The Growing Concern Regarding US Corporate Trade Secrets

By Stephen Anderson

I. Introduction

Globalization has produced many benefits for United States corporations, but a significant detraction has been the emergence of trade secret theft. As technology advances, trade secret theft has become an even more persistent threat in the general marketplace. There are various ways trade secret theft can occur, but it is increasingly common for the theft to involve cyberspace, especially as these corporations expand into foreign markets. Consequently, Congress has taken a significant interest in curbing trade secret theft, as is evidenced by the various proposals before them today. These proposals offer varying solutions to trade secret theft, which range from creating a private cause of action in federal courts to specifically targeting foreign entities and governments engaged in cyber espionage, such as Chine. Before analyzing a number of current proposals, it is necessary to define trade secrets and understand their current legal status in the intellectual property landscape.

II. Trade Secret Definition

It is first essential to identify exactly what qualifies as a trade secret, which has been notoriously difficult to define. A simple definition focuses on the presence of four elements: information, economic value (actual or potential), said information cannot be generally known, and it must be the subject of reasonable efforts to maintain its secrecy. [1] However, these four elements can encompass quite a broad spectrum of information. A U.S. federal court has described it as:

> [A trade secret is] really just a piece of information (such as customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret by

> executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort. [2]

Furthermore, the U.S. Supreme Court has stated that in order for information to be a trade secret it must meet minimal standards of novelty and inventiveness. [3] This threshold is necessary as to avoid over-extending trade secret laws, i.e. allowing trade secret laws to protect matters that are considered general or common knowledge in the industry. [4] However, the Supreme Court goes on to state that a company may have a property interest in a trade secret, which is defined by the extent the owner protects said trade secret and its ability to provide an economic advantage. [5] This creates a rather expansive standard for information that can qualify as a trade secret, as long as the owner takes certain steps to protect economically advantageous information. [6] It is apparent that although the judiciary has laid out standards by which to determine if information qualifies as a trade secret, in the end, it is still quite subjective.

With an understanding of trade secrets, it is just as important to define a misappropriation of a trade secret. Simply put, it is a tort that usually occurs in one of three ways. [7] First, a trade secret is misappropriated when it is acquired through improper means, such as theft, espionage, or bribery. A second way in which a trade secret is misappropriated occurs through a breach of confidence. [8] Misappropriation of this nature commonly takes places when an employee improperly discloses a previous employer's trade secret. [9]. Lastly, a misappropriation takes place if a trade secret has been disclosed with knowledge that it was improperly obtained. [10] It is necessary to point out that analyzing publicly available information and independently developing the subject matter of a trade secret is not a misappropriation. There must be some

improper means regarding the disclosure or use of a trade secret in order for a misappropriation to have taken place. [11]

Before discussing current trade secret law, it is necessary to quickly distinguish trade secrets from their intellectual property partners. Intellectual property includes four broad categories of subject matter, each covered by a different field of law, which consist of copyright law, trademark law, patent law, and trade secrets law. Significantly, trade secrets law is the only form of intellectual property law that is primarily governed under state law. [12] Consequently, when compared to the other three fields of intellectual property law, trade secret owners have more limited legal options when they seek to enforce their rights. Specifically, current laws do not provide trade secret owners with a private right of action in federal court, which the other three fields of intellectual property law enjoy. [13]

III. Current Trade Secret Law

Trade secret laws are also distinct in the field of intellectual property due to their relatively recent formation compared to the other three field of intellectual property. They evolved out of common law torts in the middle of the 19th century and a series of legal rules governing employment relationships. [14] Copyright law did not protect trade secrets and patent law, namely due to their standards, did not provide protection to trade secret owners. [15] They were then officially recognized in two sections of the Restatement of Torts. One section discussed the subject matter of trade secrets, while the second spelled out the elements of their misappropriation. [16] Then the Uniform Trade Secrets Act (UTSA) of 1979 became the "first comprehensive effort to codify the law of trade secrets protection." [17] Finally, the federal government provided trade secret protection with the Economic Espionage Act (EEA) of 1996.

