TULANE JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY

VOLUME 16 FALL 2013

Economic Espionage and Theft of Trade Secrets: The Case for a Federal Cause of Action

Kelley Clements Keller*
Brian M.Z. Reece†

* Kelley Clements Keller, Esq., is the Founder & Managing Member of the Keller Law Firm, LLC, located in Carlisle, Pennsylvania (Harrisburg Metro Area). Her practice focuses on a broad range of domestic and international intellectual property matters and includes representing clients across a broad spectrum of industries, including banking and payments technologies, electronics, supermarkets, manufacturing, pharmaceuticals, telecommunications, and entertainment.

† Brian M.Z. Reece, M.A., is the Lead Research Assistant for the Keller Law Firm, LLC, located in Carlisle, Pennsylvania (Harrisburg Metro Area). He conducts research on cutting-edge legal issues facing companies in the digital economy and tracks recent legislative developments on intellectual property and related legal matters.

> Our weapons have grown more sophisticated. [Now, we use] a new one: Economics.[1]
>
> [I]f this [economy] isn't a national security matter, then what is it![2]

I. INTRODUCTION

The United States Congress formally acknowledged the existence of an extraordinary network of economic spies stealing America's technological treasures when it passed the Economic Espionage Act of 1996 (EEA). With the EEA, Congress finally criminalized economic espionage and theft of trade secrets, effectively clearing a path to bring federal resources against these spies and empowering the United States Department of Justice to work with American companies and organizations to protect the U.S. economy against this economic offensive.

The economic spy is dangerously different from the traditional Cold War agent. Rather than plundering military strategies or war plans, his booty is other people's ideas, the secret intellectual "crown jewels" of U.S. corporations, research laboratories, and other targeted organizations.

---

1. BATMAN BEGINS (Warner Bros. Pictures 2005).
2. JOHN J. FIALKA, WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA 7 (1997) (quoting Stansfield Turner).

However, once these ideas are stolen and sent back home for commercial or military exploitation, the damage to the U.S. entity from their theft can reach into the billions of dollars.[3] Given the economic stakes, it is imperative that corporate America receive the federal investigative, legal, and judicial resources necessary to protect itself and its proprietary economic information from the guile of these spies.[4] Enacting the EEA was a very important step in this process.

Traditionally, the United States has been a world leader in providing legal protection for intellectual property assets.[5] Sophisticated patent, trademark, and copyright laws have been on the books for decades.[6] Conspicuously absent, however, were laws to protect embryonic technology and proprietary economic information. Because the impact on the American economy from losing embryonic technology was so severe, Congress responded by criminalizing its theft through the EEA. Interestingly, though, unlike with statutory schemes that address other intellectual property crimes, Congress did not create a companion federal cause of action for victims to pursue expedited and comprehensive civil relief for theft of their proprietary economic information or trade secrets.

This Article presents the case for Congress to reconsider the issues of economic espionage and theft of trade secrets and to enact a companion federal cause of action under the EEA. Broadening the reach of the law to include federal civil remedies would provide private litigants with the ability to pursue injunctive relief and economic compensation at the national level. It is in the nation's best economic interest to have its corporations and other research and development entities create, invent, and bring new ideas and products to market, rather than lose them surreptitiously to competitors. To make this case, Part II will explain the importance of the indissoluble link between protection of

---

3. *Id.* at 6 (citing *The Threat of Foreign Economic Espionage to U.S. Corporations: Hearings Before the Subcomm. on Econ. & Comm. Law of the Comm. on the Judiciary*, 102d Cong. 130 (1992) [hereinafter *Foreign Economic Espionage Hearings*]).

4. By the year 2000, intellectual property theft had cost American companies in excess of $1 trillion. *Protecting American Interests Abroad: U.S. Citizens, Businesses and Nongovernmental Organizations: Hearing Before the Subcomm. on Nat'l Sec., Veterans Affairs & Int'l Relations of the Comm. on Gov't Reform*, 107th Cong. 92 (2001) [hereinafter *American Interests Abroad Hearings*] (testimony of Frank J. Cilluffo).

5. The Founders provided for protection of intellectual property rights in the United States Constitution. U.S. CONST. art. I, § 8, cl. 8. Federal patent laws have existed in the United States since the Patent Act of 1790. Patent Act of 1790, ch. 7, 1 Stat. 109-112 (1790), *available at* http://www.ipmall.info/hosted_resources/lipa/patents/Patent_Act_of_1790.pdf.

6. The modern patent law, the Patent Act of 1952, is codified at 35 U.S.C. §§ 100-376 (2006); the Lanham Act, the modern trademark law passed in 1946, is codified at 15 U.S.C. §§ 1125-1141 (2012); the Copyright Act of 1976, the modern copyright law, is codified at 17 U.S.C. §§ 101-810 (2012).

U.S. intellectual property assets and economic and national security. Part III will examine the historical significance of the EEA in relation to the first federal law that dealt with trade-secrets theft, the Trade Secrets Act of 1948. Additionally, Part III will analyze the EEA's component parts along with its legislative history, giving the reader a more in-depth understanding of the EEA, and will also examine two recent updates passed by the 112th Congress and signed into law. Part IV will scrutinize the efficacy of the EEA in prosecuting economic espionage and posit the merits of creating a private federal cause of action for theft of trade secrets. Part V will make the case for why the EEA should be amended to include a federal cause of action to protect national security. Part V will also discuss the Protecting American Trade Secrets and Innovation Act of 2012 (PATSIA), the recently proposed legislation that, had it been passed, would have created the much-needed civil counterpart to the EEA.

II. THE INEXTRICABLE LINK BETWEEN PROTECTION OF U.S. INTELLECTUAL PROPERTY ASSETS AND NATIONAL AND ECONOMIC SECURITY

From its founding, the United States has recognized the importance of creating and protecting intellectual property rights. Protecting intellectual creativity was understood as a means of fostering national economic security. The Patent Act of 1790 placed the Patent Office under the joint control of the United States Departments of War and State, and the United States Office of the Attorney General.[7] Even before guaranteeing the right to the freedom of speech, the United States Constitution guaranteed authors and inventors the right to profit from their artistic, scientific, and technological creations.[8] Securing this right immediately upon establishing the new republic demonstrates the Founders' foresight. They anticipated what a fledgling America would need to accumulate wealth and grow into a robust, powerful, and enduring nation.

---

7. *Records of the Patent and Trademark Office (Record Group 241)*, U.S. NAT'L ARCHIVES & RECORDS ADMIN., http://www.archives.gov/research/guide-fed-records/groups/241.html (last visited May 23, 2013).

8. "The Congress shall have the power to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries". U.S. CONST. art. I, § 8, cl. 8. This is the only "right" enumerated in the body of the Constitution itself. All other individual rights are detailed in the Bill of Rights and subsequent constitutional amendments. *Id.* amends. I—XXVII.

It is perhaps an economic axiom that there are truly only four ways a nation grows rich.[9] First, a nation may achieve economic growth by bringing the inventions and innovations of its people to market.[10] Second, a nation may exploit cheap labor to increase profit margins from the sale of products produced by that labor.[11] Third, a nation may depend on its plentiful natural resources as a valuable commodity in international markets.[12] Finally, "logic suggests that a nation may steal any one of the above and, thereby, achieve economic prosperity for a time."[13]

Experts suggest, however, that a nation cannot prosper over long periods of time in our modern economy by relying on cheap labor and natural resources alone.[14] These resources must be combined with "a strategy of innovation and invention."[15] In fact, "whether a nation chooses to buy, develop, or otherwise acquire new technology by theft or espionage, all nations must obtain new technology."[16] In the modern economy of fast-paced innovation and complex high technologies, there is stiff competition to be a market leader for consumer products. For many nations, stealing is faster and easier than innovation and, if unchecked, extremely profitable.

Conversely, a nation that chooses to obtain new technologies by investing richly in research and development must ensure recovery of its investment by exploiting and protecting the new technologies at market.[17] These technologies cannot be used to achieve this goal, however, until they have been productized, or rendered in a novel, tangible form that can be patented. It is precisely during the product development phase, the time between the conception of the new idea and the actual creation of

---

9. James P. Chandler, *The Loss of New Technology to Foreign Competitors: U.S. Companies Must Search for Protective Solutions*, 27 GEO. WASH. J. INT'L L. & ECON. 305, 305 (1994).

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.*

14.

> [L]ong-term economic expansion and technological expansion go together, in that neither has occurred for very long without the other. But although technological and economic expansion are interwoven and inseparable, no simple law of nature makes technology the cause of economic growth or growth the cause of technological advance. . . . The interplay of people, economic institutions, growing markets and technology is the key.

Nathan Rosenberg & L.E. Birdzell, Jr., *Science, Technology and the Western Miracle*, SCI. AM., Nov. 1990, at 54, 54.

15. Chandler, *supra* note 9, at 305.

16. *Id.*

17. *Id.* at 306.

the new technology (or the embryonic stage), that the economic investment is most vulnerable and susceptible to theft. The future product or patented technology, while still in its embryonic form, does not receive protection under traditional U.S. intellectual property laws, specifically patent, copyright, and trademark laws.[18] Exposed, embryonic technology is "a prime target for theft precisely because it costs so *much* to develop independently, because it is so valuable, and because there are virtually no penalties for its theft."[19] To safeguard these ideas, their owners must guard them as trade secrets, or confidential and proprietary information that derives independent economic value as a result of being kept secret.[20] Protecting these economic secrets is indispensable to the successful creation of new technologies that, once productized, will help the nation recover and profit from its investment. These enormous expenditures, however, "can easily come to nothing . . . if a competitor can simply steal the trade secret without expending the development costs."[21] The competitor may then be able to offer competing products at a reduced price.[22] The result: over time, the true inventor's desire to continue innovation erodes, the research and development investment is not recovered, jobs disappear, and the wisdom of continued capital

---

18. 35 U.S.C. § 100-376 (2006); 15 U.S.C. §§ 1051-1141 (2012); 17 U.S.C. §§ 101-810 (2012).

