to develop or influence export markets.[52] Misappropriation of information relating to national security is outside of the exclusive jurisdiction of the ITC.[53]

c. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) is a federal statute that criminalizes a broad range of actions related to the unauthorized access of a protected computer, or a computer used in or affecting interstate or foreign commerce.[54] The CFFA criminalizes, *inter alia*, the unauthorized use of a protected computer to obtain information or to commit fraud.[55] The statute imposes both criminal and civil penalties, including compensatory damages and equitable relief for the wronged parties.[56] The CFAA has a broad scope, as it prohibits the unauthorized access of a computer, regardless of whether the computer stores trade secret information.[57]

Additionally, the CFAA specifically criminalizes the use of a protected computer to obtain national security information.[58] 18 U.S.C. § 1030(a)(1)

---

52. *See* ADMINISTRATION STRATEGY, *supra* note 1, Appx. B (describing several cases of trade secret theft and economic espionage involving technical military data stolen to improve Chinese defense systems); ONCIX REPORT, *supra* note 3, at 4–5 (noting that foreign actors, especially from China and Russia, focus their economic espionage and trade secret misappropriation efforts on information related to national security and military intelligence).

53. *See* 19 U.S.C. § 1337 (delineating the authority of the ITC to investigate import violations that affect the industry and commerce of the United States).

54. Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190–91 (codified at 18 U.S.C. § 1030 (2006)) (criminalizing unauthorized access of a computer containing sensitive information). Specific reference to "protected computers" was added to § 1030 in 1996. Economic Espionage Act of 1996, Pub. L. No 104-294, § 201, 110 Stat. 3488, 3491–92 (codified at 18 U.S.C. § 1030). A "protected computer" is a computer

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

18 U.S.C. § 1030(e)(2).

55. 18 U.S.C. § 1030(a)(4) (explaining that an individual violates § 1030(a)(4) if he "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period").

56. 18 U.S.C. § 1030(e)(11) (defining damages as "any reasonable costs to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or consequential damages incurred because of interruption of service").

57. 18 U.S.C. § 1030(a) (listing the information and sources of information protected by the statute and failing to limit that protection to trade secrets).

58. 18 U.S.C. § 1030(a)(1). This section provides that any individual who

prohibits the use of a protected computer without authorization or in excess of authorization and the subsequent willful supply of the information obtained to an unauthorized recipient.[59] The statute also prohibits the willful retention of that information.[60] However, despite the CFAA's national security provision, the statute is rarely used to prosecute national security cases because, according to the DOJ, other anti-espionage statutes offer a better precedential foundation and broader enforcement coverage.[61]

2. State Law

Each state has enacted laws, both statutorily and judicially, that protect trade secrets.[62] Trade secret protection largely depends on the state's substantive definition of a trade secret and the actions that constitute a violation of the property rights to a trade secret, or the "misappropriation" of the trade secret.[63]

Forty-six states have adopted the Uniform Trade Secrets Act (UTSA) to define, regulate, and protect trade secrets.[64] Under the UTSA, a trade secret is information that

---

> having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it . . . shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a).

59. 18 U.S.C. § 1030(a)(1).

60. *Id.*

61. H. MARSHALL JARRETT & MICHAEL W. BAILIE, PROSECUTING COMPUTER CRIMES 15 (2d ed.), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited August 23, 2013) (explaining that Assistant United States Attorneys rarely charge § 1030(a)(1) violations because of "the close similarities between sections 1030(a)(1) and 793(e)," and that, "[i]n situations where both statutes are applicable, prosecutors may tend towards using section 793(e), for which guidance and precedent are more prevalent").

62. *See* 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, 322–23 (1989) (noting that modern trade secret protection is based on the codification of common law decisions).

63. *See* Michael J. Hutter, *Trade Secret Misappropriation: A Lawyer's Practical Approach to the Case Law* 1 W. NEW. ENG. L. REV. 1, 9 (1978) (explaining that classification as a trade secret under the controlling law and "acquisition of the secret by a third party by improper conduct or unfair means" are prerequisites for liability for trade secret misappropriation).

64. MELVIN F. JAGER, TRADE SECRETS LAW § 3.29 (2013) (noting that every state except Massachusetts, New York, North Carolina, and Texas has adopted the UTSA).

> 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 [] is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[65]

The "information" in question can be "a formula, pattern, compilation, program, device, method, technique, or process."[66] A trade secret under the UTSA largely parallels the definition of a trade secret in the EEA.[67]

Although there is little state law that protects against outbound theft, all states impose civil penalties for inbound trade secret theft.[68] For example, trade secrets can be misappropriated in a UTSA jurisdiction in two ways. First, misappropriation may constitute "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."[69] Second, a trade secret is misappropriated if it is disclosed

> 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 had 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 [or her] 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.[70]

Acquiring a trade secret by "improper means" includes "theft, bribery, misrepresentation, breach or inducement of a breach to maintain secrecy, or

---

65. UNIF. TRADE SECRETS ACT § 1(4) (1986).

66. *Id.*

67. Pooley, Lemley & Toren, *supra* note 12 at 188–89 (comparing the UTSA and the EEA); *see also supra* notes 39–41 and accompanying text (detailing the definition of a trade secret under the EEA).

68. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) (defining "appropriation" of trade secrets as the receipt of the information by an unauthorized individual or in an unlawful manner); UNIF. TRADE SECRETS ACT § 1(2) (defining "misappropriation" in the same manner). Each state has developed a trade secret enforcement scheme based on the UTSA or the Restatement. Craig L. Ulrich, *The Economic Espionage Act: Reverse Engineering and the Intellectual Property Public Policy*, 7 MICH. TELECOMM. & TECH. L. REV. 147, 163–64 (2001).

69. UNIF. TRADE SECRETS ACT § 1(2)(i).

70. UNIF. TRADE SECRETS ACT § 1(2)(ii).

espionage through electronic or other means."[71] The definition of misappropriation under the UTSA is narrower than its counterpart in the EEA.[72]

Although they have not adopted the UTSA, Massachusetts,[73] New York,[74] North Carolina,[75] and Texas[76] each regulate trade secret misappropriation in a similar way. Many states have also enacted statutes that criminalize trade secret theft; however, there are significant obstacles to enforcing these statutes, including limited state budgets and jurisdiction that is restricted by the state's borders.[77]

---

71. UNIF. TRADE SECRETS ACT § 1(1).

72. Pooley, Lemley & Toren, *supra* note 12 at 188–89 (comparing the UTSA and the EEA); *see also supra* notes 42–44 and accompanying text (noting that the EEA prohibits any unlawful access to information that meets the statutory definition of "trade secret").

73. MASS. GEN. LAWS ANN. ch. 266, § 30(4) (West 2008) (defining "trade secret" as "anything tangible or intangible or electronically kept or stored, which constitutes, represents, evidences or records a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention or improvement").

74. New York trade secret protection is entirely common law based, and adopts the definition of a trade secret provided by Section 757 of the Restatement of Torts. Ashland Mgmt. Inc. v. Janien, 82 N.Y.2d 395, 407 (1993) (relying on the Restatement and state precedent to adjudicate a trade secret misappropriation case); 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) (stating that New York has not adopted a statutory regime to regulate trade secrets and instead relies on "common law principles derived from the First Restatement of Torts"). The Restatement defines a trade secret as

> any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers.

RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

75. N.C. GEN. STAT. § 66-152(3) (2011) (defining a "trade secret" as "business or technical information, including but not limited to a formula, pattern, program, device, compilation of information, method, technique, or process that (a) Derives independent actual or potential commercial value from not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from its disclosure or use; and (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy").

76. Like New York, Texas regulates trade secrets with common law decisions based on the Restatement of Torts. *In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b) ("To determine whether a trade secret exists, this Court applies the Restatement of Torts' six-factor test.").

77. Pooley, Lemley & Toren, *supra* note 12 at 186 (stating that twenty-four states have criminal trade secret theft statutes, but that "the applicability of these state criminal laws is limited by jurisdiction and lack of state resources, particularly in cases with international ramifications").

