Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 10 | Issue 2 Article 10

2016

Another Bite at the Apple for Trade Secret Protection: Why Stronger Federal Laws Are Needed to Protect a Corporation's Most Valuable Property

Alissa Cardillo

ANOTHER BITE AT THE APPLE FOR TRADE SECRET PROTECTION: WHY STRONGER FEDERAL LAWS ARE NEEDED TO PROTECT A CORPORATION'S MOST VALUABLE PROPERTY[1]

"There are only two categories of companies affected by trade-secret theft: those that know they've been compromised and those that don't know it yet."[2]

ABSTRACT

Trade secrets are one of a corporation's most valuable assets. However, they lack adequate protection under federal law, leaving them vulnerable to theft and misappropriation. As technology advances, it becomes easier and less time consuming for individuals and entities to access and steal trade secrets to a corporation's detriment. Most often these thefts involve stealing trade secrets in an intangible form. Current legislation fails to adequately protect intangible trade secrets, leaving them vulnerable to theft. An amendment to the National Stolen Property Act that encompasses intangible trade secrets would close a loophole that currently exists relating to intangible assets, allowing for unanimity in similar cases of trade secret theft. Moreover, a federal civil statute would provide an overarching framework for civil trade secrets protection and would allow corporations with trade secret theft claims access to federal courts that can provide civil remedies and emergency relief for diverse parties from different states or countries.

INTRODUCTION

Profitable use of resources drives economic development in the United States through creating today's most advanced technologies and medicines.[3] These ideas, technologies, and medicines are classified as United States

---

1. On the eve of publication of this Note, the United States Congress passed, and President Obama signed into law, the Defend Trade Secrets Act, implementing a federal civil trade secrets statute similar to the one called for in this Note. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016). I believe that Congress was correct in passing the bill, for reasons that will be discussed in Part V of this Note. By passing the Defend Trade Secrets Act, Congress has opened the doors of federal courts to trade secret owners with civil trade secrets claims, has allowed for emergency relief through ex parte seizure to prevent further harm to trade secret owners, and provided civil injunction and damage remedies to compensate trade secret owners.

2. David S. Almeling, *Recent Trade Secret Reform – And What Else Needs to Change*, LAW360 (Sept. 23, 2013), http://www.omm.com/files/upload/David%20Almeling%20Article%20RE%20Trade%20Secret%20Reform.pdf.

3. ROBERT J. SHAPIRO & KEVIN A. HASSETT, THE ECONOMIC VALUE OF INTELLECTUAL PROPERTY 2 (2016), http://www.sonecon.com/docs/studies/IntellectualPropertyReport-October2005.pdf.

intellectual property.[4] Intellectual property includes four specific types of property: copyright, trademark, patent, and trade secrets, and each come with its own form of protections.[5] However, while copyrights, trademarks, and patents are protected through federal laws, trade secrets are protected through state and common law, leaving them vulnerable to weaker protection despite their substantial economic value.[6] Trade secrets are classified as any "information, including a formula, pattern, compilation, program, device, method, technique or process."[7] More specifically, to be considered a trade secret, a corporation must: (i) "derive[] independent economic value, actual or potential," from the secret, (ii) make a reasonable effort to maintain the secret's confidentiality, and (iii) not be "readily ascertainable by proper means" to anyone that can economically benefit from the trade secret's value or disclosure.[8] Trade secret misappropriation occurs when an individual or entity obtains a trade secret through "improper means" or discloses or uses a trade secret without the owner's consent.[9]

A corporation's trade secrets are extremely valuable,[10] and today, both insiders and outsiders pose great threats of misappropriation.[11] Outside threats most often stem from "individuals, rival companies, and foreign governments" who steal trade secrets to reap substantial economic benefits.[12] Theft and misappropriation of trade secrets is egregiously harmful to corporations, and in some circumstances, leads to dissolution.[13] In 2008, companies around the world reportedly lost an average of $4.6 million worth of intellectual property because of theft and disclosure through security breaches.[14] A corporation's trade secrets are "commercially valuable . . . [and] kept confidential by companies because, by virtue of their secrecy, they give companies an edge in a competitive marketplace."[15] In addition to affecting the economic stability of a

4. *Id.*

5. BRIAN T. YEH, CONG. RESEARCH SERV., R 43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION 4 (2014).

6. *Id*.

7. UNIF. TRADE SECRET ACT § 1(4), 14 U.L.A. 438 (2005).

8. *Id.*

9. *See generally id.* § 1(2), 14 U.L.A. 438 (2005).

10. U.S. CHAMBER OF COMMERCE, THE CASE FOR ENHANCED PROTECTION OF TRADE SECRETS IN THE TRANS-PACIFIC PARTNERSHIP AGREEMENT 10–13 [hereinafter CASE FOR ENHANCED PROTECTION], https://www.uschamber.com/sites/default/files/legacy/international/files/Final%20TPP%20Trade%20Secrets%208_0.pdf.

11. *See* Dave Drab, *Economic Espionage and Trade Secret Theft: Defending Against the Pickpockets of the New Millennium*, XEROX GLOBAL SERVICES 5–8 (2003), http://www.xerox.com/downloads/wpaper/x/xgs_business_insight_economic_espionage.pdf.

12. YEH, *supra* note 5, at 1.

13. *See* Jon Swartz, *Modern Thieves Prefer Computers to Guns/Online Crime Is Seldom Reported, Hard to Detect*, S.F. GATE (Mar. 25, 1997, 4:00AM), http://www.sfgate.com/news/article/Modern-Thieves-Prefer-Computers-to-Guns-Online-2848175.php.

14. CASE FOR ENHANCED PROTECTION, *supra* note 10, at 11.

15. H.R. REP. NO. 113-657, at 5 (2014).

corporation, misappropriation of trade secrets can have a broader impact on the United States' gross domestic product (GDP).[16] Economic loss resulting from trade secret theft is estimated to be between 1 and 3 percent of the United States' GDP.[17] More specifically, in the United States alone, economic losses suffered from cybercrime were reported to be between $24 and $120 billion.[18] This egregious economic harm faced by corporations and the United States as a result of more frequent trade secret theft, coupled with the economic value of trade secrets, reiterates the need for stronger and more effective legal protection for trade secrets.

The rise in threats and number of successful misappropriations of trade secrets is largely due to new technology.[19] As technology becomes more advanced, it becomes easier and less time consuming for individuals and entities to access and steal trade secrets to a corporation's detriment.[20] Corporations and the U.S. government both derive great economic value from trade secrets.[21] The U.S. Chamber of Commerce estimates the value of trade secrets to publicly traded corporations to be about $5 trillion.[22] Moreover, for many corporations, trade secrets can make up as much as two-thirds of a corporation's information portfolio.[23] For example, companies that are considered "knowledge-intensive" (e.g., scientific and technology companies), trade secrets comprise between 70 and 80 percent of their information portfolios.[24] A study conducted by the National Science Foundation showed that about half of the companies surveyed with research and development activity categorized trade secret protection as the most important form of intellectual property protection.[25] Even those companies without research and development recognized the importance of trade secrets and categorized them as the second most important form of

16. *See* YEH, *supra* note 5, at 14.

17. CTR. FOR RESPONSIBLE ENTER. & TRADE & PRICEWATERHOUSE COOPERS, ECONOMIC IMPACT OF TRADE SECRET THEFT: A FRAMEWORK FOR COMPANIES TO SAFEGUARD TRADE SECRETS AND MITIGATE POTENTIAL THREATS 3 (2014), https://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf [hereinafter ECONOMIC IMPACT OF TRADE SECRET THEFT].

18. *Id.* at 12. Losses may be underestimated due to a difficulty in calculation because of the long lasting effects of trade secret theft. *Id.*

19. *See* Dylan W. Wiseman & Kwabena A. Appenteng, *The Defend Trade Secret Act of 2015: Proposed Legislation Would Open the Federal Courthouse Door for Trade Secret Misappropriation Claims*, LITTLER (Aug. 12, 2015), https://www.littler.com/publication-press/publication/defend-trade-secrets-act-2015-proposed-legislation-would-open-federal.

20. YEH, *supra* note 5, at 1.

21. *See generally* CASE FOR ENHANCED PROTECTION, *supra* note 10.

22. YEH, *supra* note 5, at 14.

23. CASE FOR ENHANCED PROTECTION, *supra* note 10, at 10. An information portfolio is a compilation of data that includes valuable intellectual property such as, customer lists and records, trade secrets, corporate plans, projected sales and financial statements. FORRESTER CONSULTING, THE VALUE OF CORPORATE TRADE SECRETS 3 (2010), https://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf.