19. H.R. REP. No. 104-788, at 5 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023 (emphasis added).

20. The EEA defines "trade-secrets" as

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

Economic Espionage Act, 18 U.S.C. § 1839(3) (2012).

21. *See* 142 CONG. REC. S12,207-08 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

22. "Without control of access to the new technology, there is a high risk that capital invested in the innovation will not be recovered and become profitable before others, who do not have to replicate the original development investment, copy the product and become competitors." James P. Chandler, *Protection of U.S. Competitiveness in the International Software Markets: Reexamining the Question of Copyrighting Government-Created Software*, 25 GEO. WASH. J. INT'L L. & ECON. 387, 395 (1991) (citing *Technology Transfer: Hearings Before the Subcomm. on Sci., Research & Tech. of the House Comm. on Sci. & Tech.*, 99th Cong. 21 (1985) (testimony of Dr. D. Bruce Merrifield, Assistant Sec'y for Productivity, Tech., & Innovation, Dep't of Commerce)).

investment in research initiatives is questioned.[23] Indeed, the loss of this proprietary economic information has the "overarching effect of eroding the future of United States competitiveness and trade, thereby undermining the U.S. economy."[24] The systematic unremunerated transfer of U.S. intellectual property assets to foreign economic competitors could precipitate an erosion of U.S. competitiveness "to the point of economic dependence on a foreign power, [thus causing] the national security and freedom of the United States [to] become impaired."[25]

III. THE ECONOMIC ESPIONAGE ACT OF 1996 AND THE NEED FOR LEGISLATIVE REFORM

There is an undeniable national interest in protecting the nation's economic assets. The EEA's legislative history unwaveringly states that "development of proprietary economic information is an integral part of America's economic well-being. Moreover, the nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interests are threats to the nation's vital security interests."[26] Without the force of law and access to the federal government's investigative and prosecutorial resources to help thwart and punish acts of espionage, our corporations are extraordinarily vulnerable targets.

The threats, foreign and domestic, against private companies' proprietary economic information present a host of problems for victims of trade-secret theft.[27] Before the EEA, their only form of redress was filing a civil lawsuit in state court or seeking relief under state criminal trade secret laws. State civil laws rarely provided adequate remedies, and given modern technological advancements, local law enforcement lacked the investigative resources and requisite legal tools to prosecute this type of crime.[28] Further, federal law failed to provide an effective remedy against foreign economic espionage.[29]

---

23. Inventors are rewarded for their creativity by an intellectual property system. The public credit and remuneration they receive stimulates them to continue inventing. An intellectual property system is "a meritorious method of keeping score." *Id.* at 403 n.86.

24. Chandler, *supra* note 22, at 387-88.

25. *Id.* at 402.

26. H.R. REP. NO. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022-23.

27. *American Interests Abroad Hearings*, *supra* note 4.

28. James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 178 (1997).

29. *Id.*

In a letter to Senator Orrin Hatch, then-Chairman of the Senate Committee on the Judiciary, former Attorney General Janet Reno wrote: "The need for this law cannot be understated as it will close significant gaps in federal law, thereby protecting proprietary economic information and the health and competitiveness of the American economy."[30] Continuing in the tradition of the Founders to protect American innovation and the nation's economic competitiveness, Congress heeded the call of American industry and passed the EEA. President Clinton signed it into law on October 11, 1996.

A. History of the EEA of 1996

Until Congress enacted the EEA, the Trade Secrets Act had been the only federal statute that directly addressed the misappropriation of trade secrets.[31] Regrettably, the Trade Secrets Act only provided misdemeanor sanctions for unauthorized disclosure of confidential information by government employees.[32] Absent a law on point, federal prosecutors were forced to work with alternative statutes that were not designed to penalize trade secret theft. These included the Interstate Transportation of Stolen Property Act (ITSP),[33] the Mail Fraud[34] and Wire Fraud[35] statutes, and the Racketeer Influenced and Corrupt Organizations Act (RICO).[36] However, due to the inapplicability of the ITSP to the theft of intangible property,[37] the ineffective application of the Mail Fraud and Wire Fraud statutes for crimes that do not involve the use of mail or wire, and the fact that most trade secret thefts do not permanently deprive the

---

30. 142 CONG. REC. S12,214 (daily ed. Oct. 2, 1996) (citing Letter from Att'y Gen. Janet Reno to Senate Judiciary Committee Chairman Orrin Hatch (Oct. 1, 1996)).

31. Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (2012).

32. Disclosure of Confidential Information, 18 U.S.C. § 1905. There is only one reported decision under this statute. In *United States v. Wallington*, the court sustained defendant's conviction for running unauthorized background checks. 889 F.2d 573, 580 (5th Cir. 1989). Because the statute only provides misdemeanor sanctions, it is rarely used to prosecute unauthorized disclosures of trade secrets. Pooley et al., *supra* note 28, at 189.

33. Interstate Transportation of Stolen Property Act, 18 U.S.C. §§ 2314-2315. This was the principal alternative statute upon which prosecutors relied. *See* H.R. REP. No. 104-788, at 6 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4025.

34. 18 U.S.C. § 1341.

35. *Id.*

36. Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968. For a helpful summary of alternative charges, see Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, U.S. ATTORNEYS' BULL., Nov. 2009, at 2, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf. The Computer Fraud and Abuse Act, most recently updated in 2008, has been a very helpful alternative in recent years. Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4).

37. United States v. Brown, 925 F.2d 1301, 1307-09 (10th Cir. 1991).

rightful owner of the misappropriated information,[38] there were few prosecutions, and even fewer that were successful.[39] Additionally, only a handful of states had enacted criminal trade secret laws, and there remained a lack of uniform standards for prosecuting such theft from state to state.[40]

To complicate matters, the number of foreign nations (and their corporations) seeking to acquire new technology through acts of theft and espionage, rather than through capital investment in research and development, was disturbingly large.[41] At the time the EEA was being debated in Congress, the Federal Bureau of Investigation (FBI) estimated that nearly two-dozen foreign governments were targeting U.S. trade secrets.[42] Since the end of the Cold War, "foreign nations ha[d] increasingly put their espionage resources to work trying to steal American economic secrets."[43] Espionage, or an "organized effort by one country's government to obtain the vital national security secrets of another country," was traditionally directed toward military secrets.[44] But the focus of the traditional military spy apparatus had changed in response to the increased importance of economic superiority alongside military superiority.[45] This new type of conduct ranged from foreign government-sponsored acts of stealing secrets from another country's corporations (economic espionage) to disgruntled employees misappropriating certain scientific or other proprietary business data from a former employer (theft of proprietary information or theft of trade secrets).[46] Whoever the actor, the implications of this focal shift to the industrial base were significant.[47] American corporations were ill-equipped to combat acts of espionage. They lacked the requisite

38. Many trade secret thefts involve misappropriation by copying information for ill-gotten gain. The rightful owner retains the original, but has lost exclusive control over the data.

39. Pooley et al., *supra* note 28, at 179-80.

40. *Id.* at 186.

41. *Economic Espionage: Hearing Before the Select Comm. on Intelligence and the Subcomm. on Terrorism, Tech., & Gov't Info. of the H. Comm. on the Judiciary*, 104th Cong. 7 (1996) (statement of Louis J. Freeh, Dir., Fed. Bureau of Investigation).

42. Pooley et al., *supra* note 28, at 178-79 (citing Douglas Pasternak & Gordon Witkin, *The Lure of the Steal: America's Allies Are Grabbing U.S. Technology, Washington Is Worried*, U.S. NEWS & WORLD REP., Mar. 4, 1996, at 45).

43. "Estimates of the loss to U.S. business from the theft of intangible intellectual property exceed $100 billion. The loss in U.S. jobs is incalculable." 142 CONG. REC. S12,208 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

44. H.R. REP. No. 104-788, at 5 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023-24.

45. *Id.*

46. This Article does not address theft of proprietary economic information from U.S. national laboratories, whether government-owned, government-operated or government-owned, contractor-operated. *See id.*

47. *See id.*

expertise, investigative and legal tools, and financial and human resources to counter the attacks.[48] Unfortunately, by falling victim to acts of espionage and trade secret theft, these companies contributed with their economic losses to the weakening of the country's economic security. The need for a legislative response was overwhelmingly clear.

In the early 1980s, Congress held hearings on economic competitiveness in response to the massive economic losses the nation's businesses were suffering due to piracy and other misappropriation of U.S. intellectual property assets.[49] As part of those hearings, Ian M. Ross, then-President of AT&T Bell Laboratories, testified regarding the necessity of stronger and more effective laws to adequately protect innovations, especially those coming out of the private sector.

> [G]iven the importance of technological innovation, it is not enough to simply nurture creativity and even apply it effectively. We must safeguard our innovations through the adequate protection of intellectual property rights at home and abroad. Such protection encourages new product and process development in both *high-technology* and basic industries.
>
> To an alarming degree, intellectual property rights have already begun to erode. This is a result of problems that include inadequate or nonexistent patent protection, rampant commercial counterfeiting, copyright and design infringements, and improper use of the Freedom of Information Act. Increasingly, American firms are being denied the benefits of their own inventions.
>
> As intellectual property and innovation have become ever more complex and varied, our U.S. system often responds too slowly to the newest ideas and greatest advances in knowledge, such as biotechnology and semiconductor chips. We must not only rethink our entire body of intellectual property law, but move quickly and immediately to improve the present system to afford full protection to all forms of intellectual property.[50]

A decade later, having failed to act on Mr. Ross's warning, Congress once again convened hearings to study economic competitiveness.[51] American companies are often coy about their losses from thefts of their proprietary information, their intellectual crown jewels, if you will; nonetheless, International Business Machines (IBM) testified in 1992 that their losses from economic espionage and trade

---

48. *See id.*

49. *New Technologies on Economic Competitiveness: Hearings Before the Subcomm. on Sci., Tech., & Space of the Comm. on Commerce, Sci. & Transp.*, 99th Cong. 124-25 (1985).