3. Private Protection of Trade Secrets

In addition to the common law and state and federal statutory regimes designed to deter and rectify trade secret theft, owners of sensitive information often use private legal and non-legal mechanisms to preemptively secure information. For example, companies often employ non-disclosure agreements, confidentiality agreements, and covenants-not-to-compete to add layers of protection to their confidential data.[78] Additionally, companies may use property systems such as patents or copyrights, in conjunction with trade secrets, to increase information security.[79] Finally, companies may use non-legal mechanisms used to protect trade secrets, such as well-designed human resource and compliance systems,[80] protected networks, and encryption devices.[81]

B. National Security Implications

According to ONCIX, trade secret theft by foreign agents has clear and significant implications for national competitiveness because many of the country's most profitable and rapidly-growing industries are targeted for trade secret theft.[82] For example, ONCIX states that clean technologies—energy -generating technologies that reduce carbon dioxide emissions—are highly valued targets for acquisition.[83] Clean technologies have been linked to long -term energy security,[84] and investments in these technologies have grown quickly as a result.[85] Similarly, pharmaceuticals, nanotechnology, and agricultural technologies—all of which are industries characterized by high

78. Bishara & Orozco, *supra* note 31, at 995–96; Pooley, Lemley & Toren, *supra* note 12, at 218.

79. Bishara & Orozco, *supra* note 31, at 996.

80. *See, e.g.*, Russell W. Coff, *Human Assets and Management Dilemmas: Coping with Hazards on the Road to Resource-Based Theory*, 22 ACAD. MGMT. REV. 374, 380–87 (1997), *available at*

http://www.jstor.org/stable/259327 (discussing the use of incentives, symbolic gestures, control rights, and shared governance as methods to retain employees).

81. Ari B. Good, *Trade Secrets and the New Realities of the Internet Age*, 2 MARQ. INTELL. PROP. L. REV., 51, 92–93 (1998).

82. ONCIX REPORT, *supra* note 3, at 8-9 (explaining that foreign collection of U.S. civilian technologies follows market patterns of investment and trade). ONCIX predicts that clean technologies, advanced materials and manufacturing techniques, healthcare, pharmaceuticals, and agricultural technologies will experience a surge in investment and therefore will be targeted aggressively for acquisition. *Id.*

83. ONCIX REPORT, *supra* note 3, at 8.

84. *See* David Orozco, *Administrative Patent Levers in the Software, Biotechnology and Clean Technology Industries*, *in* THE CHANGING FACE OF US PATENT LAW AND ITS IMPACT ON BUSINESS STRATEGY 42, 54–56 (Daniel C. Cahoy & Lynda J. Oswald eds. 2013); *see also* Daniel R. Cahoy, *Inverse Enclosure: Abdicating the Green Technology Landscape*, 49 AM. BUS. L. J. 805, 829–31, 834 (2012).

85. ONCIX REPORT, *supra* note 3, at 8.

research and development costs—are also targeted frequently for theft.[86] Loss of trade secrets in these quickly-evolving areas of business has a direct impact on national competitiveness. As one government enforcement official explained, "[w]e've already lost our manufacturing base. . . . Now we're losing our R. & D. base. If we lose that, what do we fall back on?"[87]

Trade secrets also significantly affect national security if they relate to classified information or information pertaining to military technologies. ONCIX stated that the "illicit transfer of technology with military applications to a hostile state [or organization] could endanger the lives of US and allied military personnel."[88] Some military technologies are especially susceptible to trade secret theft;for example, according to ONCIX and the DOD, Autonomous Underwater Vehicles (AUVs) are routinely targeted for theft.[89]

Many technologies related to national security are categorized as dual-use technologies, or technologies that can be used for both military and non

-military purposes.[90] Consequently, many dual-use technologies are regulated under export control laws rather than trade secret laws. For example, the Export Administration Act of 1979 authorizes the President to control U.S. exports for the purpose of national security.[91] The Department of Commerce's Bureau of Industry Security (BIS) is responsible for administering and enforcing the Export Administration Act.[92]

---

86. *Id.* at 8–9.

87. Nicole Perlroth, *Traveling Light in a Time of Digital Thievery*, N.Y. TIMES, Feb. 10, 2012, at A3 (internal quotation marks omitted).

88. ONCIX REPORT, *supra* note 3, at 3; *see also* United States v. Dongfan Chung, 659 F.3d 815, 828 (9th Cir. 2011) (upholding the conviction of the defendant for violating the EEA by unlawfully transferring trade secrets pertaining to military aircraft technology).

89. DEFENSE SECURITY SERVICE, TARGETING U.S. TECHNOLOGIES 16 (2011), *available at* http://www.dss.mil/counterintel/2011-unclassified-trends.pdf (describing AUVs as "a class of underwater vessels capable of submerged, self-propelled locomotion using various enabling technologies to navigate and perform diverse tasks").

90. DEPARTMENT OF COMMERCE, INTRODUCTION TO COMMERCE DEPARTMENT EXPORT CONTROLS 1 (2010) [hereinafter DEP'T OF COMMERCE], *available at* http://www.bis.doc.gov/index.php/forms-documents/doc_view/142-eccn-pdf.

91. Export Administration Act of 1979, Pub. L. No. 96-72, §§ 3(2)(B), 5(a)(1), 93 Stat. 503, 504, 506 (codified at 50 U.S.C. App. §§ 2402, 2404) (authorizing the President to "prohibit or curtail the export of any goods or technology subject to the jurisdiction of the United States or exported by any person subject to the jurisdiction of the United States," to the extent necessary "to further significantly the foreign policy of the United States or to fulfill its declared international obligations").

92. *See* DEP'T OF COMMERCE, *supra* note 90. The BIS enforces the Export Administration Act by issuing Export Administration Regulations (EARs). *Id.* An important aspect of these regulations is the Commerce Control List (CCL), which includes all of the technologies that fall under the EARs. *Id.* at 3. These technologies include broad categories such as: nuclear technologies, materials, chemicals, microorganisms, materials processing technologies, electronics, computers, telecommunications, information security, sensors and lasers, navigation and avionics, marine and propulsion systems. *Id.*; *see also* 15 C.F.R. § 777 Supp. 1 (2012) (containing the full Commerce Control List).

The Department of Commerce defines an export as "any item that is sent from the United States to a foreign destination."[93] Under the Department's regulations, the method of exportation is immaterial; the item may be classified as an export if it is sent via regular mail, hand carry, facsimile, the Internet, by telephone, or delivered in person.[94] Because trade secret theft is increasingly committed by foreign actors targeting a broad array of technologies that are regulated by export controls, many thefts have, as a practical matter, the same effect as the unauthorized exportation of goods.[95]

The BIS has the authority to regulate military technologies, dual-use technologies, and even some purely commercial technologies with export controls.[96] Regulated technologies are categorized with an Export Control Classification Number (ECCN), which identifies items based on the nature of the product.[97] ECCNs allow exporters to determine the "reasons for control," which transactions require an export license (based on the country of destination), and which license exceptions, if any, apply.[98]

II. THE CHALLENGES OF ENFORCING TRADE SECRET MISAPPROPRIATION LAWS

A. Under-Enforcement

Trade secrets can be difficult to manage and protect. First, the protection of trade secrets hinges on fiduciary relationships, which trigger mutual and corresponding duties.[99] Unlike patents, trademarks, designs, and copyrights, the safeguarding of trade secrets largely depends on individuals' ability to uphold the legal duties that arise from fiduciary relationships.[100]

---

93. DEP'T OF COMMERCE, *supra* note 90, at 2.

94. *Id.*

95. *Compare* ONCIX REPORT, *supra* note 3, at 1, 8–9 (noting that economic, scientific, and military data are subject to trade secret theft and predicting that dual-use technologies such as clean technologies, advanced manufacturing techniques, healthcare and pharmaceutical technologies, agricultural technology, and energy and national resource information will be increasingly vulnerable to misappropriation), *with* DEP'T OF COMMERCE, *supra* note 90, at 1–2 (noting that dual-use technologies and chemicals, materials processing, computers, and telecommunications and information security are all subject to export controls), *and* 15 C.F.R. § 777 Supp. 1 (listing other scientific technologies in the Commerce Control List regulated by export laws).

96. DEP'T OF COMMERCE, *supra* note 90, at 1.

97. *Id.* at 3.

98. *Id.* at 5–6 (providing instructions for determining whether a license is necessary for a particular good or technology and whether a licensing exception applies).

99. *See* RESTATEMENT (THIRD) OF AGENCY § 1.01(e) (2005). Contracts such as non-disclosure agreements, confidentiality agreements, and covenants not to compete may supplement the default duties arising under agency. *See id.* ("In addition to an agent's fiduciary duties, the agent has a duty to fulfill specific contractual undertakings" imposed by the principal).

100. The need for fiduciary controls is because trade secrets do not possess traditional *in rem* property characteristics. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939) (rejecting the

Trade secrets, like other intangible assets, are non-excludable;[101] absent vigorous monitoring and expensive judicial enforcement, trade secrets are freely accessible.[102] To successfully plead trade secret misappropriation, the plaintiff must overcome a defense of independent derivation, under which the defendant claims that he discovered the trade secret through reverse engineering, or through other permissible means.[103] The burden is also on the plaintiff to prove that he expended reasonable efforts to preserve secrecy.[104] This standard can be challenging to satisfy in cases in which the plaintiff

---

idea that the prohibition of trade secret misappropriation is based in the owner's property right in the information); MILGRIM, *supra* note 23, at § 2.01 (noting that the "property" right in a trade secret is the right to use and disclose the information).