24. CASE FOR ENHANCED PROTECTION, *supra* note 10, at 10.

25. *Id*.

intellectual property protection.[26] However, despite their extensive value, trade secrets remain especially vulnerable to theft and misappropriation due to "lackluster legal protection."[27]

As the laws currently stand, the National Stolen Property Act (NSPA)[28] and the Economic Espionage Act (EEA)[29] are the two federal criminal statutes used to protect against trade secret theft. The NSPA prohibits the transporting, transferring, or transmitting of any "goods, wares, merchandise, securities or money" with the knowledge that the same has been stolen.[30] The EEA makes illegal the theft or copying of a trade secret that is "produced for or placed in interstate commerce" with the knowledge that the offense will harm the trade secret owner.[31] However, in two federal Second Circuit cases, *United States v. Aleynikov*[32] and *United States v. Agrawal*,[33] the application of these statutes to the particular facts in each case led to different outcomes. In *Aleynikov*, the Second Circuit overturned both the NSPA and EEA convictions because Aleynikov uploaded, then downloaded, the trade secret in intangible form, which did not constitute "goods, wares, or merchandise" under the NSPA, and was not "produced for or placed in interstate commerce" under the EEA.[34] In contrast, the Second Circuit in *Agrawal* upheld both the NSPA and EEA convictions because Agrawal's printing of the source code and taking it to his home constituted a transfer of "goods, wares, or merchandise" under the NSPA, and the source code was "produced for or placed in interstate commerce" under the EEA.[35] The only difference between these two Second Circuit cases is the intangibility of Aleynikov's uploading and downloading of source code and the tangibility of the paper code that Agrawal printed out and took to his home.[36] This distinction exemplifies the holes in the current federal criminal statutes protecting trade secrets because convictions for trade secret theft should not focus on the tangibility of the trade secret, but rather the fact that a trade secret was stolen to begin with.

In addition to the problem with these criminal statutes, there is no federal civil trade secrets statue allowing corporations to bring private actions in federal court. A federal statute would not only allow trade secret claims to be brought in federal court, but would also provide for civil remedies such as injunctions and damages. Currently, a corporation will

---

26. *Id.* at 11.
27. *Id.* at 11.
28. *See generally* 18 U.S.C. § 2314 (2012).
29. *See generally id.* §§ 1831–1832.
30. *Id.* § 2314.
31. *Id.* § 1832.
32. United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).
33. United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013).
34. *See generally Aleynikov*, 676 F.3d 71.
35. *See generally Agrawal*, 726 F.3d 235.
36. *See generally id.*; *Aleynikov*, 676 F.3d 71.

bring a civil trade secret action in federal court by combining a trade secret claim with its patent claims.[37] Because federal courts have exclusive jurisdiction over patent claims, trade secret claims brought in conjunction with patent claims are litigated in federal court.[38] This practice has caused the amount of trade secret litigation in federal courts to double from 1988 to 1995, double again from 1995 to 2004, and is projected to double a third time by the year 2017.[39] Conversely, state courts have not experienced this increase as litigation in state courts has not doubled in the past fifteen years and is not projected to double for at least the next twenty years.[40] Due to the lack of a uniform federal civil trade secrets statute, when a trade secret claim is brought in federal court, the court must choose and apply a single state's trade secret law, subjecting that case to choice of law issues and leaving litigants unsure of which state's law will be applied in their case.[41] Moreover, courts make it difficult for a corporation to predict the viability of its trade secret claim by applying state laws inconsistently.[42] A federal civil trade secrets statute would provide access to federal courts for stand-alone trade secrets claims,[43] along with consistency and uniformity across the current fifty-state system.[44]

Part I of this Note discusses the economic and noneconomic (i.e., the corporation's reputation, image, goodwill, and competitive advantage) harm corporations face as a result of trade secret theft. Part II explores how the Internet contributes to the exacerbation of trade secret theft. Part III discusses the current federal and state law protections against trade secret theft. Part IV analyzes two federal cases, *United States v. Aleynikov*[45] and *United States v. Agrawal*,[46] both decided by the United States Court of Appeals for the Second Circuit, which, despite substantially similar facts, reached two different outcomes.[47] In addition, this Part highlights the July

37. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 70 (2010) [hereinafter Almeling et al., *Litigation in State Courts*].

38. *See id.*

39. David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 293 (2010).

40. Almeling et al., *Litigation in State Courts, supra* note 37, at 67. State courts are less likely to cite persuasive authority because each state has their own trade secret laws, making federal courts more favorable to plaintiff corporations. *Id* at 73, 76–77.

41. *See* Almeling, *supra* note 2.

42. *See id.*

43. *See* Alden F. Abbott, *Strengthening Property Rights and the U.S. Economy Through Federal Trade Secret Protection*, HERITAGE FOUND. 4 (Jun. 25, 2014), http://thf_media.s3.amazonaws.com/2014/pdf/LM128.pdf.

44. *See* David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 770 (2009) [hereinafter Almeling, *Four Reasons*].

45. *See generally* United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

46. *See generally* United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013).

47. The foregoing analysis on tangibility is specific to the decisions handed down in the Second Circuit.

7, 2015 decision in *People v. Aleynikov*,[48] where the same claims of misappropriation from the earlier federal case against Aleynikov were brought in state court under New York's penal code. Similar to the Second Circuit, the New York State Supreme Court found that the form with which Aleynikov stole the trade secret did not satisfy theft as set out in the penal code. This state case shows that state laws are also insufficient for protecting trade secrets.[49] Finally, Part V offers a solution to the problem with the EEA and NSPA by suggesting an amendment to the NSPA. Further, this Part offers support for, and improvements to, the proposed federal civil trade secrets legislation, the Defend Trade Secrets Act (DTSA), that is intended to provide a uniform federal private action for trade secret misappropriation.

I. TRADE SECRET THEFT'S ECONOMIC AND NONECONOMIC HARM TO CORPORATIONS

During 2000 and 2001, Fortune 1000 companies reported a loss of intellectual property information totaling between $53 and $59 million.[50] Despite the vast economic harm caused by misappropriation of trade secrets, there is no consensus regarding the exact value of corporations' trade secrets.[51] Further, there are several difficulties in measuring the exact effects theft has on business in the United States.[52] Several studies have been conducted to quantify the harm caused by trade secret theft. These studies have found that trade secrets are "fundamental building blocks" that influence "economic growth . . . by enhancing economic security and stability."[53] Furthermore, in the United States, publicly traded companies own about $5 trillion worth of trade secrets.[54] In a proxy study, researchers used "illicit economic activity" to estimate the general effect of trade secret theft.[55] The study found that when compared to the "illicit economic activity" of occupational fraud (i.e., United States tax evasion, narcotics trafficking, black market activities, illicit financial flows, copyright infringement, and software piracy), the loss attributed to trade secret theft ranged from 0.1 percent to 5 percent of the United States' GDP.[56] Another survey showed that a single corporation experienced an economic loss of up

48. People v. Aleynikov, 15 N.Y.S.3d 587, 590 (N.Y. Sup. Ct. 2015).
49. *See generally id.*
50. Drab, *supra* note 11, at 3 (citing ASIS INT'L, TRENDS IN PROPRIETARY INFORMATION LOSS 13 (2007)).
51. *See* ECONOMIC IMPACT OF TRADE SECRET THEFT, *supra* note 17, at 7.
52. *See id*.
53. *Id.* at 2.
54. CASE FOR ENHANCED PROTECTION, *supra* note 10, at 10.
55. ECONOMIC IMPACT OF TRADE SECRET THEFT, *supra* note 17, at 8.
56. *Id.* at 8–9.

to $5.5 million.[57] The survey also showed that the costs of attempted trade secret theft were either comparable or higher in 2005 than 2004.[58]

In one specific instance, Interactive Television Technologies, a corporation that created television devices with data capabilities allowing customers to browse the web on their television sets, experienced an internal network breach where virtual intruders stole trade secrets amounting to an estimated $250 million.[59] The corporation has since gone out of business.[60] In another example, a United States automobile corporation lost an estimated $500 million after hackers broke into the corporation's secure computer network.[61] This substantial loss was due to theft of confidential designs intended for future cars that ended up in the hands of the corporation's competitor.[62] From these examples, it is clear that corporations that fall victim to trade secret theft experience a "loss of competitive advantage" as well as grave economic harm.[63]

In addition to economic losses, corporations reported noneconomic losses in "reputation, image, goodwill, competitive advantage, core technology, and profitability."[64] Trade secret misappropriation deprives a corporation of its competitive advantage by denying the corporation the ability to be the first developer in a specific field.[65] This deprivation also results in harm to the corporation's reputation because of the rapid pace companies enter high technology markets.[66] Misappropriation also affects customer and employee goodwill.[67] Customers often lose confidence in a corporation after instances of trade secret theft resulting in loss of future sales of products.[68] Loss of customers may also occur if the misappropriator is able to replicate and sell the corporation's product for a lower price.[69] The loss of future sales and production harms employee goodwill and causes a decrease in morale due to employees feeling that their work product is "siphoned off by the misappropriator."[70] Furthermore, when corporations implement stronger security measures to protect these trade

57. ASIS INT'L, TRENDS IN PROPRIETARY INFORMATION LOSS 13 (2007), https://foundation.asisonline.org/FoundationResearch/Publications/Documents/trendsinproprietaryinformationloss.pdf [hereinafter ASIS INT'L, TRENDS].