50. *Id.* (emphasis added) (statement of Ian M. Ross, then-President, AT&T Bell Labs.).

51. *See* FIALKA, *supra* note 2, at 6.

secret theft were staggering, reaching "in the billions."[52] Corning Inc., another robust American corporation, complained that it was forced to try and combat—by itself—foreign state-sponsored efforts to misappropriate its fiber-optic technology.[53] One of its former executives told Congress: "It is very difficult for an individual corporation to counteract this activity. The resources of a corporation—even a large one such as Corning—are no match for espionage activities that are sanctioned and supported by foreign governments."[54] Without access to the U.S. government's vast resources, coupled with a comprehensive, coherent, and modern body of law, American corporations are nearly defenseless against the spy in search of the "billion-dollar booty."

This same analysis applies even when the economic spy is not sponsored by or working on behalf of a foreign government. Whether a foreigner or American, this spy is often a temporary or disgruntled soon-to-be-former employee, contractor, or supplier available for sale to the highest bidder.[55] When the act is not sponsored by a foreign government, it is generally referred to as the theft of proprietary economic information, such as trade secrets, rather than economic espionage. Semantics aside, whatever the motivation and whoever the sponsor, the impact is the same. The year before Congress passed the EEA, a survey of 325 anonymous U.S. corporations showed that companies reported an average of thirty-two cases of theft of proprietary economic information per month, with losses in excess of $5 million.[56] More than sixteen years later, the problem of both foreign economic espionage and theft of trade secrets persists.[57]

Colonel John Boyd, a retired United States Air Force fighter pilot, developed a theory of combat in the late 1970s that he affectionately dubbed the OODA-Loop. Originally meant for pilots, the OODA-Loop "meant that a pilot who could *O*bserve, *O*rient himself, *D*ecide, and *A*ct faster would almost always win, because he was flying inside his enemy's [l]oop."[58] Used widely in the Gulf War, "Boydian" ideas of "making quick, accurate decisions and moving faster than a competitor can react"

---

52. *Id.*

53. *Id.* at 7.

54. *Id.*; *Foreign Economic Espionage Hearings*, *supra* note 3 (testimony of J.E. Reisbeck, then-Executive Vice President of Corning Inc.).

55. FIALKA, *supra* note 2, at 15.

56. *Id.*; *see* 142 CONG. REC. S12,212 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl referencing ASIS survey).

57. *American Interests Abroad Hearings*, *supra* note 4.

58. FIALKA, *supra* note 2, at 196-97.

ultimately found their way into American business.[59] This migration of military strategy to the business world may be seen as a "good thing" because "in matters involving high technology . . . our competitors have been thinking and acting in warlike terms for decades."[60] They have systematically stolen our ideas, our technology, and our high-paying blue collar jobs, causing a rapid decline in American economic competitiveness and compromising national security.[61]

How best to address the issue is always the sticking point. In his book *War by Other Means: Economic Espionage in America*, John J. Fialka suggests that America take the offensive against its economic competitors: we must operate inside our enemy's "loop."[62] Applying Colonel Boyd's famed OODA-Loop theory to the current situation, Fialka posits that we must *O*bserve the reality of the economic war we are fighting, *O*rient ourselves to it by understanding our position in relationship to our competitors, *D*ecide to make the difficult changes required to stay competitive, and *A*ct by implementing those difficult decisions.[63]

AT&T, IBM, and Corning correctly observed that we are in an economic war. They understood their relationship to their competitors and decided that they needed assistance to change that position. They asked Congress to act to give them unfettered access to every federal investigative, legal, and judicial resource available to them to stave off the foreign spies or insiders causing the economic hemorrhage. In 1996, Congress gave them a new weapon in the EEA. But, as discussed below, it was neither a cure-all nor a fail-proof solution.

B. Explaining the EEA of 1996

1. Sections 1831 and 1832: The Two Offenses

The legislative history indicates that while the primary motivation for the federal criminalization of trade secret theft was to fight foreign economic espionage, the domestic theft of trade secrets, absent a foreign connection, was also a matter of high importance.[64] Echoing these concerns, the EEA created two offenses under which trade secret theft can be prosecuted: (1) the offense of foreign "economic espionage" set forth in 18 U.S.C. § 1831 and (2) the offense of commercial "theft of

59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.* at 198.
63. *Id.*
64. H.R. REP. NO. 104-788, at 1 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4021.

trade secrets" set forth in 18 U.S.C. § 1832.[65] The first offense, "economic espionage," punishes misappropriation of trade secrets undertaken by anyone "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."[66]

The second offense, "theft of trade secrets," also known as industrial espionage,[67] is a general provision that does not require any foreign nexus.[68] It applies to anyone who knowingly engages in any act of trade secret theft

> with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret.[69]

Although the target of each offense is different, both provisions carry identical standards for what constitutes a trade secret and what constitutes misappropriation, the *actus reus*. They do, however, impose varying penalties depending on the identity of the defendant and the purpose behind the defendant's actions.[70] It is significant that the definition of "trade secret" and the definition of "misappropriation" in the EEA are markedly different from their counterparts in most state, civil, and criminal statutes.[71] In most instances, the EEA definitions are more expansive.

---

65. H.R. 3723, 112th Cong. (1st Sess. 2011). When Congress took up the issue of updating the federal laws to reflect current technological and economic realities, it developed three separate bills to address the issue. Senator Kohl introduced S. 1556, which prohibited the theft of proprietary economic information by any person. Senator Specter introduced S. 1557, which focused on thefts by foreign nations and those working on their behalf. The Senate adopted S. 1556 with an amendment based on S. 1557 to consolidate the theft of proprietary economic information and trade secrets by private individuals and corporations and by foreign governments and those acting on their behalf. The bills were passed using H.R. 3723, the House companion bill introduced by Representative McCollum.

66. 18 U.S.C. § 1831(a) (2012).

67. *See generally Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011*, OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC. (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

68. *See* 142 CONG. REC. H12,137 (daily ed. Sept. 28, 1996) (statement of Rep. McCollum).

69. 18 U.S.C. § 1832(a). This portion of § 1832(a) was later amended by the Trade Secrets Clarification Act, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012).

70. Pooley et al., *supra* note 28, at 192.

71. Many states that have some form of civil remedy for theft of trade secrets have modeled their statutes on the UTSA. Remedies often include recognition of a tort for misappropriation of the information or enforcement of contracts governing the use of the information. *Id.* at 186. Most state criminal statutes have narrower definitions than their civil counterparts. *Id.*

2. Defining Trade Secrets

The EEA significantly broadens the definition of "trade secret" from that in the Uniform Trade Secrets Act (UTSA), the model for many state civil statutes.[72] Section 1839(3) of the EEA defines a trade secret as follows:

> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means, by the public."[73]

This enumerated list of types of secrets is much broader in the EEA's definition of "trade secret" than that in the definition in the UTSA.[74] Specifically, the EEA includes all forms of business and

---

72. As of the writing of this article, forty-seven states (along with Puerto Rico, the U.S. Virgin Islands, and the District of Columbia) have adopted some form of the UTSA. Legislation has been introduced in Massachusetts in 2013 (H. 27). Texas was the most recent state to adopt legislation: S.B. 953 was passed on May 2, 2013, with the law effective as of September 1, 2013. *Relating to the Adoption of Uniform Trade Secrets Act*, TEX. LEGISLATURE ONLINE, http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=SB953 (last updated May 2, 2013). North Carolina and New York have no legislation underway. Note that while North Carolina has not passed the UTSA or a variation thereon, the North Carolina Trade Secrets Protection Act (ch. 66, art. 24) is very similar to the UTSA in its definitions, prohibitions, and remedies. New York does not have a statute protecting trade secrets; trade secrets are protected under common law rights, with the New York courts interpreting "trade secret" based on the definition in the Restatement. *Legislative Fact Sheet—Trade Secrets Act*, UNIFORM LAWS COMM'N, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act (last visited May 23, 2013); *see also* UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005).

> (4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Id.

73. 18 U.S.C. § 1839(3).

74. Pooley et al., *supra* note 28, at 188-89.

financial information, while the UTSA limits trade secrets to more traditional scientific information.[75]

Interestingly, this definition was not added to the EEA until the final version of the bill, after the conference committee, when the term "proprietary economic information" was changed to "trade secrets."[76] This last-minute change also reflected an additional limitation in the definition from yet an earlier version of the Senate bill that included the terms "data," "tools," "mechanisms," "compounds," and "commercial strategies."[77] These changes suggest that Congress was aiming to capture a wider range of types of valuable proprietary information in light of modern technological and economic realities. This broader definition in effect brings this wider range of "secret" information within the ambit of the statute.

Additionally, the EEA's definition of trade secrets encompasses all forms of information, "whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[78] This provision suggests that information that is merely memorized and stored only in a person's "memory" constitutes theft under the statute. The UTSA is silent on the issue of information storage. Experts suggest this is not an unexpected change because "courts have periodically found defendants liable under civil statutes even though the information they took was only in their heads."[79] This provision, however, does not refer to an employee's general knowledge and skill acquired from working at a job.[80]

Another difference in the EEA's treatment of trade secrets as compared to the UTSA is the "particularity" with which trade secrets must be defined. Most civil statutes do not require specific identification of the trade secrets at issue until very late in the discovery phase of litigation.[81] In some instances, a plaintiff may proceed all the way to trial

---

75. The EEA also broadens the definition of "trade secret" in ways that fall outside the scope of this Article.

76. *See Legislation Addressing Trade Secret Theft, Computer Break-Ins Passed by Congress*, 1 ELEC. INFO. POL'Y & L. REP. 599 (1996).