101. *See* MILGRIM, *supra* note 23, at § 2.01 ("[N]either the owner of a trade secret or a copyright can use its rights to prevent genuine independent development by others."). *See generally* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 1-19 (1999) (discussing the "information economy"). Although other categories of intangible property—such as patents, trademarks, and copyright—face challenges involving non-excludability and costly enforcement, protection of these other forms of intellectual property is not as under-enforced as protection of trade secrets because of measures to reduce enforcement costs. *See, e.g.*, David L. Schwartz, *The Rise of Contingent Fee Representation in Patent Litigation*, 64 ALA. L. REV. 335, 346, 351–55 (2012) (describing the rise of contingent-fee agreements in patent litigation). Rather, protection of this information is often vigorously enforced. For example, policymakers in the field of trademark law have held hearings on the aggressive enforcement and policing of trademarks by large companies against smaller companies and individuals, leading to what is termed "trademark bullying." *See* Trademark Technical and Conforming Amendment Act of 2010, Pub. L. No. 111-146, § 4(a)(1), 124 Stat. 66, 70 (requiring the U.S. Patent and Trademark Office to study and report to Congress "the extent to which small businesses may be harmed by litigation tactics by corporations attempting to enforce trademark rights beyond a reasonable interpretation of the scope of the rights granted to the trademark owner"). The under-enforcement of trade secret law, therefore, is an anomaly.

102. *Cf.* SHAPIRO & VARIAN, *supra* note 101, at 4–5 (explaining that, because of the ease with which intellectual property can be copied, owners of intellectual property keep the information closely guarded and protect their rights with increased protection). In 2011, the American Intellectual Property Law Association (AIPLA) conducted surveys to determine the costs of intellectual property litigation. AM. INTELL. PROP. ASS'N, REPORT OF THE ECONOMIC SURVEY 2011 (2011). The survey found that, in cases in which the amount in controversy was less than $25 million, the cost of trade secret litigation through trial was $1.3 million. *Id.* If the amount in controversy exceeded $25 million, the cost of litigation increased to $3.2 million. *Id.*

103. *See, e.g.*, Int'l Election Sys. Corp. v. Shoup, 452 F. Supp. 684, 709–10 (E.D. Pa. 1978) (dismissing the plaintiff's trade secret theft claim because the defendant established that it developed its own market to sell its product, rather than misappropriating the plaintiff's customer list data). Reverse engineering is "the process of studying an item in hopes of obtaining a detailed understanding of the way it works," and is "used to create duplicate or superior products without the benefit of having the plans for the original item." Uhrich *supra* note 68 at 155–56.

104. *See* 18 U.S.C. § 1839(3)(A) (2006) (requiring the owner of information to "take [] reasonable measures to keep such information secret" for the information to be classified as a trade secret); UNIF. TRADE SECRETS ACT § 1(4) (1986) (requiring that the information be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy" for the information to be classified as a trade secret); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) ("The subject matter of a trade secret must be secret.").

created the protected information with the help of third parties, especially if the value of the information has appreciated over time.[105]

Similarly, significant hurdles impede the enforcement of criminal trade secret laws. Indeed, many believe that the DOJ imposes substantial prerequisites for enforcement under the EEA.[106] According to some accounts, U.S. attorneys' offices have imposed a six- or seven-figure loss requirement as a precondition for prosecution.[107] The DOJ is also hesitant to criminally prosecute cases unless a civil remedy is unavailable.[108] Additionally, there are several other factors that discourage parties from pursuing an EEA claim, such as the higher burden of proof necessary to criminally convict under the EEA, the possibility of a lengthy grand jury investigation, the federal government's exclusive management of important litigation issues, the forfeiture of the attorney-client privilege and work-product immunity afforded by civil trials, and the lack of monetary damages.[109] These restrictions may prevent firms from reporting trade secret theft, compounding the public safety concerns surrounding the theft of information affecting national security.

Despite the difficulty in addressing trade secret theft, civil litigation of domestic trade theft is on the rise, demonstrating the importance of trade secret information.[110] However, this increase reflects only domestic civil suits, not claims brought under the EEA.[111] Indeed, although ONCIX reports that trade

---

105. Bishara & Orozco, *supra* note 31, at 1011. A recent high-profile example of a company's failure to keep data secret involved hackers stealing LinkedIn account users' passwords. Nicole Perlroth, *Lax Security at LinkedIn is Laid Bare*, N.Y. TIMES, June 11, 2012, at B1. The media widely reported that the breach was the result LinkedIn's out-of-date and inadequate security systems. *See, e.g.*, *id.*

106. Pooley, Lemley & Toren, *supra* note 12, at 210–11 (noting that an Assistant U.S. Attorney's decision to prosecute a trade secret misappropriation case is subject to DOJ approval, from either the Attorney General, the Deputy Attorney General, or an Assistant Attorney General from the Criminal Division). U.S. Attorneys' offices consider a number of factors in determining whether a trade secret case will be prosecuted, including "(a) whether the information was clearly a trade secret; (b) whether the information was technical or scientific in natures; (c) evidence of criminal conduct and intent; (d) evidence of the information's monetary value; (e) the availability of other remedies; and (f) whether the misappropriation was promptly reported." *Id.* at 211.

107. Victoria Slind-Flor, *Industry Spying Still Flourishes*, NAT'L L.J., Mar. 29, 2000, at B8; *see also* Pooley, Lemley & Toren, *supra* note 12, at 214 (indicating that "the monetary loss to the victim must be great enough to merit criminal investigation and prosecution," greater than $100,000 in some districts).

108. Pooley, Lemley & Toren, *supra* note 12, at 215.

109. Joseph N. Hosteny, *The Economic Espionage Act: A Very Mixed Blessing*, INTELL. PROP. TODAY, Feb. 1998, 7–8, http://www.hosteny.com/articles/espionage.html.

110. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 66–68 (2011) [hereinafter *State Court Analysis*] (finding that trade secret litigation in federal courts is increasing at an exponential rate, but at the same time is increasing at only a modest rate in state courts).

111. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 303–04 (2009) [hereinafter *Federal Court Analysis*]. The Almeling study of trade secret litigation in federal courts concluded that concerns about foreign

secret theft by foreign actors is growing at a considerable pace,[112] this type of trade secret theft is rarely prosecuted.[113] The restrictions imposed by the DOJ and the EEA itself likely discourage injured parties from reporting violations and from using the statute as an enforcement mechanism. The failure to report trade secret theft and to enforce trade secret laws, in turn, motivates trade secret thieves to continue engaging in this profitable activity.[114]

B. Market Failures

Given their status as valuable property rights, the marketplace should, in theory, provide adequate incentives to safeguard and enforce trade secrets. Evidence indicates that, although prosecution of domestic trade secret thefts has increased, cases involving foreign actors remain unenforced.[115] This disparity, according to a market efficiency theory, is caused by (1) cross-border enforcement costs; (2) negative reputational impact; and (3) inadequate information technology (IT) and compliance capabilities.

1. Cross-Border Enforcement Costs

Pursuing civil remedies in foreign trade secret theft cases under the EEA is often prohibitively expensive. First, the complexities that arise during the discovery process can significantly raise litigation costs.[116] To further complicate matters, each country has its own trade secret law and hiring local counsel with adequate knowledge of a foreign jurisdiction's legal system and

---

trade secret misappropriation "may be overblown" because most trade secret theft is committed by domestic actors. *Id.* This statement, however, does not take into account the central problem of foreign trade secret theft, which is that the victim is often reluctant to pursue claims of foreign theft due to the inordinate costs of litigation. *See supra* notes 106–09 and accompanying text (discussing the barriers to trade secret law litigation and enforcement). Moreover, there is a fundamental difference between domestic theft and foreign state-sponsored theft, adding to the disparity between the number of domestic theft cases and foreign theft cases. While the majority of plaintiffs in domestic theft cases know the defendants, *State Court Analysis*, *supra* note 110, at 69 (noting that domestic thieves are often former employees or business partners), data thieves in cases involving foreign actors are usually anonymous, *Federal Court Analysis*, *supra*, at 303.

112. ONCIX REPORT, *supra* note 3, at 1.

113. *See id.* at 5 (reporting that only seven cases were adjudicated under the EEA in 2010).

114. *See id.* at 4 (estimating that a company's trade secret can be worth $20 million and that trade secret theft and economic espionage are responsible for the loss of up to $400 billion each year).

115. *See State Court Analysis*, *supra* note 110, at 66–68 (tracking the increase in trade secret theft litigation in state and federal courts); ONCIX REPORT, *supra* note 3, at 5 (reporting that there were only seven prosecutions under the EEA in 2010); *Federal Court Analysis*, *supra* note 111, at 303–04 (noting that third parties, such as foreign actors, "comprise a small percentage of alleged misappropriators").