58. *Id.*

59. Swartz, *supra* note 13.

60. *See id.*

61. George J. Moscarino & Michel R. Shumaker, *Changing Times, Changing Crimes: The Criminal's Newest Weapon and the U.S.'s Response,* 16 DICK. J. INT'L L. 597, 603–04 (1998).

62. *Id.*

63. Drab, *supra* note 11, at 2.

64. ASIS INT'L, TRENDS, *supra* note 57.

65. *See* Edmond Gabbay, *All The King's Horses – Irreparable Harm in Trade Secret Litigation*, 52 FORDHAM L. REV. 804, 824–25 (1984).

66. *Id.* at 825.

67. *Id*.

68. *Id*.

69. *See id.*

70. *Id.* at 826.

secrets, employees can react adversely, again decreasing employee goodwill.[71]

When assessing damages for harms in trade secret suits, companies can include actual loss,[72] reasonable royalties, and unjust enrichment.[73] Actual damages are recovered for a corporation's lost revenues, that result from "lost sales of the protected product or service, lost sales of complementary products and services, and price erosion resulting from the misappropriator's entry into the market with a competitive good or service."[74] In successful cases alleging unjust enrichment, the plaintiff is afforded remedies equal to the defendant's "wrongfully gained net profits."[75] Reasonable royalties compensation, a form of damages for actual loss to a plaintiff, is awarded for the use of trade secrets that "a willing licensor and willing licensee" would have negotiated and entered into a contract for prior to the theft.[76] This type of compensation is based on the idea that had the defendant negotiated a contract for a license to use the trade secret, the plaintiff would have profited from that license.[77] The vast economic harm incurred from trade secret theft, along with risks to the competitiveness of the business market, make implementing stronger trade secrets protections necessary.

II. HOW THE INTERNET EXACERBATES THE HARM CAUSED TO CORPORATIONS BY TRADE SECRET THEFT

"If you want to get away with a crime today, do it using a computer."[78] Today, there is no longer a need to enter a corporation's premises to steal its trade secrets.[79] The anonymity of computer theft, coupled with the fact that trade secrets are often more valuable than currency, has resulted in an explosion of computer crime.[80] For example, it has been said that, "[i]f I want to steal money, a computer is a much better tool than a handgun . . . . It would take me a long time to get $10 million with a handgun."[81] A

71. *Id.*

72. Glenn Perdue, *The Broad Spectrum of Trade Secret Damages*, ABA INTELL. PROP. LITIG. COMMITTEE (Apr.18, 2012), http://apps.americanbar.org/litigation/committees/intellectual/articles/spring2012-0412-broad-spectrum-trade-secret-damages.html.

73. Marc J. Pensabene & Christopher E. Loh, *How to Assess Trade Secret Damages*, MANAGING IP (June 2006), http://www.fitzpatrickcella.com/DB6EDC/assets/files/News/attachment359.pdf.

74. Perdue, *supra* note 72.

75. *Id.* It should be noted that plaintiffs cannot receive damages for unjust enrichment if the amount of profits from sales considered is already included in the calculation of actual loss. *Id.*

76. *Id.*

77. *Id.*

78. Moscarino & Shumaker, *supra* note 61, at 604 (citing Jeffery Young, *Spies Like Us*, FORBES (June 3, 1996) at 20).

79. *Id.* at 602.

80. *See id.* at 603–04.

81. Swartz, *supra* note 13.

substantial rise in theft by electronic means has occurred as the Internet has become increasingly important for commerce.[82] Although innovative technology, such as the Internet, is beneficial to corporations because it can make employee operations more efficient, this technology allows a corporation's most valuable information to be susceptible to theft because of its vulnerability to security breaches.[83]

One major challenge that corporations face when developing protections for their trade secrets is hackers.[84] The Internet has helped hackers advance from "formerly annoying, but relatively harmless" individuals, to "accomplished international criminals."[85] Companies generally respond to hacking by continuously increasing their computer security systems.[86] However, these efforts are ineffective as hackers have developed several techniques to successfully breach these heightened security systems.[87] Hacker techniques, and the computer equipment needed to perform these techniques, such as "flash drives, smart phones [and] cloud based storage devices,"[88] are relatively inexpensive and have been extremely successful.[89] The increasing equipment available that can be used to steal trade secrets also makes it easier for employees to engage in trade secret theft.[90]

The relative ease of success and low price of these new technologies have caused computer crimes to increase exponentially.[91] For example, between 1990 and 1995, economic espionage increased 300 percent because the Internet allowed trade secret information to be misappropriated with greater ease.[92] People looking to steal valuable information use the Internet with the comfort of knowing that their identity, location, and affiliation will remain anonymous.[93] An estimate by the Federal Bureau of Investigation reported that approximately 95 percent of "computer intrusions" go unnoticed because hackers know how to successfully and discretely access a system without being discovered.[94] In addition, this anonymity attracts hackers to computer theft because it "softens or even erases" the intruder's feelings of guilt.[95] These factors have led to a substantial increase in electronic trade secret theft.

---

82. *See id.*
83. Drab, *supra* note 11, at 3.
84. *See id.* at 7.
85. Moscarino & Shumaker, *supra* note 61, at 601.
86. *Id.* at 602.
87. *Id.*
88. Wiseman & Appenteng, *supra* note 19, at 1.
89. Moscarino & Shumaker, *supra* note 61, at 603.
90. *See* Wiseman & Appenteng, *supra* note 19, at 1.
91. *See* Moscarino & Shumaker, *supra* note 61, at 603.
92. Drab, *supra* note 11, at 5.
93. *Id.*
94. Moscarino & Shumaker, *supra* note 61, at 604.
95. *Id.*

Although hackers pose a substantial problem to corporations trying to protect their trade secrets, the number one threat of trade secret theft comes from employees inside a corporation.[96] These workers are the "weak link" in information security because they either intentionally leak trade secret information or unwillingly disclose the information to spies.[97] More frequently, a competitor may, through manipulation and deceit, convince an employee to release confidential information that should not be disclosed to the competitor.[98] Another method used to access a corporation's trade secrets is employee recruitment.[99] Employee recruitment occurs when an insider has been obtained by a competitor through bribery and is tasked with acquiring confidential information.[100] The collector corporation, a corporation seeking to steal another corporation's trade secrets, will recruit an insider at the target corporation to steal a trade secret for the collector corporation's benefit.[101] Employee recruitment is targeted at low-level employees because they are easier to bribe than a corporation's officers, or "disgruntled employees" because they may already be looking to harm the corporation as a form of revenge.[102] Once the collector corporation obtains an insider, that individual can easily procure and disclose trade secret information for the collector corporation's benefit.[103]

Even more appalling, some competitor corporations employ hackers to take advantage of security weaknesses in their competitors' computer systems.[104] Corporations that engage in these practices can face penalties for trade secret misappropriation through vicarious liability.[105] The Minnesota Supreme Court, in *Hagen v. Burmeister & Associates*, was the first court to suggest the possibility of bringing a successful vicarious liability claim relating to Minnesota's Uniform Trade Secret Act.[106] Today,