77. *Id.*

78. 18 U.S.C. § 1839(3).

79. *See, e.g.*, Allen v. Johar, Inc., 823 S.W.2d 824 (Ark. 1992); *see also* Stampede Tool Warehouse, Inc. v. May, 651 N.E.2d 209 (Ill. App. Ct. 1995) (imposing punishment on a defendant who memorized a customer list); PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995). Because of the "inevitable disclosure" of secrets, the court in *PepsiCo* prohibited a former employee from accepting competing employment even absent proof of trade secrets theft. Pooley et al., *supra* note 28, at 189 n.75.

80. H.R. REP. NO. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4025-26.

81. Margaret A. Esquenet & John F. Hornick, *Trade Secret Identification: The Importance of Timing in Discovery*, FINNEGAN (Feb. 2005), http://www.finnegan.com/resources/

without ever having disclosed with any particularity the trade secrets the defendant allegedly misappropriated.[82] Failure to identify timely and adequately the trade secrets that were claimed to be stolen contributes to difficult, costly, and inefficient litigation.[83] While the language of the EEA does not specifically address this issue, the legislative history indicates that Congress intended for trade secrets to be defined with specificity under EEA guidelines. In fact, a respected expert on economic espionage, Peter Schweizer, noted that an EEA "prosecution (under this statute) *must* establish a particular piece of information that a person has stolen or misappropriated."[84] This requirement for particular identification of the trade secrets during an EEA prosecution should help to balance the competing goals of the prosecutor and the defendant.

3. The *Actus Reus*: Misappropriation

Sections 1831(a) and 1832(a) radically depart from the UTSA and create a new definition for what constitutes misappropriation of trade secrets.[85] The statutory language for both sections holds liable anyone who knowingly:

---

articles/articlesdetail.aspx?news=ac7cf37b-c333-4b4e-bafe-6cb9dda0db42 ("A few jurisdictions have made early trade secret disclosure a substantive requirement of their laws. Notably, California has a statutory provision, albeit buried in its code of civil procedure, that requires a plaintiff to disclose its trade secrets with reasonable particularity before it can obtain discovery from defendants. Though not enacted by a legislature, Delaware has an equally explicit common law rule requiring a plaintiff to describe its trade secrets with reasonable particularity before discovery begins. Endorsing analogous positions to California and Delaware, federal district courts in Illinois, Minnesota, Florida, and Virginia have imposed an early disclosure requirement on plaintiffs in trade secret cases. In addition, a state court in Massachusetts has also required early disclosure of trade secrets.").

82. *Cf.* Thermodyne Food Serv. Prods. v. McDonald's Corp., 940 F. Supp. 1300, 1304-05 (N.D. Ill. 1996) (rejecting the claim that a newly asserted trade secret unfairly surprised the defendant); Pooley et al., *supra* note 28, at 191 n.86.

83. *See* Esquenet & Hornick, *supra* note 81.

84. 142 CONG. REC. S12,213 (daily ed. Oct. 2, 1996) (citing Peter Schweizer, *The Growth of Economic Espionage: America Is Target Number One*, FOREIGN AFF., Jan.-Feb. 1996, at 9 (emphasis added)).

85. The UTSA in section 1(2) defines misappropriation as:

> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who 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 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.

> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3) . . . .[86]

This definition broadens the definition of its civil counterparts by criminalizing activities that have long been considered lawful business espionage.[87] For example, including the terms "appropriate" and "take" as unlawful means of obtaining one's trade secrets implies that "conduct such as observing a competitor's property from across the street" is illegal.[88] The legislative history indicates that "the EEA is not intended to inhibit robust competition" and, moreover, the "legislative record might be sufficient to declare broad categories of competitive intelligence-gathering proper and therefore lawful."[89] Experts suggest that this may be a moot issue "since it is extremely unlikely that a United States Attorney will prosecute a defendant for activities that are permitted under civil trade secrets law."[90]

Subsection (2) broadens most state civil statutes by enlarging the domain of control trade secret owners have over their secrets. Trade secret owners, under the EEA, are permitted to prohibit others from not only acquiring their secrets by the methods set forth in subsection (1), but also "*cop[ying], duplicat[ing], sketch[ing], draw[ing], photograph[ing], download[ing], upload[ing], alter[ing], destroy[ing], photocopy[ing], replicat[ing], transmit[ing], deliver[ing], send[ing], mail[ing], communicat[ing], or convey[ing] trade secret[s without authorization]*."[91]

UNIF. TRADE SECRETS ACT § 1(2) (amended 1985), 14 U.L.A. 537 (2005).

86. 18 U.S.C. §§ 1831(a), 1832(a) (2012).

87. Pooley et al., *supra* note 28, at 192-93.

88. *Id.* at 193.

89. *Id.*; *see also* 142 CONG. REC. S12,212 (daily ed. Oct. 2, 1996) (statement of Peter Schweizer) ("Other companies can and must have the ability to determine the elements of a trade secret through their own inventiveness, creativity and hard work . . . . [P]arallel development of a trade secret cannot and should not constitute a violation of this statute.").

90. Pooley et al., *supra* note 28, at 193.

91. 18 U.S.C. §§ 1831(a)(2), 1832(a)(2) (emphasis added).

This definition extends the reach of misappropriation under the EEA to legally acquired trade secrets if they are handled in one of the ways listed in subsection (2).[92] By way of contrast, the UTSA places restrictions on uses of legally acquired trade secrets, but "limits its reach to the disclosure or use of a secret in violation of a confidential relationship."[93] In effect, under the EEA, trade secret owners may enlist the help of the Justice Department to prevent anyone, whether or not in a confidential relationship with the trade secret owner, from engaging in the prohibited conduct set forth in subsection (2).[94]

4. Penalties: Criminal Sanctions

Sections 1831 and 1832, while identical with respect to the definitions of "trade secret" and "misappropriation," impose varying punishments on guilty defendants depending on who committed the prohibited conduct and for what purpose the defendant acted. Section 1831(a) severely punishes the acts[95] of misappropriation listed in subsection (2) by anyone "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent" with up to fifteen years in prison, fines up to $10 million (or more)[96] for organizations,[97] and fines not to exceed $5 million for individuals.[98] Section 1832(a) also severely punishes violators by imposing a prison term of ten years,[99] and/or unspecified fines for individuals,[100] and fines not to exceed $5 million for corporations or other violating organizations.[101]

---

92. Pooley et al., *supra* note 28, at 193.

93. *Id.*; *see also* UNIF. TRADE SECRETS ACT § 1(2)(ii)(B), 14 U.L.A. 438 (1996).

94. Pooley et al., *supra* note 28, at 193; *see also* H.R. REP. 104-788, at 8 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026 ("The concept of control also includes the mere possession of the information, regardless of the manner by which the non-owner gained possession of the information.")

95. 18 U.S.C. § 1831(a) includes attempts to commit and conspiracies to commit the acts defined therein.

96. *Id.* The EEA set the maximum fine for organizations to $10 million, which on January 14, 2013, was amended to "the greater of $10,000,000 or *3 times the value of the stolen trade secret*." Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, § 1831, 126 Stat. 2442, 2443 (2013) (emphasis added).

97. 18 U.S.C. § 1831(b).

98. *Id.* § 1831(c). The EEA set the maximum individual fine to $500,000, which was amended to $5 million. Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, § 2(a), 126 Stat. 2442.

99. 18 U.S.C. § 1832(a).

100. *Id.* Because the individual fine is not specified, the general maximum fine for felonies of $250,000 should apply. *Id.* § 3571(b)(3); *see also* Pooley et al., *supra* note 28, at 201.

101. 18 U.S.C. § 1832(b).

Section 1834 of the EEA mandates criminal forfeiture of the defendant's property during sentencing.[102] Such forfeiture is made directly to the United States, not the victim plaintiff.[103] The congressional record indicates that legislators intended for victims to seek restitution from the United States out of the forfeited property, but this is not always an adequate remedy.[104] The EEA's forfeiture provisions are generally governed by federal drug-forfeiture laws.[105] These "laws vest title to the seized property in the United States, and provide that the Attorney General shall dispose of those assets 'by sale or any other commercially feasible means.'"[106] This is most problematic when the seized product is the trade secret itself, or a product in which the trade secret is embodied. Only the victim should be in possession of the trade secret; the fact that the secret may technically be available at a public auction to anyone other than the victim plaintiff from the Office of the Attorney General is wholly contrary to the victim's interest in keeping the information secret. Experts suggest that the victim petition the court under a special procedure within the drug-forfeiture statute to have the "property in which the victim claims an interest" returned directly to the victim, or destroyed, rather than sold at auction.[107] However, it is incumbent upon the victim, not the government, to initiate this special procedure in lieu of public sale.

5. Penalties: Civil Remedies

Although a criminal statute, the EEA does provide for a form of civil injunctive relief. Section 1836 of the EEA vests power in the Attorney General to commence civil proceedings to enjoin violations pursuant to the Federal Rules of Civil Procedure.[108] This provision works in conjunction with a criminal prosecution to allow the government to

---

102. 18 U.S.C. § 1834 states that the court shall order forfeiture as part of the sentencing (citing *id.* § 2323(b)(1)).

103. *Id.*

104. Pooley et al., *supra* note 28, at 202 (citing 142 CONG. REC. S12,201-07 (daily ed. Oct. 2, 1996) (statement of Sen. Nickles)).

105. *See* 21 U.S.C. § 853 (2012).

106. *See* Pooley et al., *supra* note 28, at 302 (citing 21 U.S.C. § 853(h)).

107. *Id.*; *see also* 18 U.S.C. § 853(n).