116. *See* J. Benjamin Bai & Gupoing Da, *Strategies for Trade Secret Protection in China*, 9 NW. J. TECH & INTELL. PROP. 351, 362 (2011) (explaining that there is no U.S.-style discovery process in China and discussing other technical hurdles that make discovery in foreign trade secret litigation more cumbersome than in domestic litigation).

paying for translation services can raise costs substantially.[117] Similarly, attempting to gather evidence abroad can pose unique challenges that require patience, creativity, and significant resources.[118]

Because it is so difficult to litigate, foreign trade secret theft is best reserved for federal authorities to address under the appropriate criminal statutes and with the aid of government intelligence information and enforcement mechanisms. The U.S. government is especially interested in discovering the sources of the theft of sensitive information because of the national security concerns.[119] The U.S. government, unlike private companies, has the intelligence capabilities needed to uncover the sources of this theft.[120] Private companies, on the other hand, are either unable to trace the party's identity or unwilling to do so.[121] It is also increasingly difficult for private companies to distinguish between cyber crime, trade secret theft, and the collection of economic or technological information by foreign intelligence services.[122]

2. Reputational Costs

When a company discovers that a trade secret has been stolen, more often than not the company will choose not to seek legal remedy. According to ONCIX, a company may keep a security breach private because it could "tarnish a company's reputation and endanger its relationships with its investors, bankers, suppliers, customers and other stakeholders."[123] An empirical study using an event study methodology confirmed that the value of a publicly traded company can decrease by millions of dollars when the company announces that it has decided to work with federal officials to prosecute a case under the EEA.[124] Many companies, absent regulations requiring affirmative disclosure, elect to remain silent and allow the theft to go unpunished.[125] Moreover, the unavailability of civil damages under the EEA

117. *See* R. Doak Bishop, *International Litigation in Texas: Obtaining Evidence in Foreign Countries*, 19 HOUS. L. REV. 361, 361 (1982).

118. *Id. See generally* HAROUT J. SAMRA, THE OPPORTUNITIES AND CHALLENGES OF USING U.S. DISCOVERY IN AID OF FOREIGN AND INTERNATIONAL PROCEEDINGS (2013), *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac2013/sac_2013/13_using_discovery_in_aird.authcheckdam.pdf (discussing various techniques to conduct U.S.-style discovery abroad).

119. ADMINISTRATION STRATEGY, *supra* note 1, at 1 (expressing a commitment to prosecuting foreign trade secret theft, which "threatens American businesses, undermines national security, and places the security of the U.S. economy in jeopardy").

120. ONCIX REPORT, *supra* note 3, at 2.

121. *Id.* at 1–2 (noting that private companies are more concerned with addressing the damage caused by trade secret theft than identifying the perpetrator).

122. *Id.* at 1.

123. *Id.* at 3.

124. *See* Chris Carr & Larry Gorman, *The Revictimization of Companies by the Stock Market Who Report Trade Secret Theft Under the Economic Espionage Act*, 57 BUS. LAW. 25, 48–49 (2001) (finding that the stock market negatively reacts to the disclosure of trade secret theft).

125. ONCIX REPORT, *supra* note 3, at 3.

to offset these reputational costs provides little incentive for private companies to report theft.[126]

3. Inadequate IT and Compliance Capabilities

Some business managers view investment in IT programs as an unnecessary cost.[127] Indeed, companies may reach a level of sophistication at which investment in IT safeguards has a negative impact on the company's ability to compete with market prices.[128] However, IT capabilities have a demonstrably positive effect on business strategy and have a significant impact on a company's bottom line.[129] The perception of investment in IT as a cost driver may, therefore, lead to suboptimal investments in IT capabilities meant to safeguard a company's most valuable technologies and knowledge-based assets.[130]

Accordingly, it is crucial for businesses to integrate IT security programs into their top leadership team, as well as into legal and compliance departments.[131] Multifunctional coordination of IT resources is important for security because it can contribute to successful legal outcomes in the event of a breach,[132] as well as to help companies proactively keep track of information moving within and in and out of the organization.[133] To compound the problem, companies increasingly rely on a "high velocity" and contingent workforce, which may facilitate the movement of sensitive information.[134] The highly mobile state of information in modern business justifies investment

126. Civil relief under the EEA constitutes injunctive relief. 18 U.S.C. § 1836 (2006). The statute provides no private cause of action for damages. *Id.*

127. Robert C. Bird, *Pathways of Legal Strategy*, 14 STAN. J.L. BUS. & FIN. 1, 9 (2008).

128. Joseph S. Nye, Jr., *Nuclear Lessons for Cybersecurity?*, STRATEGIC STUD. Q. 18, 28 (2011) (noting that "[f]irms have an incentive to provide for their own security up to a point, but the competitive pricing of their products limits" those expenditures).

129. Bird, *supra* note 127, at 10.

130. *See* Nye, *supra* note 128, at 28–29 (concluding that there is "an underinvestment in security from the national perspective").

131. *See* Russell Beck & Matt Karlyn, *IT Security: A Practical Approach to Protecting Trade Secrets*, CIO (Nov. 11 2009), http://www.cio.com/article/507359/IT_Security_A_Practical_Approach_to_Protecting_Trade_Secrets?page=3&taxonomyId=3187 (advocating for cooperation between business owners and directors, legal counsel, and IT departments to protect their companies from trade secret theft).

132. *See* David Orozco, *Legal Knowledge as an Intellectual Property Management Resource*, 47 AM. BUS. L.J. 687, 687–94 (2010) (discussing the importance of integrating legal and managerial knowledge as a source of competitive advantage); David Orozco, *Rational Design Rights Ignorance*, 46 AM. BUS. L.J. 573, 603–04 (2009) (discussing how companies can obtain unique and rare intellectual property outcomes by reducing coordination costs within the firm).

133. ONCIX REPORT, *supra* note 3, at i, 3 (noting that businesses are often uninformed of how information moves within and outside of the boundaries of the organization and that "[m]any companies are unaware when their sensitive data is pilfered").

134. Bishara & Orozco, *supra* note 31, at 1004.

in state-of-the-art IT security programs and the addition of IT representatives to various levels and departments within an organization.

C. Agency-Related Legal Impediments

In addition to market failures and high transaction costs, deficiencies in the general legal framework result in poor management and enforcement of trade secret laws and insufficient reporting of trade secret theft. The two most problematic impediments to the enforcement of trade secret laws are the inadequate protection of whistleblowers and lax corporate governance requirements.

1. Inadequate Protection of Whistleblowers

None of the existing trade secret statutory regimes require a party to report a suspected trade secret theft.[135] Additionally, none of the statutes provide whistleblower protection for an individual who discloses trade secret theft and consequently faces retaliation from his employer.[136]

Although the majority of states have enacted laws to shield public employees from retaliation by their employers, few states extend that protection to employees of private companies.[137] Moreover, state whistleblower laws vary significantly in the level of protection offered to employees.[138] Employers are also able to circumvent whistleblower protection laws by hiring at-will employees, who can be fired at any time and for any reason—including purely retaliatory discharge—without exposing the employer to liability.[139]

Because there is no affirmative legal duty to disclose trade secret theft, existing state laws largely fail to protect employees who report trade secret theft. Many state whistleblower laws, however, require the disclosure to be of violations of law committed by the employer in order for the employee to qualify for protection from retaliation.[140] Consequently, without a duty to

---

135. *See supra* Part I.A. and accompanying text (detailing the federal and state regulation of trade secrets).

136. *See* 18 U.S.C. § 1030 (2006) (no protection for whistleblowers); 18 U.S.C. §§ 1831–39 (2006 & Supp. 2012) (same); 19 U.S.C. § 1337 (2006) (same); UNIF. TRADE SECRETS ACT (1986) (same).

137. Elletta Sangrey Callahan & Terry Morehead Dworkin, *The State of State Whistleblower Protection*, 38 AM. BUS. L.J. 99, 111 (2000); Kevin Rubenstein, Note, *Internal Whistleblowing and Sarbanes-Oxley Section 806: Balancing the Interests of Employee and Employer*, 52 N.Y.L. SCH. L. REV., 637, 643 (2007) ("Most states offer general whistleblower protection to public employees, while a minority of states provide the same protection to all workers.").

138. Rubenstein, *supra* note 137.

139. *Id.* at 640 (observing that a "[s]trict application of [the at-will] doctrine would allow an employer to terminate a whistleblower without facing any liability even if the discharge was purely for retaliatory purposes").

140. For example, New York's whistleblower protection statute states that:

report trade secret theft and corresponding protection for the disclosing employee, an employer is free to take action against employees revealing trade secret theft without violating any law.