---

96. Drab, *supra* note 11, at 6.
97. Swartz, *supra* note 13.
98. Drab, *supra* note 11, at 7.
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *See id.*
104. *See* Moscarino & Shumaker, *supra* note 61, at 602.
105. Tanya J. Dobash, *Recent Decisions of the Minnesota Supreme Court: Trade Secret Theft & Employer Vicarious Liability In Hagen v. Burmeister & Associates, Inc.*, 29 WM. MITCHELL L. REV. 375, 380 (2002).
106. *Id.* at 384. In the case of *Hagen v. Burmeister*, the Minnesota Supreme Court held that American Agency, Inc., was not vicariously liable for Hagen's solicitation of over 200 Burmeister & Associate customers—in violation of a noncompete and confidentiality agreement classifying customer information as trade secrets—because Burmeister did not present evidence that it was foreseeable for employees of insurance agencies to engage in the misappropriation of trade secrets. Hagen v. Burmeister & Assocs., 633 N.W.2d 497 (Minn. 2001). However, the Supreme Court reasoned that vicarious liability could be imposed on employers for acts "committed within the scope of employment" if the tort is "related to the employee's duties" and "the tort occurs within work-related limits of time and place." *Id.* at 504 (citing *Lange v. Nat'l Biscuit Co.*, 211

under *Hagen*, a corporation can be held liable for an employee's trade secret theft if the employee's misappropriation was related to the employee's scope of work and the theft occurred "within work-related limits of time and place."[107] Another way a corporation can be held vicariously liable is if it is involved in, has knowledge of, or endorses an employee's misappropriation of another corporation's trade secrets.[108]

The rationales for vicarious liability include fairness and economic justifications.[109] The main fairness justification, endorsed by the Minnesota Supreme Court in *Hagen*, is that an employer should bear the costs resulting from employee misconduct if the misconduct is foreseeable and related to the employee's necessary duties because they are part of the "costs of doing business."[110] In other words, it would be unjust for employers to profit from their employees' commendable work without being held responsible for any improper actions employees took to benefit the corporation.[111] The main economic rationale for vicarious liability is based on the concept of risk sharing: the corporation provides "deep pockets" for plaintiffs seeking recovery and a secondary source for damage recovery.[112] An additional justification is that vicarious liability will encourage better hiring and oversight practices by employers, and provides a "financial incentive" to regulate and restrain employees.[113] This is representative of the *Hagen* court's willingness to "enforce corporate responsibility."[114]

III. CURRENT TRADE SECRET PROTECTIONS

Prior to 1996, the most prominent federal statute that protected trade secrets was the Trade Secrets Act enacted in 1948, which made it a crime for federal employees and contractors to disclose any confidential information, including trade secrets.[115] In 1996, Congress passed the EEA[116] to broaden the protection of trade secrets.[117] Congress sought to remedy several concerns about competitors and foreign nations who steal a corporation's trade secrets to gain an economic advantage.[118] Sections 1831 and 1832 of the EEA target economic espionage and theft of trade secrets

---

N.W.2d 783,786 (Minn. 1973)). The court based their justification for vicarious liability on the fact that employee actions are a "cost of doing business." *Hagen*, 633 N.W.2d at 504.

107. Dobash, *supra* note 105, at 407.
108. *See id*. at 380.
109. *Id.* at 394.
110. *Id.* at 394–95.
111. *See id.* at 394–95.
112. *Id.* at 395.
113. *Id.*
114. *Id.* at 396.
115. YEH, *supra* note 5, at 7.
116. *See generally* Economic Espionage Act, 18 U.S.C. §§ 1831–1832 (2012).
117. YEH, *supra* note 5, at 7.
118. *Id.*

respectively.[119] Section 1831 of the EEA provides for imprisonment of fifteen years or a substantial fine for anyone who, with the intent or knowledge that their offense will economically benefit a foreign entity, "steals or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret."[120] Section 1832 of the EEA protects against the theft of trade secrets by imposing a fine or imprisonment on any person who intends to "convert a trade secret" that is "related to a product or service used in or intended for use in interstate or foreign commerce" with the knowledge that the offense will cause harm to the owner and economically benefit third parties.[121] Congress amended the EEA in 2012 to broaden the interstate commerce language to expand the scope of trade secret protection.[122]

The NSPA protects trade secrets by criminalizing the transfer of stolen goods.[123] The NSPA provides criminal sanctions of a fine or imprisonment up to ten years for anyone who "transports, transmits, or transfers . . . any goods, wares, merchandise, securities or money," through channels of interstate commerce with the knowledge that the property is stolen or has been converted through fraudulent means.[124] Furthermore, fines and imprisonment can be imposed on anyone who "with unlawful or fraudulent intent" puts into the stream of interstate commerce any "falsely made, forged, altered, or counterfeited securities" with the knowledge that these materials are "forged, altered, or counterfeited."[125]

In addition to these two federal statutes, states also have their own trade secret laws, which are used by corporations as their primary source of trade secret misappropriation protection.[126] A majority of states drafted and enacted statutes similar to the model set forth in the Uniform Trade Secrets Act (UTSA).[127] The UTSA provides definitions for the terms "trade secret," "improper means," and "misappropriation."[128] It also sets forth equitable remedies for corporations whose trade secrets are misappropriated, such as injunctions, damages for the actual economic loss the corporation suffered and the "unjust enrichment" it causes another party, and attorneys' fees for actions taken in "bad faith."[129]

Although the UTSA establishes a model for states to follow when enacting their own laws, Massachusetts and New York have yet to enact

---

119. *See generally* 18 U.S.C. §§ 1831–1832.
120. *Id.* § 1831.
121. *Id.* § 1832.
122. *See id.* The 2012 amendment is further discussed in Part V as support for the proposition that the National Stolen Property Act should be amended.
123. *See generally id.* § 2314.
124. *Id.*
125. *Id.*
126. YEH, *supra* note 5, at 6.
127. *Id.*
128. *See* UNIF. TRADE SECRET ACT § 1, 14 U.L.A. 438 (2005).
129. *See id.* §§ 2–3.

any version of the UTSA and instead protect their trade secrets primarily through the common law.[130] In addition to its common law, New York uses sections 156.30 and 165.07 of its Penal Code to protect "computer related material" and "scientific material," respectively.[131] New York Penal Code section 156.30 relates to the copying of "computer related material," and makes it a Class E felony to (i) copy computer related material when a person "intentionally and wrongfully deprives or appropriates" an owner of economic value or (ii) copy computer material with the "intent to commit or attempt to commit or further the commission of any felony."[132] New York also seeks to protect a specific type of trade secret, "secret scientific material," through section 165.07 of its penal code, which provides criminal penalties for the unlawful use of any "secret scientific material" with the "intent to appropriate" or make use of the material through the process of "tangible reproduction or representation" of such material.[133]

IV. THE SECOND CIRCUIT'S APPLICATION OF THE EEA AND NSPA

The Second Circuit Court of Appeals' inconsistent application of the EEA and NSPA in *United States v. Aleynikov* and *United States v. Agrawal* illustrates the need for refined statutory language. In April of 2011, the Second Circuit in *United States v. Aleynikov* overturned Sergey Aleynikov's conviction of violating the EEA and NSPA.[134] Aleynikov was a computer programmer who developed source code for Goldman Sachs' high-frequency trading system.[135] A high-frequency trading system is a system that makes large volume trades in securities in a fraction of a second based on a computer algorithm.[136] More specifically, Aleynikov's position at Goldman Sachs required him to write source code for the "infrastructure programs that facilitate the flow of information throughout the trading system and monitor the system's performance."[137] During the creation of the source code, Aleynikov was exposed to secret scientific material that constituted Goldman Sachs' trade secrets, because the material provided economic benefit to Goldman Sachs, was closely safeguarded, and was not readily ascertainable to the public.[138]

---

130. *Latest Updates on Federal Trade Secret Legislation*, TRADING SECRETS (Aug. 26, 2015), http://www.tradesecretslaw.com/latest-update-on-federal-trade-secret-legislation/.

131. *See generally* N.Y. PENAL LAW §§ 156.30, 165.07 (McKinney 2012). It should be noted that these are the statutes at issue later in the case of *People v. Aleynikov*. *See* People v. Aleynikov, 15 N.Y.S.3d 587, 590 (N.Y. Sup. Ct. 2015).

132. N.Y. PENAL LAW § 156.30.

133. *Id.* § 165.07.

134. *See* United States v. Aleynikov, 676 F.3d 71, 73, 75 (2d Cir. 2012).

135. *Id.* at 73.

136. *Id.*

137. *Id.*

138. *Id.* at 74.