108. 18 U.S.C. § 1836 reads as follows:

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

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this section.

use its injunctive power to prevent public disclosure of the victim's trade secret or, at a minimum, maintain the status quo.[109]

6. Extraterritorial Jurisdiction

The EEA has a broad reach that grants extraterritorial jurisdictional power to the government to investigate and prosecute misappropriation that occurs outside of the United States.[110] Section 1837 applies to conduct outside the United States, if:

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or
(2) an act in furtherance of the offense was committed in the United States.[111]

This provision helps to ensure that acts of foreign espionage are properly within the scope of the statute, because most of them occur outside the United States.[112] Absent this jurisdictional grant, the FBI would lack the authority to investigate foreign espionage adequately and would be crippled in its ability to gather evidence sufficient to prosecute the illegal conduct.

C. Legislative Updates to the EEA of 1996 from the 112th Congress (2011-2012)

Toward the end of the 112th Congress, significant updates to the EEA were adopted for the first time: Public Law 112-236 was approved on December 28, 2012, and Public Law 112-269 was passed in late 2012 and approved on January 14, 2013.

1. Public Law 112-236: The Theft of Trade Secrets Clarification Act of 2012[113]

The Theft of Trade Secrets Clarification Act of 2012 (TTSCA) amended § 1832(a) on Theft of Trade Secrets of the EEA. The TTSCA was written in direct response to a controversial decision in April 2012 in the case *United States v. Aleynikov*, in which the United States Court of

109. Pooley et al., *supra* note 28, at 203.
110. 18 U.S.C. § 1837.
111. *Id.*
112. Pooley, *supra* note 28, at 204.
113. Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627. Sponsored by Senator Patrick Leahy (D-Vt.), Chairman of the Senate Judiciary Committee. Cosponsored by now-retired Senator Herb Kohl (D-Wis.). It was signed by the President on December 28, 2012.

Appeals for the Second Circuit overturned a conviction under the EEA. The defendant, Sergey Aleynikov, a Goldman Sachs programmer, had been convicted of stealing source code for Goldman Sachs's proprietary trading program.[114]

The original language of § 1832(a) of the EEA, defining the "what" of a trade secret, had originally read:

> Whoever, with intent to convert a trade secret, that is related to *or included in a product that is produced for or placed in* interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—[115]

In *Aleynikov*, the Second Circuit interpreted the clause "related to or included in a product that is produced for or placed in . . . commerce" to mean that only secrets related to goods—or "products"—were protectable under the statute, effectively excluding services from protection. This was not an obvious or anticipated interpretation of the clause. The court would have more broadly construed the clause had they applied the verb phrase "related to" to the indirect object of the clause, "interstate or foreign commerce."[116] With this application, the clause would essentially read, "that is related to interstate or foreign commerce, or included in a product that is produced for or placed in interstate commerce." The clause would thus indicate that the protectable trade secret could be a *service* used in commerce (*related to*), as well as a *good* used in commerce (*included in*). If one assumes the court's conclusion that the "product" is the only and essential direct object of the clause, then the verb phrase "included in" becomes irrelevant and thus loses all meaning, because any trade secret "included in" a product is by its nature also "related to" that same product. The court's interpretation eviscerates the clause by failing to acknowledge both separate verb phrases.

The practical result of the court's strange reading of § 1832 and the resulting holding was that computer code was not considered a protectable trade secret unless it was part of a product in commerce. The ruling effectively excluded a broad range of proprietary information from trade secret protection. Because much trade secret theft involves electronic data used within a company, this holding could have had

---

114. United States v. Aleynikov, 676 F.3d 71, 73-75 (2d Cir. 2012).

115. Economic Espionage Act of 1996, Pub. L. No. 104-294 § 1832(a), 110 Stat. 3488, 3489 (emphasis added).

116. *Aleynikov*, 676 F.3d at 82.

devastating consequences in the prosecution of trade secret theft if left to stand.[117]

Knowing that successful prosecutions under § 1832 had been rare and recognizing that the holding would further dilute the efficacy of the prosecutorial mission of the EEA, Congress took swift action to remedy the court's decision, passing the TTSCA through both chambers in November (Senate) and December (House) of 2012. The amendment to the section struck the italicized words above ("or included in a product that is produced for or placed in") and replaced them so that the section now reads:

> Whoever, with intent to convert a trade secret, that is related to *a product or service used in or intended for use in* interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—[118]

The change in language should provide clear guidance to future courts in their application of the now-amended law. The closing of the loophole was an important step forward, though its impact on ongoing prosecutions remains unknown.[119]

2. Public Law 112-269: The Foreign and Economic Espionage Penalty Enhancement Act of 2012[120]

The Foreign and Economic Espionage Penalty Enhancement Act of 2012 (FEEPEA) amended § 1831(a) and § 1831(b) of the EEA. The

---

117. *See generally Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, *supra* note 67.

118. Theft of Trade Secrets Clarification Act of 2012, Pub. L. 112-236, § 2, 126 Stat. 1627 (codified as amended at 18 U.S.C. § 1832 (2012)) (emphasis added).

119. Peter Toren, "*Clarification" to the Economic Espionage Act Awaits President Obama's Signature*, PETERTOREN.COM, http://petertoren.com/clarification-to-the-economic-espionage-act-awaits-president-obamas-signature/ (last visited May 23, 2013).

120. Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-264, 126 Stat. 2442 (codified as amended at 18 U.S.C. § 1831 (2012)). The Senate version of the bill, S. 678, was sponsored by now-retired Senator Kohl, with cosponsored Senators Richard Blumenthal (D-Conn.), Tom Coburn (R-Okla.), Chris Coons (D-Del.), Dianne Feinstein (D-Cal.), Lindsey Graham (R-S.C.), Chuck Grassley (R-Iowa), Amy Klobuchar (D-Minn.), Sheldon Whitehouse (D-R.I.), and now-retired Senator Jon Kyl (R-Ariz.).

The House companion bill, H.R. 6029, which was amended by the Senate and passed into law, was sponsored by Representative Lamar Smith (R-Tex.), with cosponsors Representatives Steve Chabot (R-Ohio), Jason Chaffetz (R-Utah), Howard Coble (R-N.C.), John Conyers (D-Mich.), Ted Deutch (D-Fla.), Bob Goodlatte (R-Va.), Ted Poe (R-Tex.), Adam Schiff (D-Cal.), Mel Watt (D-N.C.), Frank Wolf (R-Va.), and now-retired Representative Howard Berman (D-Cal.). It was signed by the President on January 14, 2013. This same group of congresspersons, a majority of whom serve on their (respective) Judiciary Committees, should have a strong interest in supporting a federal civil cause of action.

principal change was to the maximum fine amount, which for individuals was increased from $500,000 to $5 million, and which for organizations was changed from $10 million to "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 and other costs of reproducing the trade secret that the organization has thereby avoided."[121] The changes in the maximum amounts reflect not only inflation but also the increased value of proprietary information. The enhanced penalties for organizations set a seemingly limitless cap on the amount, relative to the cost of creating or discovering the secret in question.

The FEEPEA also requires the United States Sentencing Commission (the Commission) to review and possibly amend its sentencing guidelines for all offenses related to foreign trade secret theft and economic espionage. The Commission must consult with the United States Departments of Justice, Homeland Security, and State, and the Office of the United States Trade Representative, as well as individuals or groups representing law enforcement, "owners of trade secrets [, and] victims of economic espionage offenses."[122] The purpose of the review, which was to be completed by July 13, 2013, was ultimately to increase sentencing guidelines to levels commensurate with the great damage inflicted by economic and industrial espionage.[123] The law also aims to deter economic espionage primarily through the threat of punishment, because it gives some teeth to the seldom-enforced § 1831.[124]

IV. MAKING THE CASE FOR A PRIVATE FEDERAL CAUSE OF ACTION

The EEA does not criminalize every instance of trade secret theft. In many cases, civil remedies are the more effective, indeed preferred, means for victims to seek meaningful relief.[125] Despite scores of indictments, there remains only one reported decision regarding an EEA

---

121. Foreign and Economic Espionage Penalty Enhancement Act § 2, 126 Stat. at 2442.

122. *Id.*

123. This follows the recommendation of Victoria Espinel, former United States Intellectual Property Enforcement Coordinator. *See* H.R. REP. No. 112-610 (2012), *reprinted in* 2012 U.S.C.C.A.N. 1184.

124. Since the enactment of the EEA, there have been 118 prosecutions under § 1832 (on Theft of Trade Secrets), while there have only been 9 under § 1831 (on Economic Espionage), none since 2011. EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_stragegy_on_mitigating_the_theft_of_U.S._trade_secrets.pdf.

125. The EEA, however, criminalizes the incomplete crimes of conspiracy and attempt. Mark D. Seltzer & Angela A. Burns, *Criminal Consequences of Trade Secret Misappropriation: Does the Economic Espionage Act Insulate Trade Secrets from Theft and Render Civil Remedies Obsolete?*, 1999 B.C. INTELL. PROP. & TECH. F. 052501, 052501-02 (1999).

prosecution.[126] In *United States v. Hsu*, the core issue concerned disclosure of confidential trade secret information, with particular concern over the level of access given to the defendant.[127] This is one of American industry's primary concerns in referring misappropriation cases to the government. In the case, the court denied the government's motion to prevent disclosure, allowing "select members" of the defense team access to the documents.[128] For companies faced with the *Hsu* dilemma, where discovery in criminal proceedings requires disclosure to the defendant of the very trade secret information the victim was trying to protect, they must carefully consider whether making a criminal referral is worth the risk, even though pursuing remedies under state civil statutes or common law theories may be challenging.[129] While putative plaintiffs are not fully immunized from mandatory disclosures in civil proceedings, they retain considerable control over the scope and timing of those disclosures.[130]

There are numerous other benefits to creating a federal statute on point. Topping the list is the fact that not all reported instances of economic espionage or trade secret theft are prosecuted. Federal prosecutors may, in their sole discretion and for a variety of reasons, choose not to pursue a case. Absent a federal prosecution, these victims are often unable to pursue civil remedies that take into consideration the

---

126. *See* United States v. Hsu, 155 F.3d 189 (3d Cir. 1998).