Conversely, federal law offers a patchwork of whistleblower protection, but only in cases in which the specific statute grants immunity from retaliation.[141] The federal law that could offer the most protection to whistleblowers of trade secret misappropriation is Section 806 of the Sarbanes-Oxley Act.[142] Section 806 provides a civil remedy to any employee who suffers retaliation for reporting a securities fraud or violation, or the violation of any provision of federal law prohibiting fraud against shareholders.[143] Section 806 applies to companies "with a class of securities registered under Section 12 of the Securities Exchange Act of 1934 . . . or that [are] required to file reports under

---

> An employer shall not take any retaliatory personnel action against an employee because such employee . . . discloses, or threatens to disclose to a supervisor or to a public body an activity, policy, or practice *of the employer* that is in violation of law, rule or regulation which violation creates and presents a substantial and specific danger to the public health or safety, or which constitutes health care fraud.

N.Y. LAB. LAW § 740(2)(a) (McKinney 2002 & Supp. 2013) (emphasis added).

141. Some federal statutes offer protection for whistleblowers who charge or testify against their employers for violating the particular statute. *See, e.g.*, 15 U.S.C. § 15(a) (2006) (prohibiting the discharge of an employee who reports violation of the Clayton Act); 15 U.S.C. § 2622(a) (2006) (prohibiting the discharge of an employee who reports violation of the Toxic Substances Control Act); 18 U.S.C. § 1514A (2006 & Supp. 2012) (prohibiting the discharge of an employee who reports violation of the Sarbanes-Oxley Act); 29 U.S.C. § 158(a)(4) (2006) (prohibiting the discharge of an employee who reports violation of the National Labor Relations Act); 29 U.S.C. § 206(d) (2006) (prohibiting the discharge of an employee who reports violation of the Equal Pay Act); 29 U.S.C. § 215(a)(3) (2006) (prohibiting the discharge of an employee who reports violation of the Fair Labor Standards Act); 29 U.S.C. § 623(d) (2006) (prohibiting the discharge of an employee who reports violation of the Age Discrimination in Employment Act); 29 U.S.C. § 660(c) (2006) (prohibiting the discharge of an employee who reports violation of the Occupational Safety and Health Act); 29 U.S.C. §§ 1132(a), 1140 (2006 & Supp. 2012) (prohibiting the discharge of an employee who reports violation of the Employee Retirement Income Security Act); 29 U.S.C. § 2615 (2006) (prohibiting the discharge of an employee who reports violation of the Family and Medical Leave Act); 31 U.S.C. § 3730(h) (2006 & Supp. 2011) (prohibiting the discharge of an employee who reports violation of the False Claims Act); 42 U.S.C. § 300j-9(i)(1) (2006) (prohibiting the discharge of an employee who reports violation of the Safe Drinking Water Act); 42 U.S.C. § 12203(a) (2006) (prohibiting the discharge of an employee who reports violation of the Americans with Disabilities Act); 42 U.S.C. § 2000e-3(a) (2006) (prohibiting the discharge of an employee who reports violation of the Civil Rights Act of 1964); 42 U.S.C. § 5851(a) (2006) (prohibiting the discharge of an employee who reports violation of the Energy Reorganization Act); 42 U.S.C. § 6971(a) (2006) (prohibiting the discharge of an employee who reports violation of the Solid Waste Disposal Act); 42 U.S.C. § 7622(a) (2006) (prohibiting the discharge of an employee who reports violation of the Clean Air Act); 42 U.S.C. § 9610(a) (2006) (prohibiting the discharge of an employee who reports violation of the Comprehensive Environmental Response, Compensation, and Liability Act).

142. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 806, 116 Stat. 745, 802–04 (codified at 18 U.S.C. § 1514A).

143. § 806, 116 Stat. at 802.

Section 15(d) of the Securities Exchange Act of 1934."[144] However, Section 806 would likely fail to offer relief to an employee suffering from retaliation by his employer as a consequence of disclosing trade secret theft because the failure to report trade secret misappropriation has never been classified as a fraud on a company's shareholders.[145] Furthermore, because Section 806 applies to only the small subset of public companies registered under Section 12, many of the companies most vulnerable to trade secret theft—those companies developing technologies that affect national security—fall outside of the statute's reach.[146]

2. Ineffective Corporate Fiduciary Law

A basic tenet of American law is that a corporation's directors and executives have a fiduciary duty to the organization. The fiduciary relationship is created by the law of agency, under which the agent agrees to act on the principal's behalf and is subject to the principal's control.[147] This relationship creates duties and corresponding rights between the parties.[148]

Existing corporate fiduciary laws are poorly equipped to address cases involving trade secret theft, particularly those cases involving a foreign state -sponsored entity. Consequently, if a foreign actor misappropriates trade secrets as the result of the breach of a corporate fiduciary duty, there is no adequate safeguard to establish liability.

a. The Business Judgment Rule and Trade Secret Misappropriation

Directors of a corporation are legally required to oversee fundamental transactions, such as the sale of the business, a merger, changes to the capital structure, and the appointment and compensation of the chief executive officer.[149] These decisions are fundamental transactions of the corporation and are therefore evaluated under the business judgment rule.[150] The business

144. *Id.*

145. *Cf.* Rustad, *supra* note 9, at 474 (noting that there is no affirmative duty to report trade secret misappropriation); Rubenstein, *supra* note 137, at 647 (asserting that Sarbanes-Oxley protects employees reporting violations of securities laws, which excludes trade secret misappropriation).

146. *See* § 806, 116 Stat. at 802 (protecting only employees of companies registered under the Securities and Exchange Act of 1934).

147. RESTATEMENT (THIRD) OF AGENCY § 1.01 (2005).

148. *Id.* at § 1.01 cmt. e (discussing the rights and duties of the agency relationship).

149. *See, e.g.*, *In re* Caremark, 698 A.2d 959, 968 (Del. Ch. 1996) (requiring the board of directors to authorize "significant corporate acts"); *see also* DEL. CODE ANN., tit. 8, 141(a) ("The business and affairs of every corporation organized under this [statute] shall be managed by or under the direction of a board of directors, except as may be otherwise provided in this [statute] or in its certification of incorporation.").

150. *See* Smith v. Van Gorkom, 488 A.2d 858, 872–73, 893 (Del. 1985) (holding that the directors of the defendant corporation breached their duty of care to the corporation by failing to fully investigate before approving a merger), *overruled on other grounds by* Gantler v. Stephens,

judgment rule protects the directors or officers if they act with adequate information, in good faith, and with the subjective belief that their action was in the best interests of the corporation.[151]

The business judgment rule rests on the assumption that managers and directors have "skills, information[,] and judgment not possessed by reviewing courts, and [that] there is great social utility in encouraging the allocation of assets and the evaluation and assumption of economic risk by those with such skill and information."[152] Generally, courts avoid second-guessing legitimate business decisions.[153] Delaware courts, for example, subscribe to the contractarian approach to corporate governance, which allows companies to determine their rights and responsibilities contractually, rather than rely on the legislature to allocate them statutorily.[154]

As a consequence of the contractarian approach, Delaware courts apply the business judgment rule only in cases in which corporate directors act affirmatively; cases in which directors simply fail to act fall outside of the

---

965 A.2d 695, 713 & n. 54 (Del. 2009); *Caremark*, 698 A.2d at 967 (explaining that the business judgment rule is applied to cases involving harmful decisions by the board of directors).

151. Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244, 254 (Del. 2000); *see also Caremark*, 698 A.2d at 967 ("[C]ompliance with a director's duty of care can never appropriately be judicially determined by reference to *the content of the board decision* that leads to a corporate loss, apart from consideration of the good faith or rationality of the process employed.").

152. *In re* J.P. Stevens & Co. S'holders Litig., 542 A.2d 770, 780 (Del. Ch. 1988) (quoting Solash v. Telex Corp., C.A. No. 9518, 1988 WL 3587, at *8 (Del. Ch. Jan. 19, 1988)).