As mentioned earlier, trade secrets law is grounded in state law and that is where trade secret owners currently find their greatest amount of protection. The UTSA codifies the basic principles of common law trade secret protection. [18] A trade secret owner can enforce their rights by filing a civil suit in state court against the individual or organization that allegedly misappropriated the trade secret. The remedies that are available include compensatory damages, injunctive relief, and punitive damages. Additionally, a few states have criminal laws under which state prosecutors may bring criminal charges against defendants in trade secret cases. [19]

The most significant federal protection that has been afforded to trade secret owners is the EEA. [20] This legislation grew from the increasing concern regarding international and domestic economic espionage against United States businesses. [21] Therefore, the legislature enacted the EEA in order to establish a broader federal scheme that protects United States trade secrets. The EEA has a rather expansive trade secret definition that works as a threshold for triggering a violation. [22] A violation will fall under one of two criminal offenses: the theft of a trade secret for the benefit of a foreign entity ("Section 1831") and trade secret theft intended to confer an economic benefit to another party ("Section 1832"). [23] There are a number of fundamental differences between Section 1831 and 1832, but namely Section 1832 may apply when any trade secret theft occurs, as long as the theft economically benefitted, or intended to, someone other than the trade secret owner. [24]

When looking at the language of Section 1831, it is clear that this section is focused on addressing Congress's fear of foreign government's attempts to acquire United States businesses trade secrets, rather than foreign or domestic corporations attempting the same. This is apparent when defining the term "benefit," which according to the EEA encompasses any economic, reputational, strategic, or tactical gain that derives from a foreign espionage effort. [25]

Furthermore, a "foreign entity" encompasses any "entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." [26] Therefore, it becomes quite clear that Section 1831 is aimed at foreign governments.

However, despite its best intentions, implementation of Section 1831 has been quite difficult. The challenge revolves around proving that the theft was meant to benefit a foreign entity or government and acquiring the necessary information to prove such a benefit. [27] Namely, the "availability of foreign evidence and witnesses, diplomatic concerns, and the presence of classified or sensitive information required to prove the foreign nexus element." [28] Simply put, there is a significant obstacle regarding the production of sufficient evidence that proves a foreign government benefited from the trade secret theft. To that extent, since the enactment of the EEA, there have reportedly been only 125 indictments and 10 convictions. [28] Therefore, there are a number of legislative proposals that have been introduced in Congress directly related to updating and improving trade secret protection.

IV. Current Congressional Proposals

This brings us to the current discussion in trade secrets law regarding the importance of a federal civil cause of action in trade secrets law. There are certain aspects of the argument that should be taken as fact. At the moment, the relief under federal criminal actions is not sufficient for proper trade secrets protection. Yet, there is need to look at the realities of this situation. There seems to be a serious logistical obstacle of how the United States can actually stop foreign trade secret thieves from sharing and disseminating trade secrets, especially once they are outside of the United States borders. [29]

Advantages for a federal civil cause of action are numerous though. Policy-wise, it would create uniformity that would ease implementation and creation of procedural and substantive

standards. [30] Moreover, it will fix the fundamental trade secret difference that currently exists across the states, namely the definition of a trade secret and its misappropriation. [31] Even though it could be argued that neither is adequately equipped to protect trade secrets, the federal court is seemingly the lesser of the two evils. Furthermore, cooperation from international jurisdictions has been impeded partially due to the lack of a federal statute that can be referenced when discussing trade secret protection. [32] Finally, and possibly the most practical element of this discussion, one that even detractors of the federal civil cause of action would concede, is the fact that the current system is hampering United States companies and the economy. [33] Some change, seemingly any change, is necessary in order to better address the growing problem of trade secrets theft. The following two proposals provide separate approaches on how to best improve U.S. trade secret protection that have been introduced in Congress.

a. S. 884, Deter Cyber Theft Act

Introduced by Senator Carl Levine, the DCTA would require an annual report to Congress that identifies foreign countries that engage in economic or industrial espionage in cyberspace with respect to U.S. trade secrets. [34] The Director of National Intelligence would compile this list, which would be prioritized based on level of espionage each foreign country has allegedly conducted. [35] Additionally, the report must identify the technology or proprietary information that is being targeted, goods and services made or provided using said technology or proprietary information, and the foreign entities that are taking part in the espionage. [36] The President then has the option to embargo any goods produced or exported by the foreign entities he finds are engaged in intellectual property theft, if he believes that such an exclusion is necessary to enforce intellectual property rights. [37]

The DCTA provides the U.S. and its companies with two appealing outcomes. First, consolidating the information regarding trade secret misappropriation and the actors that consistently take part it in would seemingly allow the U.S. companies to improve their preventative measures regarding trade secrets. Additionally, it would allow the President to take substantive steps to curb these foreign countries behavior, by directing the U.S. Customs and Border Control to exclude their goods from entry. [38] However, there is a question regarding the implementation of the DTCA. Specifically, the Act could run into many of the same problems that hamper Section 1831 of the EEA. To that extent, it would seem likely that the President would err on the side of caution when implementing the powers given to him by the DTCA. For example, if the President were to mistakenly embargo goods from a foreign country based on the actions of an independent entity, the ramifications could be significant. Nonetheless, the information compilation proposed by the DTCA is seemingly a necessary step in order to improve the preventative measures U.S. companies take to protect their trade secrets.