Aleynikov's source code knowledge proved to be economically beneficial when he received an offer from Teza Technologies LLC (Teza) to develop their high-frequency trading system in six months' time.[139] Once hired by Teza, Aleynikov's salary more than doubled, increasing from $400,000 per year at Goldman Sachs to $1 million per year at Teza.[140] The issue in this case occurred when Aleynikov, before leaving Goldman Sachs, uploaded Goldman's source code to a server in Germany and subsequently downloaded it to his home computer and other storage devices in New Jersey.[141] He was charged with violation of the EEA because he downloaded a trade secret that was "related to or included in a product that is produced for or placed in interstate or foreign commerce," and the NSPA for transferring "in interstate or foreign commerce any goods, wares, merchandise, securities or money," which he knew were stolen or fraudulently transferred.[142] The source code constituted a trade secret because the source code, as part of the high-frequency trading system, yielded "enormous profits" for Goldman Sachs, Goldman Sachs "went to great lengths" to keep the code confidential, and the code was not for sale or available for licensing.[143]

The Second Circuit reversed Aleynikov's conviction under both the NSPA and EEA.[144] The court concluded that the NSPA does not apply to "purely intangible" property.[145] Under the NSPA, the court reasoned that Aleynikov's upload and subsequent download of the source code did not constitute the stealing of "goods, wares, or merchandise" because he "stole purely intangible property" that was taken in an intangible form, which is not covered by the language of the statute.[146] The court also reversed Aleynikov's conviction under the EEA, finding that the source code as a part of Goldman Sachs' high-frequency trading system was not "produced for nor placed in interstate or foreign commerce" because Goldman Sachs did not intend to sell or license their system to anyone."[147] When interpreting the EEA, the court recognized a jurisdictional limitation that the products must "be 'produced for' or 'placed in' interstate or foreign

139. *Id*.
140. *Id*.
141. *Id*. None of the information downloaded by Aleynikov was his own intellectual property. In fact, Goldman Sachs did not allow Aleynikov to release open-source software, obtained from the Internet, back into open source because Goldman believed it was their property. Michael Lewis, *Did Goldman Sachs Overstep in Criminally Charging Its Ex-Programmer?*, VANITY FAIR (Aug. 1, 2013, 12:00 AM), http://www.vanityfair.com/news/2013/09/michael-lewis-goldman-sachs-programmer.
142. *Aleynikov*, 676 F.3d at 74.
143. *Id.* at 82.
144. *See id.* at 78.
145. *Id.*
146. *Id.*
147. *Id.* at 79, 82.

commerce."[148] The Second Circuit held that because the high-frequency trading system used by Goldman Sachs was not "produced for or placed in interstate commerce," it did not fall within the scope of the EEA.[149]

A little over a year later, the Second Circuit in *United States v. Agrawal* upheld the convictions of Samarth Agrawal under the NSPA and EEA.[150] Agrawal, similar to Aleynikov, was a "quantitative analyst" at Société Générale (SocGen), working with the corporation's high-frequency trading system.[151] SocGen's high-frequency trading system made use of two computer-trading systems that were used to determine which securities to purchase and sell.[152] The team that worked on the high-frequency trading systems generated trades that led to annual revenues of $10 million for SocGen.[153] However, in June of 2009, Agrawal met with Tower Research Capital (Tower), a hedge fund that wanted to create a high-frequency trading system, and Agrawal assured Tower he was capable of assisting them in building a system similar to SocGen's system.[154]

Just after the meeting, Agrawal returned to SocGen in New York, printed out over 1000 pages of source code used in their high-frequency trading system and brought the material back to his apartment in New Jersey.[155] Charged with the same crimes as Aleynikov in *United States v. Aleynikov*, Agrawal was indicted under the EEA for stealing a trade secret that was "produced for and placed in" interstate commerce to provide an economic benefit to himself and a competitor, and under the NSPA for illegally transferring through interstate commerce "goods, wares, merchandise, securities and money" worth more than $5000 with the knowledge that the same was stolen.[156] Agrawal admitted to printing the source code and bringing it back to his apartment and the court upheld the conviction under the NSPA.[157] The Second Circuit reasoned that because he stole the computer source code in tangible form by printing it out on paper, Agrawal's actions fell squarely within the definition of "goods, wares, [or] merchandise" under the NSPA.[158] The court also upheld the conviction under the EEA, stating that the securities traded on the high-frequency trading system were in the stream of interstate commerce, and that the computer code was related to the trading of securities, thereby satisfying the language and jurisdictional limitation of the EEA.[159]

148. *Id.*
149. *Id.* at 82.
150. *See generally* United States v. Agrawal, 726 F.3d 235, 237 (2d Cir. 2013).
151. *Id.* at 237–38.
152. *See id.* at 238.
153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.* at 240.
157. *Id.* at 240.
158. *Id.* at 244.
159. *Id.* at 245–46.

The only factual difference between *United States v. Aleynikov* and *United States v. Agrawal* is the tangibility of the stolen trade secret. The Second Circuit overturned Aleynikov's conviction based on the intangibility of uploading source code, while the same court affirmed Agrawal's conviction based on the tangible theft of the paper code. To draw a distinction on this trivial difference fails to adequately protect trade secrets and secret scientific material because both defendants stole material that derived independent economic value, were kept confidential, and were not readily ascertainable to the public. However, Aleynikov's conviction was overturned because the form in which he stole the trade secret did not constitute "goods, wares or merchandise" under the NSPA. It is problematic that courts, when interpreting the NSPA, are focused on the *form* in which trade secrets are stolen rather than the actual *act* of misappropriation. Therefore, more comprehensive protection against trade secret theft is necessary for maintaining a corporation's economic value because it is the actual theft of the trade secret, whether tangible or intangible, that causes economic harm to the corporation, while benefiting both the criminal and potential competitors who wrongfully acquired the information.

After the Second Circuit overturned Aleynikov's conviction in federal court, the Manhattan District Attorney aired a press release announcing that the State of New York was now charging Aleynikov with, "accessing and duplicating a complex proprietary and highly confidential computer source code owned by Goldman Sachs."[160] In *People v. Aleynikov*, Aleynikov was charged with two violations of New York Penal Code section 165.07, prohibiting the illegal use of secret scientific material, and one violation of New York Penal Code section 156.30, relating to the duplication of "computer related material."[161] Despite a guilty jury verdict with respect to the second count under section 165.07, the court granted Aleynikov's motion to dismiss.[162] Similar to the Second Circuit, the New York State Supreme Court held that no legally sufficient evidence was offered to show that Aleynikov intended to take the code for its economic benefit or value and that the purely intangible form and reproduction of the source code did not fall under the statute, which is specific to "tangible reproductions."[163] The state court's grant of Aleynikov's motion to dismiss shows that in addition to federal law, state law is also insufficient in protecting trade secrets, leaving a corporation's most valuable material with inadequate legal protection.

---

160. Lewis, *supra* note 141.

161. People v. Aleynikov, 15 N.Y.S.3d 587, 590 (N.Y. Sup. Ct. 2015).

162. *Id.*

163. *Id.* The Government argued that, as a policy matter, it did not make sense to allow Aleynikov to "escape criminal liability" simply because he stole the source code in an intangible form rather than print form. *Id.* at 615. This Note argues a similar point, using that fact as a basis for amending the NSPA.

V. A PROPOSED AMENDMENT TO THE NSPA AND FEDERAL CIVIL TRADE SECRETS STATUTE

To better protect a corporation's trade secrets, criminal convictions of individuals that misappropriate trade secrets, such as Aleynikov and Agrawal, should no longer turn on whether the material is taken in tangible or intangible form. Instead, a criminal conviction should be based on an individual or entity taking the trade secret and using it to the owner's detriment, without regard to the form in which the trade secret was stolen. Furthermore, a federal civil statute protecting trade secrets is necessary to provide a uniform private cause of action without preempting current state laws and would allow corporations to seek economic remedies against employers or competitors who misappropriate trade secrets across states with diverse protections.

From a policy perspective, allowing Aleynikov to be freed from criminal liability because he misappropriated a trade secret electronically,[164] while holding Agrawal liable because he physically printed out and took the source code from the corporation[165] does not comport with general fairness. Therefore, in order to remedy the inconsistency between these two similar cases at the federal level, the NSPA needs to be amended to include intangible property in the meaning of "goods, wares, or merchandise."

The purpose of the criminal paradigm is to provide sanctions for wrongful actions because the public considers them to be wrong and they violate a group interest, as opposed to an individual interest.[166] In the case of trade secret theft, the collective harm is twofold, affecting both the corporate community, because of the economic harm caused by trade secret theft, and the United States nationally, because of the decrease in profits resulting from the economic harm to corporations. Furthermore, the harm to corporations comes from the trade secrets being stolen—regardless of the form in which the theft occurs—then disclosed or used in competing businesses, which results in the loss of a corporation's competitive advantage and control of the market.