153. *See* Hal R. Arkes & Cindy A. Schipani, *Medical Malpractice v. The Business Judgment Rule: Differences in Hindsight Bias*, 73 OR. L. REV. 587, 587 (1994) (describing the rules in place to prevent "retrospective evaluations" of "negligent business decisions"). Courts are keenly aware of the potential to engage in hindsight bias, or "the tendency for people with knowledge of an outcome to exaggerate the extent to which they believe the outcome could have been predicted." *Id.*

154. Sandra K. Miller, *What Fiduciary Duties Should Apply to the LLC Manager After More than a Decade of Experimentation?*, 32J. CORP. L. 565, 569 (2007) (noting that contractarian states, including Delaware, "expressly defer to the parties' agreement" in resolving corporate disputes). The contractarian approach rests on the perception of the corporation as a collection of contracts or agreements by which the corporation can be governed. *See generally* Frank H. Easterbrook & Daniel R. Fischel, *The Corporate Contract*, 89 COLUM. L. REV. 1416, 1426, 1428 (1989) ("The arrangements among the actors constituting the corporation usually depend on contracts and on positive law, not on corporate law or the status of the corporation as an entity."). *See also* Melvin A. Eisenberg, *The Conception That the Corporation is a Nexus of Contracts, and the Dual Nature of the Firm*, 24 J. CORP. L. 819, 822–23 (1999) (describing the corporation as a "nexus of reciprocal agreements" relied upon to govern the company); Thomas S. Ulen, *The Coasean Firm in Law and Economics*, 18 J. CORP. L. 301, 318–28 (1993) (arguing that corporations use contracts to address both internal and external affairs). Rather than favoring mandatory and uniform public regulation, contractarians favor private market-ordering transactions that allow shareholders and directors to opt in or out of regulations. *See* J. Robert Brown, Jr. & Sandeep Gopalan, *Opting Only In: Contractarians, Waiver of Liability Provisions, and the Race to the Bottom* 42 IND. L. REV. 285, 285-86 (2009).

scope of the business judgment rule.[155] Delaware courts instead evaluate inaction under the duty of loyalty, which requires plaintiffs to specifically plead that the directors or officers of the corporation intentionally acted against—or chose not to act in—the corporation's best interests.[156] Corporate directors or officers are, therefore, free from liability under most state corporate governance laws if they pay only cursory attention to trade secret reporting or management practices, even if they are grossly negligent in their inaction.

b. The Oversight Doctrine and Trade Secret Misappropriation

Corporate governance law related to business processes, such as trade secret management, may also fall under the "oversight doctrine," which has been developed over the years by Delaware courts.[157] The oversight doctrine protects directors and some officers from personal liability unless they breach the duty of loyalty owed to the corporation.[158]

The oversight doctrine stands for the proposition that the duty of loyalty may be breached if a director or officer neglects to impose information and reporting requirements.[159] In *In re Caremark*, the Delaware Court of Chancery explained that "a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system . . . exists and that

155. *Aronson*, 473 A.2d at 813. In practice, although the duty of care liability standard for affirmative decisions is perceived as lax, the Delaware Legislature tempered the standard by amending the Delaware General Corporation Law "to allow for an optional charter provision to exculpate directors for violations of the duty of care." *See* Hillary A. Sale, *Delaware's Good Faith*, 89 CORNELL L. REV. 456, 466 (2004). This amendment allows a corporation to elect whether or not it wishes to immunize corporate directors and officers from *any* duty of care liability whatsoever. *Id.* Many corporations today provide this liability waiver.

156. *See* Stone v. Ritter, 911 A.2d 362, 367 & n.9, 370 (Del. 2006) (requiring the plaintiff to plead specific factual allegations, rather that conclusory, general, or speculative statements). This specificity standard also requires the plaintiff include specific facts that indicate intent, which can be a difficult hurdle to overcome. *Id.*

157. *See* Nadelle Grossman, *The Duty to Think Strategically* 28–29 (Jan. 1, 2012) (Marquette Univ. Law Sch., Working Paper No. 11-19) [hereinafter *Duty to Think Strategically*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1919145. Delaware law has significant influence over general corporate governance law because most public corporations are incorporated in Delaware. Nadelle Grossman, *Director Compliance with Elusive Fiduciary Duties in a Climate of Corporate Governance Reform*, 12 FORDHAM J. CORP. & FIN. L. 393, 397 (2007). Other jurisdictions often look to Delaware law for guidance. *Id.*

158. *See Stone*, 911 A.2d at 370 (holding that a director breaches his duty of loyalty under the oversight doctrine if he *completely* neglects to enact a risk monitoring system, or he enacts a system but consciously fail to monitor it). It remains unclear whether officers are held to the same standard as directors. Although the existing Delaware cases involved actions by both directors and officers, the cases interpreting the oversight doctrine exclusively mention the duties imposed on and breached by directors. *See Duty to Think Strategically*, *supra* note 157, at 32–33.

159. *In re* Caremark, 698 A.2d 970, 970–71 (Del. Ch. 1996).

failure to do so under some circumstances may . . . render a director liable for losses caused by non-compliance with applicable legal standards."[160]

The general reaction following *Caremark* was that directors would face greater liability for deficient oversight of business performance, such as the mismanagement of trade secrets.[161] However, the oversight doctrine was narrowed in subsequent cases, and it became clear that oversight issues would be assessed under the higher duty of loyalty standard. Indeed, in *Stone v. Ritter*, the Delaware Supreme Court refined *Caremark*'s mandate by outlining the evidence required to establish liability in business-oversight cases.[162] *Stone* requires the plaintiff to show that either "(a) the directors utterly failed to implement any reporting or information system or controls; *or* (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[163]

However, in practice, the test articulated in *Stone* offers little chance of recovery. If the company has some type reporting system in place, it is not liable unless the plaintiff satisfies the difficult burden of proving that the director intentionally relinquished his monitoring responsibilities.[164] Consequently, the oversight doctrine often protects the director from liability so long as a control system exists, even if trade secret misappropriation or other harm results from an outdated or inadequate oversight mechanism that falls well behind the industry's best practices.[165] As explained in *Caremark*, director liability based on the duty of oversight "is possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment."[166]

---

160. *Id.*

161. *See, e.g.*, Charles M. Elson & Christopher J. Gyves, In re Caremark*: Good Intentions, Unintended Consequences*, 39 WAKE FOREST L. REV. 691, 691 (2004) (predicting that, following *Caremark*, "boards that fail to establish effective corporate compliance procedures may face substantial liability").

162. 911 A.2d at 370 ("We hold that *Caremark* articulates the necessary conditions predicate for director oversight liability.").

163. *Id.*

164. *See id.* (emphasizing the disjunctive nature of the test articulated in *Caremark*).

165. *See* William W. Bratton, *Lyondell: A Note of Approbation*, 55 N.Y.L. SCH. L. REV., 561, 570–72 (2010) (arguing that Delaware's "lesser rather than [] greater" approach in *Caremark* and *Stone* "slams down the book of best practices" because it requires "knowing and complete failure" to fulfill responsibilities); *see also* Perlroth, *supra* note 105 (arguing that, because there are no legal consequences for negligent monitoring, some companies have "a devil-may-care attitude toward data"). Increasing corporate liability for business-related trade secrets may be appropriate, but considering a change in state corporate fiduciary law is beyond the scope of this Article.

166. *In re* Caremark, 698 A.2d 959, 967 (Del. Ch. 2006).

III. POLICY JUSTIFICATIONS FOR AMENDING THE ECONOMIC ESPIONAGE ACT

The gap in the enforcement of trade secret protection laws, especially in situations of foreign trade secret theft, indicates that the EEA should be amended to increase protection of trade secret information. This could best be accomplished by imposing an affirmative duty of disclosure of trade secret misappropriation that affects national security.[167]

In American jurisprudence, affirmative legal duties are generally an exception to the rule favoring negative duties.[168] It is well accepted that a governmental demand to perform is significantly more burdensome than a command to refrain from harmful action.[169] As a result, the imposition of an affirmative duty requires strong public policy justifications.[170] The public policy justifications for imposing an affirmative duty to disclose trade secret theft are detailed below.

However, it is important to note that American law also recognizes that clearly defining the scope of an affirmative duty to perform minimizes the governmental intrusion.[171] Here, the duty is clearly defined as a duty to report a trade secret theft if the theft applies to any technology that affects national security.[172] This requirement would not impose an obligation to prevent the theft, or correct the harm arising from the theft. Rather, the duty is simply to disclose the theft to an enforcement agency, which would then decide whether to pursue the matter if it involves a state-sponsored attack, a threat to national security, or if it would be useful to intelligence-gathering agencies.

A. Protection of the Public Interest

An affirmative duty to act must be justified by a significant public interest.[173] In the case of trade secret misappropriation, the significant public interest is the substantial value of information and the impact of the theft of that information on public welfare and national security.

Many state governments have recognized the public interest in information security and have imposed affirmative disclosure duties in analogous cases of information theft. For example, several states require companies to disclose

---

167. *See infra* Part IV (proposing the text of the amendment and discussing its provisions and the benefits of imposing an affirmative duty to disclose).

168. Paul H. Robinson, *Criminal Liability for Omissions: A Brief Summary and Critique of the Law in the United States*, 29 N.Y.L. SCH. L. REV., 101, 104 (1984) (describing the "general reluctance in the United States to impose affirmative duties").

169. *Id.*

170. *Id.* (arguing that an affirmative duty must be both justified by strong public policy benefits and "imposed in a way that minimizes the extent of the intrusion").