127. *Id.* at 197.

128. Seltzer & Burns, *supra* note 125, at 052502.

> [*United States v. Hsu*] involved the attempted theft from Bristol-Myers Squibb Company of trade secrets regarding its highly successful anti-cancer drug Taxol. In this case, the defendants, who were employees of a company in Taiwan seeking to diversify into biotechnology, offered to pay bribes to a Bristol-Myers employee in exchange for information about Taxol. According to the indictment, the defendants first contacted an information broker in the United States who, unbeknownst to them, was in fact an FBI undercover agent. After learning from the information broker that Bristol-Myers would be unlikely to share its Taxol technology, the defendants directed him to obtain the information by bribing a corrupt Bristol-Myers employee. The agent then represented that such a corrupt employee had been found and arranged a meeting, after which the defendants were arrested and charged with the attempted receipt and/or possession of a trade secret and conspiracy to receive or possess a trade secret under § 1832 (a) (4) and (5).

John F. Hornick, *The Impact of the Economic Espionage Act of 1996*, FINNEGAN, http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=e406fccb-8d4c-4d88-8369-991a1bed3819 (last visited Nov. 14, 2013).

129. *Hsu*, 155 F.3d at 187-88.

130. Although plaintiffs in civil actions are required to disclose the trade secret at issue, they are in control of the disclosure to the defendant. In criminal prosecutions, the victim discloses the information to the government, who in turn presents the information to the defendant.

larger definition of what constitutes a trade secret as set forth in the EEA. To pursue redress for harm suffered from the misappropriation in federal courts pursuant to a federal statute that defines "trade secrets" as broadly as the EEA does would simplify the litigation process for both plaintiffs and defendants and increase judicial economy. Second, a federal cause of action resolves jurisdictional, forum selection, and other procedural issues arising from litigation in state courts. Third, adopting the EEA's definition of "trade secrets" and "misappropriation" sweeps a wide variety of acts not punishable at the state level into the ambit of a federal statute. Fourth, a federal cause of action would ensure availability of proportional remedies often lacking in state statutes.[131] Finally, a federal civil right of action provides a single comprehensive scheme, "one stop shopping," for both plaintiffs and defendants to litigate valid claims, thus decreasing the cost of litigating multiple lawsuits in multiple jurisdictions and increasing judicial efficiency. These five benefits are considered in more detail below.

A. Prosecutorial Discretion

There are many reasons why the government may decline a prosecution. One of the primary litmus tests used by prosecutors to decide whether to seek an indictment is the government's ability to meet its burden of proof at trial. In criminal cases, the burden is on the prosecution to prove each and every element of the offense beyond a reasonable doubt,[132] a much higher burden than the "preponderance of the evidence" generally required for civil cases. It is not a simple feat to convince twelve jurors of a defendant's guilt beyond a reasonable doubt.[133] If the prosecutor's office lacks confidence in the sufficiency of the evidence to meet the high burden at trial, it will likely pass on the case.[134] Even though the case warrants prosecution on the merits, absent

---

131. Pooley et al., *supra* note 28, at 204.

132. U.S. CONST. amend. IV; *see also Hsu*, 155 F.3d at 195 (citing 18 U.S.C. § 1832 (2012)). In addition to the threshold intent requirements of the EEA, the government must prove beyond a reasonable doubt that (1) "the defendant acted with specific intent to convert the trade secret with knowledge that the trade secret was proprietary or closely guarded; (2) that the defendant attempted to or conspired to convert the trade secret for the economic benefit of anyone other than the rightful owner; and (3) that the defendant intended or knew that the conversion offense would injure the lawful owner of the trade secret." Seltzer & Burns, *supra* note 125, at 8.

133. Pooley et al., *supra* note 28, at 222.

134. Or, more likely, the prosecutor will not receive approval to prosecute. *See* Thomas Reilly, *Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and the "Foreign Instrumentality" Element*, U.S. ATTORNEYS' BULL., Nov. 2009, at 24, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf. "[T]he Assistant Attorney General (AAG) for the National Security Division (NSD) must approve [any] action [involving a

a criminal indictment, the victim is left with no judicial alternative but to pursue a state civil judgment against the wrongdoer.

The government also favors prosecuting thefts of scientific and technical data over thefts of business and financial information.[135] Not only is it easier to ascribe a monetary value to scientific data, as opposed to less precise business information, but victims are also generally more capable of producing tangible evidence of the value of the stolen property when it concerns scientific or technical data.[136] The higher the value and the greater its determinability, the more likely the government will become involved.[137] Many victims of business information theft are therefore forced to seek state civil redress.

The actual monetary value of the stolen information is a pivotal component of the decision of whether to seek an indictment. There are ninety-three United States Attorneys in the United States who serve under the direction of the Attorney General as the nation's principal litigators.[138] With limited resources, they handle a wide variety of federal cases, often involving defendants accused of committing reprehensible crimes.[139] A combination of heavy workload and limited resources has resulted in their only considering cases with a minimum monetary threshold in "white collar crime cases" that often depend on the "amount of the defendant's financial gain or the amount of the victim's financial loss."[140]

Absent sufficient confidence that the government will be able to satisfy its burden of proof, and evidence showing that a significant amount of money is at stake, the government will likely decline prosecution. Without a federal civil statute on point, trade-secret-theft victims who succumb to a prosecutor's discretion are left to pursue the accused under applicable state law, if any law. This can be harmful to both the victims and the accused, whose subjection "to the laws of

---

charge of economic espionage]." The only relief from this high burden is the lack of necessity to prove association of the defendant with the intended beneficiary. *Id.* at 25. "All that is necessary is that the *intent or knowledge* to benefit a foreign government, instrumentality, or agent is provable" *Id.* (emphasis added).

135. Pooley et al., *supra* note 28, at 222.

136. *Id.* at 205.

137. *Id.* at 222.

138. *Mission*, OFFS. U.S. ATT'YS, http://www.justice.gov/usao/about/mission.html (last visited May 23, 2013).

139. *Id.*

140. Pooley et al., *supra* note 28, at 205.

dozens of states creates a confusing web of conflicting standards and punishments."[141]

B. Federal Jurisdiction, Forum Selection, and Other Procedural Requirements

High-technology crimes and related causes of action generally involve sophisticated technology and often cross multiple state lines.[142] Because they tend not to be "local" activities, they are not optimally governed by "local" law. Victims may be required to sue the accused in several states in order to fully litigate the claims.[143]

Courts may not exercise judicial power over a defendant without establishing subject-matter jurisdiction over the claims and in personam (personal) jurisdiction over the defendant.[144] Federal jurisdictional reach is defined in Article III, Section 2 of the U.S. Constitution;[145] all other cases must be brought in state court.[146] Article III courts (as they are often referred to) may hear cases arising under federal law; they do not have original jurisdiction over cases arising under state law.[147] A federal cause of action, theft of trade secrets would confer immediate and exclusive original jurisdiction—*in any federal court*—over valid misappropriation claims.[148]

Litigating trade secret claims at the federal level benefits the litigation process in several ways. First, the federal law applies to all claims, regardless of the state where the prohibited conduct took place. Neither plaintiff nor defendant must master the substantive nuances of different state statutes, whether in state court or applying state law in federal court upon proper removal of a case. Second, the litigation

---

141. Robert Damion Jurrens, Comment, *Fool Me Once:* U.S. v. Aleynikov *and the Theft of Trade Secrets Clarification Act of 2012*, 28 BERKELEY TECH. L.J. 833 (2013). Referring to the many victims who are harmed in cyberspace, Jurrens cites Peter Menell in asserting, "[T]he ubiquity of the Internet begs for something less provincial than state laws to regulate its activities." Note that Jurrens cites an outdated source when he states (at 4) that the UTSA or a variation has been adopted by forty-four states. *See Legislative Fact Sheet—Trade Secrets Act*, *supra* note 72.

142. *See generally* KENNETH S. ROSENBLATT, HIGH-TECHNOLOGY CRIME: INVESTIGATING CASES INVOLVING COMPUTERS (1995).

143. Jurrens, *supra* note 141.

144. Plaintiffs are not free to bring suit wherever they choose. *See* Pennoyer v. Neff, 95 U.S. 714, 727 (1877).

145. U.S. CONST. art. III.

146. *Id.* amend. X (instructing that the federal government has the authority to exercise powers expressly granted or implied in the Constitution; all other powers are reserved to the states).

147. *Id.* art. III, § 2.

148. 18 U.S.C. § 1331 (2012).

process is subject to the Federal Rules of Civil Procedure, rather than state procedural rules, which vary from state to state. This may be particularly useful in connection with issues of joinder of parties[149] and joinder of claims[150] in a single action, as well as the discovery process,[151] thus bringing predictability and consistency to the litigation. Third, with federal subject matter jurisdiction automatically conferred and the choice of law resolved, plaintiffs may be less limited in their choice of venue than at the state level, having only to establish that the forum can exercise personal jurisdiction over the defendant.[152] Venue rules exist to impose limitations on where a plaintiff can bring suit to those forums that bear a rational relationship to the parties and the claims.[153] In trade secret cases, there are likely many different suitable forums. Easing restrictions on venue selection would be highly attractive to plaintiffs, particularly because plaintiffs and defendants have competing interests in where a suit is brought: plaintiffs seek a venue where the probability of seating a sympathetic jury is high, something defendants assiduously avoid.