b. S. 1770, the Future of American Innovation and Research (FAIR) Act of 2013

FAIR, which was introduced by Senator Jeff Flake, would create federal civil liability for trade secret misappropriation when there is extraterritorial misappropriation or misappropriation of U.S. trade secrets for the benefit of foreign entities. [39] An owner of a "covered trade secret" could bring a civil action in federal court if a person who misappropriates, threatens to misappropriate, or conspires to misappropriate is either located abroad or is acting on behalf of, or for the benefit of, a foreign person. [40] FAIR would also apply if such foreign conduct causes or is reasonably anticipated to cause injury within the U.S. or to a U.S. person. [41] The bill includes several relevant definitions, including "covered trade secret," "improper means," "misappropriate," "person," and "trade secret." [42] Furthermore, potential remedies would

include injunctive relief, affirmative actions to be taken in order to prevent further misappropriation, and an award of damages. [43] Additionally, FAIR would include an affirmative defense, if the trade secret was acquired through proper means, and a statute of limitations that begins when misappropriation was discovered or should have been discovered. [44]

Controversially, the bill would grant a court the power to issue an ex parte seizure order, if a number of qualifications were met. [45] Specifically, (1) the owner must provide a bond that is adequate to pay any damages for a wrongful seizure; (2) the ex parte seizure order must be the only adequate means of ending the misappropriation; (3) the owner must not have publicized the seizure; (4) the merits of the case support the owner; (5) the owner will suffer immediate and irreparable injury without the seizure; (6) the trade secret is located at the place identified by the owner; (7) the harm to the owner outweighs the interests of the person against whom seizure is sought; and, (8) the person against whom seizure is sought would destroy, move, or hide the trade secret if that person knew of the seizure. [46] If an ex parte seizure were to take place, the court would then have to set a hearing date between three and ten days after the seizure was issued. [47] Additionally, if the owner fails to meet the factual and legal burdens necessary to support the seizure order, the court would be required to dissolve or modify the seizure order. [48] Finally, in the case of a wrongful seizure, the injured party would be allowed to bring a civil action against the owner and recover damages, which include punitive damages and lost profits. [49]

If FAIR were to be passed, it would be the first private cause of action available in federal courts for trade secret owners. [50] Therefore, it would establish uniformity in trade secret law and set procedural and substantive standards for courts and trade secret owners.

Furthermore, it would fix fundamental differences that trade secret law has when compared to the other field of intellectual property law. In the world we live in today, one that is increasingly mobile and globally interconnected, a federal system is better equipped to handle trade secret theft that crosses state and international borders.

Nonetheless, there are a number of detractors regarding a private cause of action in federal courts for trade secret misappropriation that believe bills, such as FAIR, "create or exacerbate many existing legal problems but solve none." [51] FAIR would employ system that would undoubtedly create additional burdens and costs upon the federal judiciary. [52] Furthermore, there is a legitimate concern surrounding the use of an ex parte seizure order. As described above, there are a number of qualifications in order to utilize an ex parte seizure order. Nonetheless, it is still a tool that could be abused, namely in situations where information is incorrectly defined as a trade secret. [53]. Additionally, dissenters argue that bills such as FAIR do not even necessarily provide more uniformity. They would add another law to the "already cluttered landscape." [54] Unfortunately, it is difficult to determine the correct answer without the existence of a private cause of action in the federal court. Regardless of which side you find yourself on, there is no doubt that U.S. companies are facing a new and complex threat regarding their trade secrets.

V. Protecting Trade Secrets

Despite the current landscape of trade secret law, there are preventative measures that can be currently taken to protect trade secrets. Although, many of these seem, and in reality are, rather simple and straightforward, one just need look at the headline stories regarding the issues Sony has recently experienced, to realize the importance of these measures. [55] A trade secrets protection program begins with addressing employment relationships. [56] From the outset,

companies and trade secret owners should require employees to sign confidentiality agreements, non-solicitation agreements, covenants not to compete, and assignment of invention agreements. [57] Consequently, companies and trade secret owners should implement appropriate policies, such as the proper use of computers, and train company employees in basic security awareness, security policies, appropriate procedures, and their security responsibilities. [58] Perhaps the most important time to protect trade secrets is upon an employee's termination. In order to do so, companies should take all reasonable measures, such as disabling their accounts and changing passwords, to protect their trade secrets. [59] Finally, companies and trade secret owners need to control access to their trade secrets. [60] Therefore, securing the physical environment surrounding the trade secrets, managing their access, securing the computer system and network, and protecting against third party disclosures are of prime importance. [61] Although the current status of trade secret law is not up to date with the rest of intellectual property law, there are still measures companies and trade secret owners can take in order to protect their trade secrets.