A. THE AMENDED EEA AND AMENDING THE NSPA

In response to *United States v. Aleynikov*, Congress passed an amendment to the EEA, the Theft of Trade Secrets Clarification Act (TTSCA).[167] United States Senator Patrick Leahy, a notable supporter of intellectual property reform, introduced the amendment because he believed

164. *See generally* United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

165. *See generally* United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013).

166. Kenneth Mann, *Punitive Civil Sanctions: The Middleground Between Criminal and Civil Law*, 101 YALE L.J. 1795, 1806 (1992).

167. *See* Daren Orzechowski, *Amendments to the Economic Espionage Act Broaden Trade Secret Protection*, WHITE & CASE (Jan. 13, 2013), http://www.whitecase.com/publications/article/amendments-economic-espionage-act-broaden-trade-secret-protection#.

there was a need to "help 'American companies . . . protect the products they work so hard to develop.'"[168] The TTSCA simply clarifies the existing EEA language by replacing "a product that is produced for or placed in" with "a product or service used in or intended for use in" interstate commerce.[169] This amendment corrects the Second Circuit's narrow judicial interpretation of the EEA in *Aleynikov*, whereby the provision applied only to products containing trade secrets that were placed in interstate commerce.[170] The very reason the court overturned Aleynikov's conviction under the EEA was because the court determined the stolen code was not "placed in interstate commerce, nor produced to be placed in interstate commerce."[171]

United States Senator Leahy urged the President to sign the TTSCA into law in order to ensure that federal criminal laws provide adequate protection to trade secrets that are related to a product or service that is used in interstate commerce.[172] Representative Lamar Smith, of the House of Representatives also supported the TTSCA and recognized the need to close the gap in federal law that was exposed in the Second Circuit's decision in *Aleynikov*.[173] In passing this amendment, Representative Lamar Smith believed the government was implementing a necessary adaptation to the digital age.[174] Similarly, Representative Jackson Lee noted the need for protection of trade secrets that are part of software that is used internally rather than commercially.[175] The TTSCA was successfully enacted in 2012.[176]

Despite the TTSCA's amendment of the EEA expanding the interstate commerce language,[177] the EEA and NSPA still do not specifically encompass intangible property. Therefore, in order to sufficiently protect trade secrets, the NSPA should be amended to explicitly cover the transfer or transporting of new intangible trade secrets and methods used to misappropriate trade secrets that did not exist in 1934. This Note proposes an amendment to the NSPA's language because it covers only "goods, wares, merchandise, securities or money," leaving out the transfer of

168. Robert D. Jurrens, *Fool Me Once: U.S. v. Aleynikov and the Theft of Trade Secrets Clarification Act of 2012*, 28 BERKELEY TECH. L.J. 833, 848 (2013) (citation omitted).

169. Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012).

170. *See* 158 CONG. REC. S6878-03, 2012 WL 5932548 (2012) (statement of Sen. Leahy).

171. *Id.* Had Aleynikov been convicted under the amended language of the EEA, it is likely that his conviction would have been upheld.

172. *Id.*

173. 158 CONG. REC. H00000-52, 2012 WL 6605649 (2012) (statement of Rep. Smith).

174. *Id.*

175. Jurrens, *supra* note 168, at 849 (citing 158 Cong. Rec H00000-52, 2012 WL 6605649 (2012) (statement of Rep. Jackson Lee)).

176. Orzechowski, *supra* note 167.

177. *See* Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, § 2, 126 Stat. 1627 (2012).

intangible property, and in turn, excluding many trade secrets from legal protection.[178] Because courts are reluctant to alter laws passed by Congress,[179] it is Congress's responsibility to remedy any unfairness or inconsistencies resulting from the application of its laws. Currently, the NSPA only punishes individuals for stealing "goods, wares, merchandise, securities or money."[180] As seen in *United States v. Aleynikov*, this language does not cover theft of trade secrets through intangible means, such as uploading and downloading source code,[181] or any future intangible means of theft created as technology evolves. Without explicitly encompassing theft of intangible property in the language of the NSPA, trade secrets in intangible form are subject to judicial interpretation of the NSPA, which has resulted in a lack of legal protection for trade secret theft. The statute should be amended to punish whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise securities, money, or intangible assets of the value of $5000[182] or more, knowing the same to have been stolen, converted or taken by fraud.

Furthermore, Congress should define an intangible asset in the NSPA based on the definition of trade secrets in the UTSA. The amended NSPA should define an intangible asset as, "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."[183] It would then be left to the courts to decide if a corporation both derives economic value and provides means of protection to the intangible asset at issue in a particular case. By defining intangible assets using the UTSA's definition of trade secrets, Congress would encompass intangible trade secrets not currently covered by the NSPA, while also not overreaching because the language would not cover all intangible assets, only those that meet the three requirements for trade secrets set forth in the UTSA.

The supporting arguments for this amendment are similar to the supporting arguments made by Congress when they first enacted the EEA in 1996. The EEA was proposed primarily as a response to "theft of proprietary economic information."[184] The House of Representatives argued that the preexisting federal criminal statues being used to combat crimes

178. *Compare* Economic Espionage Act, 18 U.S.C. § 1832 (2012), *with* National Stolen Property Act, 18 U.S.C. § 2314 (2012).

179. *See* People v. Aleynikov, 15 N.Y.S.3d 587, 630 (N.Y. Sup. Ct. 2015).

180. 18 U.S.C § 2314.

181. *See generally* United States v. Aleynikov, 676 F.3d 71, 73, 75 (2d Cir. 2012).

182. *Id.*

183. UNIF. TRADE SECRET ACT § 1(4), 14 U.L.A. 438 (2005).

184. 142 CONG. REC. H10460, H104601 (daily ed. Sept. 17, 1996) (statement of Rep. Buyer).

relating to "theft of proprietary economic information" were drafted several decades ago and that at the time of drafting, no one could have foreseen the type of intellectual property that now needs protection.[185] Similar arguments apply for the amendment of the NSPA. The statue was passed in 1934 before advances in technology and the rise of the Internet. It is difficult to imagine in 1934 members of Congress anticipating not only the existence of a computer network, but one that puts a corporation's intangible assets at risk. However, now that Congress is aware of this new technology, it is appropriate to update the NSPA to coincide with these significant technological advances.

Another argument made in favor of enacting the EEA in 1996 was that as a creative nation, the U.S. government must have the appropriate "legal tools" to protect its innovations.[186] The Department of Justice alerted Congress to a loophole in the federal statutes used to protect trade secrets prior to 1996, noting that they were insufficient in protecting the theft of intangible property. Congress responded by acknowledging that as the nation moves toward a technologically advanced economy, most economic assets that need protection, such as trade secrets, would also become intangible.[187] A similar loophole is found in the NSPA because it only applies to "physical property" and not intangible trade secrets.[188] The continuous move toward a technological economy where more assets are becoming intangible requires an amendment to the NSPA that covers the theft of these intangible assets.

Those who opposed the 1996 enactment of the EEA claimed that the statute, if passed, would infringe on business practices such as employee mobility,[189] which is an argument that Congress would likely face when amending the NSPA. Employee mobility is the ability of skilled employees to leave a current job and begin working for another corporation, applying their skills and knowledge to their work at the new corporation.[190] The fear is that employees will be discouraged from moving to another company because employees would naturally take knowledge and experience from their former job with them, and that this knowledge may unintentionally include the knowledge of trade secrets.[191] However, safeguards against infringement on employee mobility already exist in the intent requirement included in the NSPA. Similar to the EEA, the intent requirement in the NSPA allows for employee mobility because it only criminalizes theft of

185. *Id.*
186. *Id.*
187. *See id.*
188. *See generally id.*
189. *See id.*
190. Charles T. Graves & James A. Diboise, *Do Strict Trade Secret and Non-Competition Laws Obstruct Innovation?*, 1 ENTREPRENEURIAL BUS. L.J. 323, 324 (2007).
191. *See* 142 CONG. REC. H10460, H10461.