Section 1837 of the EEA confers extraterritorial jurisdiction over conduct outside the United States provided:

> (1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or
> (2) an act in furtherance of the offense was committed in the United States.[154]

This is an extremely broad jurisdictional grant aimed primarily toward ensuring acts of foreign espionage directed toward U.S. assets are swept within the ambit of the statute.[155] Acts of espionage or theft of trade secrets committed against U.S. corporations abroad, some of the most common targets, are therefore violations of the EEA.[156]

Extraterritorial jurisdiction would be particularly beneficial in instances where "civil injunctive relief may prove to be an appropriate *substitute* for criminal punishment. In other cases, particularly those with foreign defendants, federal civil injunctive relief [provided under § 1836 of the EEA] may be able to reach further than injunctive relief

149. FED. R. CIV. P. 20(a).
150. FED. R. CIV. P. 18(a).
151. FED. R. CIV. P. 16.
152. 28 U.S.C. § 1391 (2006).
153. JOSEPH W. GLANNON, CIVIL PROCEDURE 50 (4th ed. 2001).
154. 18 U.S.C. § 1837 (2012).
155. Pooley et al., *supra* note 28, at 204.
156. *See Economic Espionage, Technology Transfers and National Security: Hearing Before the J. Econ. Comm.*, 105th Cong. 1 (1997) (statement of John Fialka).

under existing state trade secret laws."[157] Injunctive relief under the EEA, however, must be sought by the United States on behalf of the victim. Inclusion of a similar provision in a private right of action would allow litigants to pursue injunctive relief directly from the court against foreign defendants who act against their assets. No longer would foreign activity escape civil liability for lack of civil adjudicatory reach.

One of several procedural problems with many state laws is inconsistent statutory requirements for disclosure of the trade secret at issue. In civil trade secret litigation, the timing and scope of trade secret disclosure are problematic. Plaintiffs wish to delay disclosure for as long as possible, while defendants press for full and immediate disclosure at the beginning of discovery. Without statutory guidance, balancing these competing goals can be a long, frustrating, and potentially tricky process.[158]

The EEA circumvents this problem because it is a criminal statute. A criminal defendant has a constitutional right to be fully informed of the charges against him.[159] The government bears the burden of specifying with particularity exactly what the defendant is accused of stealing—here, it is secret information. This burden falls squarely on the prosecution. A similarly styled disclosure requirement, one that statutorily requires the "plaintiff to identify its alleged trade secrets with reasonable particularity in an initial trade secret disclosure statement before the defendant is required to respond to plaintiff's discovery requests," would greatly increase the pace and efficiency of litigation.[160]

C. Broad Definition of Trade Secrets and Misappropriation

The EEA defines the scope of the trade secret, as well as what constitutes an unauthorized taking, with significantly broader terms than the UTSA. Unlike in most state laws, what constitutes a trade secret in the EEA definition is not limited to scientific and technical data, but also includes business and financial information. Additionally, the EEA enlarges the modes of misappropriation by bringing things such as memorized information not recorded in a tangible medium within the scope of the statute.

Assuming the same definitions of "trade secret" and "misappropriation" would be included in a companion civil statute, federal litigants would benefit in at least two ways. First, plaintiffs would be able to rely

157. Pooley et al., *supra* note 28, at 203.
158. Esquenet & Hornick, *supra* note 81.
159. U.S. CONST. amend. IV.
160. Esquenet & Hornick, *supra* note 81.

on the broader definition included in the EEA of what constitutes trade secret information when drafting civil complaints. In those jurisdictions where state trade secret laws have not been passed (note that New York is among them), plaintiffs would no longer be solely limited to remedies arising under common law contract or tort theories. Second, a civil statute enhances the practical application of the EEA because prosecutors carefully consider civil definitions of trade secrets as part of their decision to seek an indictment or file charging documents.[161] The government tends to decline prosecution when "bad acts" may be fairly redressed by civil action.[162] Although these "bad acts" are technically crimes, prosecutors are mindful to avoid meddling in what are properly business disputes.[163] By codifying business information as trade secret information in the civil code, federal courts will begin to create a body of civil trade secret jurisprudence. For the first time, both the government and private litigants will be able to rely on federal precedent and mandatory judicial authority, which will help bring stability to this body of law. Moreover, the government may begin to prosecute egregious instances of business information theft, rather than render them mere business disputes best resolved in civil courts. Uniform definitions will also bring more certainty and stability to business relationships with vendors, customers, and even competitors.[164]

D. Proportional Remedies

The EEA does not replace existing remedies.[165] A companion civil statute would likewise seek to supplement existing state statutory and common law remedies, particularly where they are insufficient.

Trade secret plaintiffs desire to be made whole from their loss: they seek relief proportional to the economic and competitive harm resulting from the theft, which usually combines elements of equitable and legal remedies. To make proper restitution, the defendant should be enjoined from continued use of the stolen information and should be required to pay compensatory and, where appropriate, punitive damages to the

---

161. *See* Pooley et al., *supra* note 28, at 211.

162. *Id.* at 215.

163. *Id.*

164. David V. Radack, *The Uniform Trade Secrets Act*, JOM, Jan. 2006, at 72, *available at* http://www.tms.org/pubs/journals/JOM/matters/matters-0601.html.

165. 18 U.S.C. § 1838 (2012) ("This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).").

victim. Unfortunately, state remedies are generally inadequate to achieve this goal.[166] Injunctions issued by a state court are not enforceable outside the boundaries of the issuing state, and damage awards are limited to the harm arising from activity over which the state court has jurisdiction.

Criminal forfeiture of the defendant's property to the United States is a significant penalty and should not be viewed lightly.[167] However, to repossess the misappropriated assets from the government, victims must affirmatively initiate a repossession action because there is not an automatic right of return. On the civil side, the statute should create an appropriate procedure, allowing for plaintiffs to receive their returned trade secrets and/or derivative property without the burden of further legal action. Arguably, this procedure would be less burdensome than the procedure specified by the criminal forfeiture laws and used in EEA prosecutions.

E. "One Stop Shopping" Litigation

A private right of action under the EEA, together with the criminal provisions, provides a single, comprehensive scheme for expedient resolution of misappropriation claims at the national level. If a victim pursues civil remedies in various state courts for expedited relief, such as a preliminary injunction and compensatory damages, the civil suits may "impede the successful prosecution of EEA violations by subjecting the [g]overnment's material witnesses in the pending criminal case to searching and protracted depositions and interrogatories even before the [g]overnment can present testimony to a jury."[168] Further, without a federal cause of action, "victim litigants who fear on-going harm and the defendant's secretion of valuable assets may oppose [g]overnment requests for a stay of the parallel civil proceeding."[169] By working in

---

166. *See* Pooley et al., *supra* note 28, at 186.

167. 18 U.S.C. § 1834 refers to 18 U.S.C. § 2323(b)(1), which states that the court "shall order" forfeiture as part of the sentencing.

168. Seltzer & Burns, *supra* note 125, at 3.

169. Seltzer & Burns, *supra* note 125, at 9. Avery Dennison Corp. and the U.S. Government were involved in this type of dispute during the prosecution of Pin Yen Yang. *See* United States v. Yang, 74 F. Supp. 2d 724 (N.D. Ohio 1999).

> In this case, Pin Yen Yang, President of Four Pillars Enterprise Company of Taiwan, and his daughter allegedly negotiated and won the cooperation of a chemical engineer working for Avery Dennis [sic] Corp., an Ohio adhesive manufacturer, to obtain proprietary information regarding Avery Dennison's adhesive products. This arrangement lasted for several years, during which Four Pillars received over $50 million worth of trade secret information. The employee, however, subsequently confessed to his employer after being caught going through a colleague's files, and, in

tandem with the criminal provisions, a private cause of action under the EEA obviates these procedural obstacles to a speedy resolution of the claims. Still, because federal civil relief does not trump existing state remedies, it does not impede those litigants who prefer local venues. Given the ubiquity of the problem, the complexity of the fact patterns, and the enormous financial stakes, providing the most effective and efficient tools for litigating trade secret misappropriation is indispensable to attacking theft of vital economic information.

V. THE FEDERAL CAUSE OF ACTION AS A NATIONAL SECURITY PROTECTIVE MEASURE

A federal right of action works in tandem with the EEA. It does not detract from, but rather enhances, the criminal statute. Theft of trade secrets should be penalized civilly for the same reasons it is penalized criminally. Allowing theft of proprietary economic information—the very seeds of economic growth—to go unpunished is careless, irresponsible, and destructive to U.S. economic security. As the former executive vice president of Corning Inc. reminded us, "State-sponsored industrial espionage is occurring in the international business community," and it should be thwarted and defeated by any possible means.[170] According to the National Counterintelligence Center (NACIC), there are no fewer than twenty different methods used by economic spies to conduct economic espionage against a variety of highly targeted industries, including "biotechnology, aerospace, telecommunications, computer software, transportation, advanced materials, energy research, defense, and semiconductor companies."[171] Theft by insiders is also rampant. Twenty-five years ago, before many modern technologies now used to steal information were developed, 48% of 150 high-technology companies polled had been victims of trade secret theft, and 48% of those victims learned of the theft from their

---

> exchange for leniency, agreed to cooperate with the FBI. The Yangs were arrested following an FBI "sting" operation in which they were filmed accepting stolen Avery Dennison documents and removing a portion of the cover page marked "confidential" and "Property of Avery Dennison Corp." They were subsequently indicted for attempt and conspiracy to misappropriate trade secrets under Sections 1832(a)(4) and (5) of the EEA, as well as for wire fraud, receipt of stolen goods, and money laundering.

Hornick, *supra* note 128.

On April 29, 1999, the jury found the defendants guilty of attempt and conspiracy to commit theft of a trade secret, and acquitted them on the remaining fraud charge. United States v. Yang, 281 F.3d 534 (6th Cir. 2002).

170. 142 CONG. REC. S12,211 (daily ed. Oct. 2, 1996) (statement of Sen. Kohl).