171. *Cf. id.* (noting that the rule against affirmative duties is based, in part, on the difficulty of defining the scope of the duty, which makes the duty difficult to enforce).

172. *See infra* Part V (providing the text of the proposed amendment).

173. Robinson, *supra* note 168, at 104–05 (explaining that the public interest, including the health and safety of the public, can justify an affirmative duty).

breaches of data security.[174] California was the first state to enact such a disclosure requirement with the Security Breach Notification Act.[175] Other states followed suit and enacted similar legislation, and now forty-six states impose notification requirements.[176] This trend suggests that more, if not all, states will adopt such legislation in the future.

Similarly, several members of Congress recently proposed the Cybersecurity Act of 2012, which was written to protect critical domestic infrastructure from cyber warfare attacks.[177] Had Congress passed the Act, it would have imposed an affirmative duty on companies that control critical infrastructure to report any "significant cyber incidents affecting critical cyber infrastructure."[178]

Additionally, some corporate governance laws impose an affirmative duty on managers in situations in which nondisclosure of information would cause significant harm to the corporation.[179] For example, the Sarbanes-Oxley Act requires the Chief Executive Officer (CEO) of an organization to certify the correctness of financial statements and that the company has promulgated adequate internal controls.[180] Likewise, the Securities and Exchange Commission (SEC) requires directors to take affirmative steps to ensure that the corporation's communications with the public are truthful.[181]

---

174. *See* Andrew B. Serwin, *Poised on the Precipice: A Critical Examination of Privacy Litigation*, 25 SANTA CLARA COMP. & HIGH TECH. L.J. 883, 884 (2009) (detailing the states that have enacted security breach laws that "mandate public disclosure of data incidents").

175. *Id.* The statute requires

> [a]ny person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

CAL. CIV. CODE § 1798.82(a) (West 2009 & Supp. 2013).

176. Serwin, *supra* note 174.

177. Cybersecurity Act of 2012, S.3414, 112th Cong. (2012). The Act was originally introduced as S.2105, but the Senate voted on the version of the Act introduced as S.3414. 158 CONG. REC. S.5919 (daily ed. Aug. 2, 2012). The Act ultimately failed a vote of cloture and was not passed. *Id.*; *see supra* note 13 and accompanying text (detailing the progression of the Act and its reintroduction in 2013).

178. Cybersecurity Act of 2012, S.3414, 112th Cong. § 102(b)(4) (2012). "Critical cyber infrastructure" includes infrastructures that affect life-sustaining services and the U.S. economy. S.3414, § 102(b)(3)(B).

179. *See Duty to Think Strategically*, *supra* note 157, at 27 (explaining that the duties of loyalty and care require affirmative actions by directors of corporations).

180. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 906, 116 Stat. 745, 806 (codified at 18 U.S.C. § 1350 (2006)).

181. Conduct of Certain Former Officers and Directors of W.R. Grace & Co., Exchange Act Release No. 34,39157, [1997 Transfer Binder] Fed. Sec. L. Rep. (CCH) ¶ 85,963, at 89,893 (Sept.

B. Protection of Critical Technologies with a Unified National Policy

Adding a disclosure requirement to the EEA would also be consistent with the policy goals of export control laws. Export control laws are aimed at regulating the export of tangible goods to prevent the use of those goods in a manner that may harm national interests.[182] From a policy perspective, however, the laws' emphasis on actual goods fails to ensure the protection of the underlying technology involved in creating the goods, allowing for recreation of the goods through reverse engineering.[183]

Policymakers are increasingly recognizing the eroding distinction between goods and the underlying technology used to create them, viewing the nation's infrastructure as a combination of tangible and intangible components.[184] Accordingly, because of the increasing technological competence and sophistication of foreign states and organizations,[185] export control laws should regulate not only actual goods, but also the technology behind these goods. This can be accomplished by amending the EEA. Requiring disclosure of the misappropriation of trade secret information will help to increase protection of the intellectual property associated with the manufacturing of some exported goods.

C. Expansion of Protection for Explicit Knowledge

The importance of explicit knowledge to the modern economy provides additional justification for amending the EEA to address trade secret misappropriation. The rapid evolution toward a knowledge-based economy has had a significant impact on business, society, and national competitiveness.[186] One of the key challenges in this environment is to

---

30, 1997) (asserting that an officer or director of a public company has "substantial obligations" and that "[i]f an officer or director knows or should know that his or her company's statements concerning particular issues are inadequate or incomplete, he or she has an obligation to correct that failure").

182. *See, e.g.*, Export Administration Act of 1979, Pub. L. No. 96-72, § 3(2), 93 Stat. 503, 504 (codified at 50 U.S.C. App. § 2402 (2006)) (controlling the export of goods that "would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States").

183. Reverse engineering is an accepted form of recreating the item in question without misappropriating the information underlying its creation. Ulrich, *supra* note 68, at 156–57 (noting that reverse engineering is "implicitly accepted" by trade secret law).

184. *See* NAT'L COUNTERINTELLIGENCE EXECUTIVE, NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA 4 (2007) [hereinafter NCIX STRATEGY], *available at* http://www.fas.org/irp/ops/ci/cistrategy2007.pdf ("In collaboration with our colleagues throughout the government, the counterintelligence community will protect our vital national assets—critical infrastructure, sensitive technologies, key resources, networks, and knowledge—from intelligence-related attack.").

185. ONCIX REPORT, *supra* note 3, at 1, 5–6 (describing the sophisticated techniques foreign actors use to misappropriate sensitive information).

186. *See* ADMINISTRATIVE STRATEGY, *supra* note 1, at 1–2 (describing intangible assets and intellectual property as "the innovation that drives the American economy and supports jobs in

incentivize innovation, which is accomplished by protecting knowledge-based assets that are non-rivalrous and non-excludable.[187] Accordingly, the legal system has evolved to provide some measure of security and efficiency in the marketplace of ideas.[188] Enforcement costs and ease of replication, however, pose significant challenges to innovators who wish to protect their intellectual property.[189] The problem is compounded when business is conducted overseas in jurisdictions that do not adequately protect knowledge.[190]

Trade secrets are especially vulnerable to this type of knowledge theft because companies routinely memorialize information. In its tacit form, knowledge is difficult to perceive and replicate.[191] The information used to develop important technologies, therefore, is often made explicit to extract its full value.[192] However, when knowledge is made explicit and recorded, it is substantially easier to misappropriate the information.[193] The codification of trade secret information creates an exact blueprint for replication and, if the information is misappropriated, the technology can easily be "reverse -engineered."[194]

Lastly, the process of creating a technology is often a key ingredient to using the technology. For example, a manufacturing process may be the main source

---

the United States" and noting that this information affects American businesses and the economy, national security, and economic competitiveness); SHAPIRO & VARIAN, *supra* note 101, at 4 (discussing the value of information).

187. SHAPIRO & VARIAN, *supra* note 101, at 4 (arguing that owners of intellectual property are unable to recover the high production cost of information without the enforcement of their intellectual property rights).

188. *See, e.g.*, 17 U.S.C. § 501 (2006) (prohibiting the infringement of copyrights); 18 U.S.C. 1831–32 (2006) (protecting trade secrets from misappropriation); 35 U.S.C. 271 (2006 & Supp. 2012) (prohibiting the infringement of patents).

189. SHAPIRO & VARIAN, *supra* note 101, at 3–4 (noting that intellectual property rights do not "confer complete power to control information" because the ability to copy and instantly send information around the world has made enforcement difficult).

190. *See, e.g.*, Bai & Da, *supra* note 116, at 362–63 (stating that, even though China has implemented many laws and regulations to protect trade secrets, significant challenges exist due to technical and procedural aspects of the Chinese legal system).

191. *See* IKUJIRO NONAKA & HIROTAKA TAKEUCHI, THE KNOWLEDGE-CREATING COMPANY: HOW JAPANESE COMPANIES CREATE THE DYNAMICS OF INFORMATION 8 (1995) (explaining that tacit knowledge, in part, consists of "hard-to-pin-down skills or crafts captured in the term 'know-how'").

192. *Id.* ("Explicit knowledge can be expressed in words and numbers, and easily communicated and shared in the form of hard data, scientific formulae, codified procedures, or universal principles.").