trade secrets with the knowledge that the trade secret was stolen,[192] and does not criminalize the use of trade secrets when there is no knowledge that they were stolen,[193] or that are not encompassed by the UTSA definition of trade secrets.[194] Further, the current intent requirement would apply to theft of all property—tangible and the added intangible, which would be covered under the proposed amendment to the NSPA—thus avoiding infringement on employee mobility or competition. A supporting argument for amending the NSPA is similar to an argument made by Chuck Schumer, United States Senator and Vice Chair of the Democratic Conference,[195] in support of the 1996 enactment of the EEA, who stated, "[w]e cannot . . . afford to let this loophole remain in our law. American inventiveness is the key to our economy."[196]

B. A PROPOSED FEDERAL CIVIL TRADE SECRETS STATUTE

In addition to amending the NSPA to protect trade secret misappropriation, Congress should pass a federal civil trade secrets statute similar to the DTSA of 2015, House of Representative Bill H.R. 3326,[197] and Senate Bill S. 1890,[198] to offer corporations a federal civil remedy for the misappropriation of their trade secrets. The basic purpose of the implementation of civil sanctions is to afford individuals who have been harmed a compensation remedy.[199] If corporations lose economic value through trade secret theft, it follows that the corporation should have an economic remedy against the employee or defendant corporation, and upon proving a case of misappropriation, be awarded damages to be made whole again.[200]

There have been several steps taken by the federal government to implement a federal civil trade secrets statute, however, a corporation today is still left without a federal civil cause of action to pursue when its trade secret has been misappropriated.[201] The U.S. government issued a report entitled *The Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, describing its intentions to "vigorously combat" theft of trade secrets that could be disclosed to foreign governments or corporations that may derive economic benefit from their disclosure.[202] Included in this report

192. National Stolen Property Act, 18 U.S.C. § 2314 (2012).
193. 18 U.S.C. § 2314.
194. *See generally* UNIF. TRADE SECRET ACT § 1 (4), 14 U.L.A. 438 (2005).
195. *See About Chuck*, U.S. SENATE, http://www.schumer.senate.gov/about-chuck (last visited Feb. 5, 2016).
196. 142 CONG. REC. H1046001, H10461.
197. Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. (2015).
198. Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. (2015).
199. Mann, *supra* note 166, at 1808.
200. *See id.* at 1809–10.
201. *See* Wiseman & Appenteng, *supra* note 19.
202. YEH, *supra* note 5, at 17.

are several initiatives to combat trade secret theft, including enhancing domestic law enforcement by making trade secret theft a priority, and improving U.S. trade secrets legislation.[203] In addition to this report, the Senate proposed the DTSA of 2014, and the House of Representatives introduced a companion bill, the Trade Secrets Protection Act of 2014, to provide further protection of domestic trade secrets.[204] The DTSA of 2015 is substantially similar to the 2014 proposed bills,[205] also allowing for ex parte seizure of property upon a hearing showing that this seizure is necessary to avoid disclosure of trade secret information.[206] The DTSA of 2015 also sets a statute of limitations of five years and allows for remedies, including injunctions, damages for actual loss and for unjust enrichment, increased damages for willful and malicious misappropriation, and attorney's fees if a claim is made in bad faith.[207] Finally, the DTSA of 2015 includes definitions for misappropriation and improper means that are similar to the definitions set forth by the UTSA.[208]

The federal trade secrets statute called for in this Note is substantially similar to the DTSA of 2015 that has been proposed by Congress. The federal civil statute should allow for civil seizure, where the court can issue an ex parte order to seize the stolen trade secret. However, to protect property rights, there should be several prerequisites for the issuing of the order. These requirements should include that before issuance, a court must find that: (i) any other order available for issuance under the Federal Rules of Civil Procedure (FRCP) will not successfully preserve the confidentiality of the trade secret, (ii) there will be immediate harm if the seizure is not ordered, (iii) the benefit of granting the order outweighs the harm that would result from denying it, (iv) the information is a trade secret and the person will likely misappropriate the secret if it is not seized, (v) the party can prove that the trade secret in question belongs to them, and (vi) the defendant may make the material inaccessible if it is not seized.[209] The justification for this order is that the court, by seizing the trade secret, can preserve evidence and prevent additional harm to the corporation from disclosure of the trade secret.[210] This preservation of evidence justification is similar to courts allowing for the seizure of property during a search incident to arrest under the Fourth Amendment of the Constitution.

A federal civil trade secrets statute should also include damages at equity and at law. An injunction remedy should be included in the statute to

---

203. *See id. at* 17–18.
204. *See generally id.* at 28, 31.
205. Trade Secret Protection Act of 2014, H.R. 5233, 113th Cong. (2014); Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014).
206. H.R. 3326, S. 1890.
207. *See* H.R. 3326, S. 1890.
208. *See* H.R. 3326, S. 1890.
209. H.R. 3326.
210. Abbott, *supra* note 43.

prevent any further disclosure or harm that would result from the trade secret theft. Money damages should be available as a remedy to compensate the corporation for the misappropriation of a trade secret, including any actual or potential loss incurred by the corporation. Monetary damages would also compensate the corporation for the unjust enrichment to the person who engaged in the theft or a competitor who receives the benefits of the trade secret. These damages would prevent a hacker or employee misappropriator from benefiting as a result of the theft of a corporation's trade secret. Punitive damages should be available to deter trade secret theft by awarding additional damages for any willful or malicious misappropriation. Finally, attorney's fees should be available for any claims brought in bad faith, which would help alleviate the possibility of a court becoming backlogged with frivolous trade secret cases.[211] By providing damages and injunctive relief, federal trade secrets legislation would limit the rewards from misappropriation of trade secrets, which would decrease incentives to steal trade secrets and thereby inhibit the growth of trade secret theft in the United States.[212]

In some cases of trade secret theft, excessive civil damages could have the perverse effect of actually hurting the plaintiff's ability to recover losses. Where civil damage awards are significantly large, the defendant may not be able to fully compensate the corporation's losses, making these damages insufficient to remunerate the corporation and deter future trade secret theft.[213] However, as the United States Chamber of Commerce stated, "a combination of robust civil enforcement as well as criminal penalties is important for protection of trade secrets."[214] Therefore, where a corporation cannot be made whole through civil remedies, "strong criminal sanctions can both complement and fill gaps in existing civil remedies."[215] An example of this strategy is *United States v. Kolon Industries Inc.*, a case from 2012, where federal prosecutors indicted a South Korea-based corporation for "conspiring to steal trade secrets" from an American corporation, with the indictment carrying a loss of $225 million.[216] In addition to this substantial civil award, if found guilty, the South Korean executives would face up to thirty years in prison for their crimes.[217] The same American corporation also filed a civil suit, *E.I. du Pont de Nemours and Company v. Kolon Industries Inc.*, where it was awarded $920 million and an injunction.[218] Moreover, in a case where a single employee may not

211. *See* H.R. 3326.
212. Abbott, *supra* note 43, at 4.
213. *See* CASE FOR ENHANCED PROTECTION, *supra* note 10, at 13.
214. *Id.*
215. *Id.* at 18.
216. *Id.* at 20.
217. *Id.* at 21.
218. *Id.*; *see also* E.I. du Pont de Nemours and Co. v. Kolon Indus. Inc., 803 F. Supp. 2d 469 (E.D. Va. 2011).

be able to pay civil damages and criminal sanctions are not sought, a plaintiff can bring a claim for vicarious liability requiring the corporation that benefited from the stolen trade secret, which often has "deep pockets," to pay a portion of damages.[219]

A federal civil statute would also provide companies with access to federal courts,[220] without preempting current state law.[221] Trade secrets are the only significant type of intellectual property not governed by federal law.[222] Currently, federal law only governs trademarks, copyrights, and patents,[223] with federal courts having exclusive jurisdiction over patents.[224] Trade secrets, on the other hand, are governed by state and common law.[225] Therefore, the next logical step in the protection of trade secrets is the enactment of a federal civil trade secrets statute to accompany the criminal sanctions set forth in the NSPA and EEA.[226] The principle of federalism, which grants both the state and federal government the right to exercise their own powers,[227] would allow both federal and state trade secrets laws to coexist. An example of federal and state intellectual property laws coexisting is with trademarks, where the Lanham Act, a federal statute, and state trademark laws have successfully coexisted for decades.[228] A federal statute would also provide for additional civil remedies, such as injunctions, allow for the preservation of evidence and further prevention of disclosure through ex parte seizures, while also providing additional compensation to American corporations for the economic harm resulting from the theft and misappropriation of trade secrets.[229] These remedies are consistent with those offered by federal law for patent, copyright, and trademark.[230]