171. *Id.*

competitors.[172] Norman Augustine, then-President of Lockheed Martin Corporation, testified before Congress in February 1996 that a recent survey revealed that 100% of aerospace companies "believe[d] that a competitor, either domestic or international, ha[d] used intelligence techniques against them."[173]

When Congress enacted the EEA, it addressed foreign economic espionage and theft of trade secrets with equal force. According to Senator Kohl, the "legislation will be used to go after the foreign intelligence services that take aim at American companies and at the people who walk out of businesses with millions of dollars worth of information."[174] There is no dispute that the criminal law is particularly well-suited to target foreign-sponsored espionage and also punish trade secret theft without a foreign connection. The EEA was purposefully designed to protect our economic security against all of these crimes, and it was carefully drafted to apply to "flagrant and egregious cases of information theft," regardless of the sponsor.[175] Likewise, a civil companion statute should be drafted with equal care to apply to those very same "flagrant and egregious cases of information theft" that warrant prosecution, but that escape indictment.[176] It is indisputably in the national well-being to deter all forms, foreign or domestic, of economic information theft.

Senator Herb Kohl, a sponsor of the original EEA, along with Senator Chris Coons and Senator Sheldon Whitehouse, started taking steps to amend the EEA to include a much-needed civil component on July 17, 2012, when they introduced the Protecting American Trade Secrets (and Innovation) Act of 2012 (PATSIA) in the United States Senate.[177] Senator Kohl's passion for this legislation was evident.[178] He introduced the bill categorizing it as a simple and straightforward solution to the lack of federal civil remedies in the EEA.[179] The bill would provide companies with the most effective and efficient ways to

---

172. *Id.* at 12,212 (referencing the 1988 National Institute of Justice study of trade secret theft among research and development companies in the high-technology industry).

173. *Id.*

174. *Id.*

175. *Id.*

176. *Id.*

177. Protecting American Trade Secrets and Innovation Act, S. 3389, 112th Cong. (2d Sess. 2012).

178. *Id.*

179. *Id.*

hold their competitive edge in the global market, all while fighting trade secret theft and attempting to recoup their losses.[180]

PATSIA would grant U.S. companies federal recourse in the event of trade secret thefts, allowing them to rely on one law as opposed to several individual-state trade secret laws.[181] Unlike the UTSA or the Restatement of Torts, PATSIA creates a higher pleading standard to bring claims for federal civil remedies. The pleading standard states:

> (A) describe with specificity the reasonable measures taken to protect the secrecy of the alleged trade secrets in dispute; and (B) include a sworn representation by the party asserting the claim that the dispute involves either substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country.[182]

This legislation will allow only the most serious trade secret cases to come before the federal courts, providing limitations that protect against companies trying to bring de minimus or frivolous trade secret claims. The legislation's limitations require that victims subject to trade secret theft certify: (1) the "substantial need for nationwide service of process or [(2)] the misappropriation of trade secrets from the United States to another country."[183] Additionally, this legislation will grant judges the power to issue, on *ex parte* application, seizure orders having an execution time of seventy-two hours, in order to prevent the defendant from destroying evidence related to the alleged misappropriation of trade secrets.[184]

PATSIA does not just provide parties with a federal cause of action, it expands the EEA's minimal criminal injunctive relief remedies by allowing trade secret theft victims to receive federal civil remedies in the form of injunctive relief and monetary damages. This includes the possibility of royalties and any additional legal remedies that would prevent further use by the trade secret thief and provide protection of a company's trade secrets.[185]

---

180. *Id.*; Kelley Clements Keller, *Congress Makes Great Move in Amending the Economic Espionage Act*, KELLER L. FIRM LLC, http://thekellerlawfirm.com/congress-makes-good-move-in-amending-the-economic-espionage-act/ (last visited May 23, 2013).

181. Trade Secrets Inst., *Protecting American Trade Secrets Act of 2012 (PATSIA)*, BROOKLYN L. SCH., http://tsi.brooklaw.edu/content/protecting-american-trade-secrets-and-innovation-act-2012-patsia (last visited May 23, 2013).

182. *Id.*

183. S. 3389.

184. *Id.*; Trade Secrets Inst., *supra* note 181.

185. S. 3389.

Unfortunately, the bill died in committee when the 112th Congress ended in early January 2013. PATSIA represented an important move forward that complemented already existing state trade secret law. We urge Senators Coons and Whitehouse to reintroduce the bill in the near term and to take up the leadership mantle on intellectual property and security left by Senator Kohl.[186] We also urge House Judiciary Committee Chairman Goodlatte and Ranking Member Conyers to join them in strengthening our economy and our national security by creating a private federal cause of action. While it would not solve all the problems of industrial espionage, a federal cause of action would give American corporations and other organizations another arrow in their quiver in the fight to protect their economic interests.

VI. CONCLUSION

Every President from Reagan to Obama has publicly recognized in rhetoric and in policy the importance of protecting American trade secrets,[187] and each of the last two administrations has used the "language of security to describe IP issues."[188] Additionally, there has been broad bipartisan support in Congress for ensuring that IP protections protect American innovation in the global economy.[189] From this synthesis of opinion across time and party, we can gather that the lack of successful indictments and prosecutions does not come from an absence of will; it comes from an absence of tools. The criminal penalties may be sufficiently steep, thanks to the Foreign and Economic Espionage Penalty Enhancement Act of 2012, but there must be an option for swift redress for the companies that have been irreparably harmed.

The United States prides itself on having the "largest, richest, industrial economy on earth."[190] But our economic competitiveness is not guaranteed. Because of "America's feeble defenses against economic espionage from the sixties to the eighties[,] . . . the scent of U.S. blood [is] in the air [and i]t creates a hunger for more."[191] As spies and thieves pursue U.S. economic assets and federal investigations and scores of prosecutions are underway, we are reminded that this decades-old

---

186. Keller, *supra* note 180.

187. *See* Debora Halbert, *The Politics of IP Maximalism*, 3 WORLD INTELL. PROP. ORG. J. 81, 84-91 (2011), *available at* http://www.wipo.int/export/sites/www/freepublications/en/intproperty/wipo_journal_3_1.pdf.

188. *Id.* at 86.

189. *Id.* at 88.

190. FIALKA, *supra* note 2, at xiv.

191. *Id.* at 16. The statement is attributed to Edward Miller, former President of the National Center for Manufacturing Sciences. *Id.*

problem has not been cured with a single legislative act.[192] As Senator Specter acknowledged at the time the EEA was enacted:

> Corporations must exercise vigilance over their trade secrets and proprietary information. Contract law may provide civil remedies. In addition, some States have adopted legislation to allow the owners of trade secrets to use civil process to protect their ownership rights. We [the Congress] have been made aware that available civil remedies may not be adequate to the task and that a [f]ederal civil cause of action is needed. This is an issue we need to study carefully, and will do so next year.[193]

More than sixteen years after the passage of the EEA, this issue of civil remedies has not been adequately addressed. With the distractions of corporate malfeasance and international terrorism over the past decade, the attention and resources of the government and private industry have been directed away from this breed of economic crime. Still, only Congress can act to create a private federal right of action for economic espionage and theft of trade secrets; and, in accordance with its constitutional mandate to enact laws that promote the general welfare of the United States, it should do so now.[194] We urge the 113th Congress to pass PATSIA or a similar bill[195] as a means of protecting American business and increasing our standing internationally.[196]

As Peter Toren, former federal prosecutor with the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, points out, in an era of shrinking government resources, businesses must

---

192. Mark Krotoski, National Computer Hacking and Intellectual Property (CHIP) Coordinator, notes two types of investigations—the uncover, prospective investigation of an ongoing offense and the much more common reactive investigation, which often involves a defendant's imminent departure from the country or the company. Krotoski, *supra* note 36, at 11-14.

193. 142 CONG. REC. S12, 207-11 (daily ed. Oct. 2, 1996) (statement of Sen. Specter).

194. *See* U.S. CONST. art. I.

195. On June 20, 2013, U.S. Representative Zoe Lofgren (D-Cal.) introduced H.R. 2466, the "Private Right of Action Against Theft of Trade Secret Act of 2013" (PRATSA). It was referred to the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations on July 15, 2013. For more on PRATSA, see Kelley Clements Keller, *Congress Makes Great Move in Amending the Economic Espionage Act*, KELLER L. FIRM LLC, http://thekellerlawfirm.com/congress-makes-good-move-in-amending-the-economic-espionage-act (last visited Nov. 13, 2013).

196. R. Mark Halligan, who advocated for a federal civil cause of action companion to the EEA in 2008, points out that enacting such a law would, in effect, create a federal trade secrets statute. This would, in turn, answer a "prevailing argument" in the international community explaining the "[lack of] cooperation from our allies in prosecuting foreign spies." *See* R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 671 n.122 (2008) (quoting Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 477 (2006)).

do more to protect their proprietary information.[197] A civil companion to the EEA, such as PATSIA, would lower the cost to businesses of combating economic espionage and trade secret theft by allowing them to recoup the losses sustained. The United States must take the offensive in this economic war. We must protect our economic position in the global community. As one scientist at Sandia National Laboratory observed: "[W]e didn't win the Cold War because our bombs were superior. We won because our economy was superior."[198]

The United States must continue to *O*bserve the reality of our fight to retain economic superiority in an increasingly competitive world; we must *O*rient ourselves to the "newest ideas and greatest advances in knowledge"[199] and retool our resources in response to the changing nature of our competitors; we must *D*ecide to renew our national commitment to winning; and finally, we must not fear to *A*ct and implement necessary legislative measures to succeed. In short, we must fly in our competitors' "loop," the OODA-Loop.

197. Peter Toren, *Read My Federal Register Comments on Existing Laws Related to the Enforcement of Trade Secrets*, PETERTOREN.COM, http://petertoren.com/comments-to-the-request-by-the-intellectual-property-enforcement-coordinator-for-input-on-the-eea/ (last visited May 23, 2013).

198. FIALKA, *supra* note 2, at 204-05 (quoting J. Pace VanDevender of Sandia National Laboratory in Albuquerque, New Mexico).

199. *New Technologies on Economic Competitiveness: Hearings Before the Subcomm. on Sci., Tech., & Space of the Comm. on Commerce, Sci. & Transp.*, 99th Cong. 125 (1985).