SOURCES

[1]. Fenwick & West, LLP, *Trade Secrets Protection: A Primer and Desk Reference for Managers and In House Counsel*, (2011), https://www.fenwick.com/FenwickDocuments/Trade_Secrets_Protection.pdf

[2]. *ConFold Pac. v. Polaris Indus*., 433 F.3d 952, 959 (7th Cir. 2006).

[3]. *See Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 476 (1974).

[4]. *See id.*

[5]. *Ruckelshaus v. Monsato Co.*, 467 U.S. 986, 1002 (1984).

[6]. Brian T. Yeh, *Protection of Trade Secrets: Overview of Current Law and Legislation*, *Congressional Research Service, (*September 5, 2014), https://www.fenwick.com/FenwickDocuments/Trade_Secrets_Protection.pdf. (See for a more comprehensive discussion of trade secret protection).

[7]. *See id.*

[8]. Restatement (Third) of Unfair Competition §40 (1994).

[9]. *See Implementing a Trade Secrets Protection Program*, Mondaq Business Briefing, (January 10, 2011), http://proxy.bc.edu/login?url=http://go.galegroup.com.proxy.bc.edu/ps/i.do?id=GALE%7CA246198575&v=2.1&u=mlin_m_bostcoll&it=r&p=ITOF&sw=w&asid=0ddde6f2f0f14063c39e7162d14e57b0.

[10]. Restatement (Third) of Unfair Competition §40 (1994).

[11]. Brian T. Yeh, *supra*.

[12]. *See Kewanee Oil Co.*, 416 U.S. at 476.

[13]. Brian T. Yeh, *supra*.

[14]. *See id.*

[15]. Robert C. Denicola, *The New Law of Ideas*, 28 Harvard Journal of Law & Technology, 195, 229 (2014).

[16]. Restatement of Torts §§ 757-758 (1938).

[17]. Brian T. Yeh, *supra*.

[18]. *See id.* (The UTSA has been adopted by 47 states and the District of Columbia. New York, North Carolina, and Massachusetts have not adopted the UTSA, but they offer trade secret protection through statutes or common law).

[19]. *See id.*

[20]. *See id.* (Before the EEA, the Trade Secrets Act of 1948 provided some level of trade secret protection, but it had a very limited scope).

[21]. *See id.*

[22]. *See* 18 U.S.C.A. § 1839 (West).

[23]. *See* 18 U.S.C.A. §§ 1831-1832.

[24]. *See* Brian T. Yeh, *supra*.

[25]. *See id.*

[26]. *See* 18 U.S.C.A. § 1839 (1).

[27]. *See* Brian T. Yeh, *supra*.

[28]. *See* Brian T. Yeh, *supra*. (quoting *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threat?: Hearings Before the Senate Judiciary Comm. Subcomm. On Crime and Terrorism*, 113th Cong. 2d Sess. (2014))

[29]. *See id.*

[30]. *See id.*

[31]. *See id.*

[32]. *See id.*

[33]. *See id.*

[34]. S. 884, §2(a), 113th Cong. (2013).

[35]. *See id.*

[36]. *See id.* §2(b).

[37]. *See id.*

[38]. *See id.*

[39]. S. 1770, §3(a), 113th Cong. (2013).

[40]. *See id.*

[41]. *See id.* §3(c).

[42]. *See id.* §2.

[43]. *See id.* §4 (damages could include requiring payment of a reasonable royalty for any ongoing disclosure, actual loss, unjust enrichment, punitive or exemplary damages, and reasonable costs and attorneys fees).

[44]. *See id.* §§ 5(a)(2); (e).

[45]. *See id.* §6(b).

[46]. *See id.*

[47]. *See id.* §6(e).

[48]. *See id.*

[49]. *See id.* §6(f).

[50]. *See* Brian T. Yeh, *supra*.

[51]. *Id.* at 23.

[52]. *See id.*

[53]. David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls,* 71 Wash. & Lee L. Rev. 230, 256-57 (2015).

[54]. *See* Brian T. Yeh, *supra*.

[55] Sony To Pay Out $3.5M To Lawyers To Settle Hacking Class Action Suit." Deadline. 20 Oct. 2015. Web. 1 March. 2016.

[56] *See Implementing a Trade Secrets Protection Program, supra*.

[57]. *See id.*

[58]. *See id.*

[59]. *See id.*

[60]. *See id.*

[61]. *See id.*