The lack of a federal civil statute to protect trade secrets is problematic because the absence of such a statute has allowed for inconsistencies in the application of trade secrets legislation vital to the success of American corporations.[231] A federal trade secrets statute would remedy the lack of uniformity that exists in current state laws.[232] These state laws are inconsistent and confusing because state legislatures modify their trade

219. Dobash, *supra* note 105, at 395.
220. *See* Abbott, *supra* note 43, at 4.
221. *See id.*
222. Almeling, *Four Reasons*, *supra* note 44.
223. *Id.*
224. Almeling et al., *Litigation in State Courts*, *supra* note 37, at 73.
225. *See* Almeling, *Four Reasons*, *supra* note 44, at 770.
226. *Id.*
227. *See generally* 20 N.Y. JUR. 2D CONST. LAW § 108.
228. Abbott, *supra* note 43, at 4.
229. *See* Press Release, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets (July 29, 2015), http://www.hatch.senate.gov/public/index.cfm/releases?ID=ad28f305-f73a-4529-84ba-ad3285b09d6e.
230. *See id.*
231. *See* Almeling, *supra* note 2.
232. Almeling, *Four Reasons*, *supra* note 44, at 770.

secret statutes often and state courts often apply these laws inconsistently across cases.[233] As stated by Congressman Jerrold Nadler, "[a] fifty-state system does not work well in our increasingly mobile and globally interconnected world."[234]

Some scholars argue that a federal civil trade secrets statute would provide more confusion because it does not preempt state law,[235] but would instead overlap state law.[236] However, the very problem in the absence of a federal law is the lack of uniformity that would in fact be remedied by a federal law.[237] The uniformity that would be accomplished by a federal trade secrets law is important because it reduces uncertainties that arise out of varying state laws.[238] Further, the fact that some trade secrets would be left uncovered by federal law because they do not involve a "product or service" in interstate commerce,[239] is not a persuasive argument to abandon the federal trade secrets bills altogether. First, some of these trade secrets may still be subject to federal jurisdiction under diversity jurisdiction or supplemental jurisdiction. More importantly, simply because a slight minority of trade secrets that are not involved in interstate or foreign commerce[240] would not be covered under the federal law does not mean that the majority of trade secrets that would be covered should not be granted stronger federal protections.

Another problem with the differences in state law is the issue arising from the choice of law.[241] The lack of a federal civil trade secrets statute that provides uniform protection can prevent trade secret owners from "vindicating their rights" when theft occurs across state lines or if the defendant attempts to flee the country.[242] In cases where the plaintiff corporation and the defendant who stole the corporation's trade secret reside in different states, the corporation would be uncertain about which state's law would apply.[243] In federal court, it is clear that federal law would apply and companies can look to precedent (once developed) to determine the viability of their case prior to a trial. Similarly, increasing employee

233. Almeling, *supra* note 2.

234. Press Release, Jerrold Nadler, Representative, U.S. House of Representatives, Rep. Nadler on Protecting Trade Secrets of American Companies (June 24, 2014), http://nadler.house.gov/press-release/rep-nadler-protecting-trade-secrets-american-companies.

235. *See* Letter from David Levine et al., Professors Intellectual Property Law, to Congress Opposing Trade Secret Legislation (Aug. 26, 2014), http://infojustice.org/wp-content/uploads/2014/08/Professor-Letter-Opposing-Trade-Secret-Legislation.pdf.

236. Bill Donahue, *6 Big Problems With Federalizing Trade Secrets Law*, LAW360 (Sept. 12, 2014), http://www.law360.com/ip/articles/575060.

237. *See* Abbott, *supra* note 43, at 4.

238. *Id.*

239. Donahue, *supra* note 236.

240. *Id.*

241. Almeling, *supra* note 2.

242. Abbott, *supra* note 43, at 3.

243. *See* Almeling, *supra* note 2.

mobility, where employees change jobs more frequently, often moving to different states exacerbates the choice of law problem, making it difficult for corporations to effectively protect their trade secrets from theft and misappropriation nationwide.[244] Employee mobility increases the risk of trade secret misappropriation by creating an opportunity for a past employee to use the former employer's trade secret in his or her new position in a different state.[245] This again creates a choice of law issue where the corporation and employee reside in different states.[246] However, granting access to federal courts under a federal civil statute can mitigate these issues because one uniform federal law would apply and federal courts have a greater ability to "facilitate discovery, serve defendants or witnesses, or prevent a party from leaving the country."[247]

Although choice of law issues may still arise when trade secret claims are intertwined with employment and contract claims governed by differing state law,[248] such choice of law issues would still exist in these cases even in the absence of a federal civil statute. Therefore, a choice of law issue for employment or contract claims is an unpersuasive argument for rejection of a federal law with several benefits specifically when federal courts are better suited to deal with issues arising across state and national boundaries, because they often deal with diverse litigants.

A benefit of a federal civil trade secrets statute is that it provides "emergency relief."[249] Although it can be argued that a federal trade secrets statute would result in greater risk of "accidental disclosure of the trade secrets"[250] by providing for emergency relief, a federal court is authorized to seize the trade secret to prevent its promulgation where irreparable injury would occur,[251] therefore mitigating any harm to the corporation resulting from the disclosure of the trade secret. Furthermore, the federal civil statute would allow for this relief to be ex parte, where there is no requirement for the "presence or participation" of the party opposing the seizure.[252] The arguments that ex parte relief can inhibit competition[253] and be abused[254] are also unpersuasive. There are several safeguards to prevent the issues surrounding ex parte relief in both the DTSA and the statute proposed in

244. *See* CASE FOR ENHANCED PROTECTION, *supra* note 10, at 13.
245. *See id.*
246. Almeling, *supra* note 2.
247. YEH, *supra* note 5, at 20.
248. *See* Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 364 (2015).
249. Wiseman & Appenteng, *supra* note 19, at 2.
250. *See* Levine et al., *supra* note 235.
251. Wiseman & Appenteng, *supra* note 19, at 2.
252. *Id.*
253. Michael Weil & Johanna Jacob, *Defend Trade Secrets Act of 2015 Faces Criticism 2.0*, ORRICK: TRADE SECRETS WATCH (Sept. 28, 2015), http://blogs.orrick.com/trade-secrets-watch/2015/09/28/defend-trade-secrets-act-of-2015-faces-criticism-2-0/.
254. Donahue, *supra* note 236.

this Note, such as requiring an adequate showing of necessity by the applicant, a showing that "immediate and irreparable injury will occur," and a cost-benefit analysis concluding that the benefit of granting the seizure will outweigh any potential harm to third parties.[255] In addition to these safeguards, a judge can prevent and punish any instances of "foul play."[256] The safeguards against infringing on competition and business practices, coupled with the benefits of stronger protection and emergency relief, makes the passing of a federal civil trade secrets statute the best option to afford trade secrets the appropriate legal tools needed to enforce a corporation's right to protect their trade secrets and preserve their economic value to the corporation and the United States.

CONCLUSION

With the growth of the Internet and the explosion of cybercrime, trade secrets have become increasingly vulnerable to theft, increasing the need for greater legal protection. The NSPA needs to be amended to better protect trade secrets by encompassing the intangible trade secrets that contribute to a substantial amount of a corporation's economic value and United States GDP. By amending the NSPA, a loophole that currently exists relating to intangible assets would be closed, allowing for unanimity in similar cases of trade secret theft by punishing the theft of the trade secrets and the subsequent misappropriation of those trade secrets, rather than focusing on the form in which the trade secrets were stolen.

Moreover, a federal civil law should be passed to provide an overarching framework for civil trade secrets protection to allow corporations with trade secret theft claims access to federal courts. Federal courts can provide civil remedies, such as injunctive relief and damages, to corporations who have suffered economic harm because of trade secret theft, as well as emergency relief, such as ex parte seizure, to prevent further irreparable injury to the corporation. Finally, the federal court system is better suited to deal with diverse parties from different states or countries and those defendants who attempt to flee the country in an effort to escape liability for their actions. With these two statutes in place, a corporation's most valuable economic property would be better protected,

Alissa Cardillo[*]

255. Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2 (2015).

256. Donahue, *supra* note 236.

* B.A., University at Albany, 2014; J.D. Candidate, Brooklyn Law School, 2017. I would like to thank everyone on the *Brooklyn Journal of Corporate, Financial & Commercial Law* for their time and effort in helping prepare this Note for publication. A special thanks to Professor Christina Mulligan for her introduction to this topic and assistance throughout the research and writing process. Finally, I want to thank my family and friends, particularly my parents and brother, for their constant love and support.