193. *Id.* at 8–9. Conversely, tacit knowledge is internalized and cannot be easily transmitted through formula or code. *Id.*

194. For example, some codified technologies such as software are copied or reverse engineered when the source code is misappropriated. *See* Markoff *supra* note 4, at A1 (predicting that the theft of Google's software system will provide the hackers with the information needed to replicate—"reverse engineer"—Google's system).

of competitive advantage for innovative manufacturing firms.[195] If the process is tacit, it can be very difficult to replicate.[196] Companies, however, often seek to record processes and business methods to increase the store of knowledge within the company.[197] Often, this methodology is classified as a trade secret.[198] Consequently, the misappropriation of a process-based technology may completely undermine the company's competitive advantage.[199]

IV. AMENDING THE ECONOMIC ESPIONAGE ACT TO REQUIRE DISCLOSURE OF TRADE SECRET MISAPPROPRIATION IN CASES INVOLVING NATIONAL SECURITY

The EEA should be amended to require disclosure of suspected outbound trade secret theft. The amendment would read as follows:

> No person with reasonable knowledge that a violation of this Act has been or is being committed with respect to technologies that are subject to export regulations shall fail to report such information to a federal law enforcement agency.
>
> Whoever violates this section shall be fined not more than $_____ or imprisoned more than _____ years, or both.

The proposed amendment would both serve the policy goals explained above and encourage better data security to protect trade secret information and, as a consequence, national security.

The technologies affected by the amendment are those that qualify as trade secrets under the EEA.[200] The technologies and products that are regulated by export laws but that are not considered trade secrets by the EEA are excluded by the amendment. Technologies that both qualify as trade secrets under the EEA and are subject to export control, however, are covered by the amendment.

Although some whistleblower laws require *actual* knowledge of a violation,[201] the proposed amendment imposes a lesser mens rea standard by

---

195. *See* TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 1324–25 (Fed. Cir. 2011); David Orozco, *Administrative Patent Levers*, 117 PENN. ST. L. REV. 1, 8–9 (2012) (noting that business methodology and "fundamental business techniques" are important economic resources).

196. *See* NONAKA & TAKEUCHI, *supra* note 191, at 8–9 (explaining that tact knowledge is internal and not easily disseminated).

197. *See* Orozco, *supra* note 195, at 8–14 (explaining that some business methods can be converted into explicit knowledge, which takes the form of a utility patent).

198. *See, e.g.*, *TianRui Grp. Co.*, 661 F.3d at 1325 (classifying a manufacturing process as a trade secret).

199. *See id.* (emphasizing the need for a remedy for the misappropriation of a business process).

200. *See* 18 U.S.C. § 1839(3) (2006).

201. *See, e.g.*, N.Y. LAB. LAW § 740(2)(a) (McKinney 2002 & Supp. 2013) (prohibiting retaliatory action against an employee where the employee discloses or threatens to disclose a practice that "*is* in violation of law" (emphasis added)).

requiring reasonable knowledge of a violation. Several data security breach and whistleblower statutes impose a similar reasonable knowledge standard.[202] A reasonable knowledge requirement is appropriate because although trade secret misappropriation can be difficult to ascertain due to the thieves' efforts to conceal the activity,[203] there are still indicators that signal trade secret theft. For example, a company's IT department may have knowledge of a data breach that would lead a reasonable person to conclude that trade secrets were accessed or obtained.

The proposed amendment also imposes a substantial penalty on any individual who fails to report a suspected trade secret theft. As with many other white collar offenses, prosecutors may evaluate the defendant's level of culpability and conclude that imposing a fine is more appropriate than criminal penalties.[204] Likewise, judges may rely on the organizational sentencing guidelines to impose the most effective fine.

Prosecutors may also reach a settlement agreement that defers or avoids criminal prosecution if the defendant agrees to institute a compliance program.[205] Such compliance programs typically encompass: (1) a written policy related to the legal issue distributed throughout the company; (2) employee training; (3) improved recordkeeping; (4) compliance certification at all organizational levels; (5) internal audits and, sometimes, external monitoring; (6) improved screening of third party agents; and (7) a mechanism for rapid and thorough investigation if the defendant suspects a violation.[206]

The proposed amendment imposes an affirmative duty to report suspected theft to federal enforcement authorities rather than to a superior within the organization. This avoids the harm that might occur if the organization fails to take action. Requiring a party to report the theft directly to a public

---

202. *See, e.g.*, 18 U.S.C. § 1514A(a)(1) (2006 & Supp. 2012) (prohibiting retaliation of an employee who reports violation of securities laws); CAL. CIV. CODE § 1798.82(a) (West 2009 & Supp. 2013) (requiring disclosure if an individual reasonably believes that a data breach has occurred); N.H. REV. STAT. ANN. § 275-E:2 (2008) (prohibiting retaliation against an employee who "has reasonable cause to believe" that the employer has violated the law); *see also* Passaic Valley Sewerage Comm'rs v. Dep't of Labor, 992 F.2d 474, 474–75 (3d Cir. 1993) (considering whether an employee's allegations against his employer were reasonable under the Clean Water Act, which would provide him immunity from retaliation).

203. *See* Rustad, *supra* note 9, at 481–82 (highlighting the measures taken by computer hackers to preserve anonymity, including "false email headers, offshore sites, and anonymous e-mailers").

204. *Cf.* 15 U.S.C. § 78dd-2(a), (g) (2006) (basing the defendant's penalty on his level of culpability).

205. Virginia G. Maurer & Ralph E. Maurer, Rethinking Compliance Settlements and the Foreign Corrupt Practices Act (2012) (unpublished paper) (on file with author) (discussing the prevalence of DOJ settlements in relation to the Foreign Corrupt Practices Act).

206. *Id.*

enforcement agency such as the FBI[207] will help to alleviate the problems caused by companies failing to report suspected trade secret theft.[208]

The proposed amendment also protects whistleblowers who comply with the statute's disclosure requirement from retaliation by their employers. Likewise, if an individual within an organization has knowledge that another individual within the organization has violated the amendment by failing to report a suspected trade secret theft, he may alert law enforcement with immunity from retaliation by the organization. Immunity under the amendment is afforded by the existing federal obstruction of justice statute, which states that:

> Whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than 10 years, or both.[209]

The proposed amendment will also improve data security practice among organizations that develop the affected technologies. Most companies go to great lengths to avoid prosecuting trade secret thefts because of the burdens imposed by the EEA.[210] The proposed amendment provides government enforcement and prosecuting agencies with the opportunity to prosecute previously unreported theft, which in turn will help to improve data security. Increased prosecution of the EEA will signal that lax security practices will likely lead to sanctions under the amendment.[211] To avoid the difficulties associated with prosecuting trade secret theft under the EEA, companies will be more willing to increase security to avoid reporting suspected trade secret theft in the first place.

---

207. Counterintelligence efforts to protect U.S. economic interests are the FBI's second priority, after terrorism. *Counterintelligence: Economic Espionage*, FEDERAL BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage (last visited Sept. 8, 2013). To achieve this high priority, the FBI has a dedicated Economic Espionage Unit. *Id.*

208. *See supra* Part II and accompanying text (discussing the under-enforcement of trade secret laws).

209. 18 U.S.C. 1513(e) (2006 & Supp. 2011).

210. *See supra* notes 106–109 and accompanying text (detailing the difficulties in litigating a claim under the EEA).

211. Given the close nexus between employment, American competitiveness and trade secrets, the political climate has been receptive to greater trade secret enforcement actions. *See, e.g.*, Press Release, Department of Justice, Department of Justice Joins in Launch of Administration's Strategic Plan on Intellectual Property Enforcement as Part of Ongoing IP Initiative (June 22, 2010), *available at* http://www.justice.gov/opa/pr/2010/June/10-ag-722.html. (reporting that the DOJ has increased efforts and resources to prosecute trade secret cases in response to the Obama Administration's first-ever Joint Strategic Plan on Intellectual Property Enforcement, which resulted in a new DOJ Task Force on Intellectual Property).

In sum, organizations would have an additional and powerful incentive to create programs to encourage compliance with the amendment's reporting requirement.[212] Entities that develop technologies relevant to national security would implement more robust network security programs and better human resource practices in order to safeguard trade secrets and avoid the penalties for failing to report a breach. Additionally, under the federal sentencing guidelines, an organization may implement a compliance program that bolsters data security as part of a settlement agreement with the Department of Justice.[213]

V. CONCLUSION

Trade secret law protects the owner of valuable knowledge from misappropriation of the information by third parties. The current legal regime is largely designed to protect trade secrets from theft by domestic actors. As a consequence, the current regime fails to protect many trade secrets that are stolen by foreign state-sponsored entities. This problem is compounded when the misappropriated trade secrets involve technologies that affect national security.

Amending the EEA to mandate disclosure of suspected trade secret thefts related to any technology that is subject to export restriction would help to protect information relevant to national security. Mandated disclosure would help to address the underreporting of foreign trade secret theft, which impedes the EEA's goal of deterrence; inspire better trade secret management practices; protect whistleblowers from retaliation by their employers retaliation; and encourage cooperation between companies that develop sensitive technologies and federal law enforcement agencies, which is necessary to safeguard the nation's critical infrastructure and knowledge-based assets.

212. A firm's audit committee and compliance director would appropriately oversee compliance with this amendment.

213. Maurer & Maurer, *supra* note 205.