Journal of Legislation

Volume 43 | Issue 2 Article 6

4-6-2017

Two Steps Forward, One Step Back: The Defend Trade Secrets Act of 2016 and Why the Computer Fraud and Abuse Act of 1984 Still Matters for Trade Secret Misappropriation

Patrick J. Manion

TWO STEPS FORWARD, ONE STEP BACK: THE DEFEND TRADE SECRETS ACT OF 2016 AND WHY THE COMPUTER FRAUD AND ABUSE ACT OF 1984 STILL MATTERS FOR TRADE SECRET MISAPPROPRIATION

Patrick J. Manion

INTRODUCTION

Trade secrets are a form of intellectual property provided legal protection due to their independent economic value. What material satisfies as a "trade secret" depends on the jurisdiction where relief is sought and which law is applied. However, generally a trade secret is information—including a formula, pattern, compilation, program, device, method, technique or process.[1] Until recently, trade secrets were unique among the various forms of intellectual property because they were not afforded federal protection.[2] Indeed, today trade secret misappropriation is primarily addressed through state versions of the Uniform Trade Secrets Act, as well as the common law.[3] Trade secret theft costs the United States economy between $300 and $480 billion a year.[4] Fights over valuable trade secret theft have ensnared some of the largest and most recognizable names in U.S. industry.[5] In recognition of this growing concern, Congress passed the Defend Trade Secrets Act of 2016 with overwhelming bipartisan support in May of 2016.[6] The legislative intent of the Act was

[1] *See Trade Secret*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information — including a formula, pattern, compilation, program, device, method, technique, or process — that (1) derives independent economic value, actual or potential, from not being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use, and (2) is the subject of reasonable efforts, under the circumstances, to maintain its secrecy.").

[2] In contrast, federal laws existed which protected trademarks, patents, and copyrights.

[3] *See, e.g.*, RESTATEMENT OF TORTS, § 757 (AM. LAW INST. 1939) and RESTATEMENT OF UNFAIR COMPETITION, § 39 (AM. LAW INST. 1995).

[4] S. REP. NO. 114-220, at 2 (2016).

[5] *See, e.g.*, Siobhan Hughes, *Senate Passes Trade-Secrets Bill*, THE WALL STREET JOURNAL, (Apr. 4, 2016), https://www.wsj.com/articles/senate-passes-trade-secrets-bill-1459807973 ("DuPont Co. spent six years on a trade-secrets case involving Kevlar, a fiber used in bulletproof vests. In that case, DuPont enlisted the Justice Department's help to go after Kolon Industries Inc., alleging that it had recruited former DuPont employees in to steal technological know-how that took DuPont decades to develop. The companies ultimately settled about a year ago, with Kolon agreeing to pay DuPont $275 million in restitution.").

[6] Office of the Clerk of The United States House of Representatives, Final Vote Results for Roll Call 172, (Apr. 27, 2016), http://clerk.house.gov/floorsummary/floor.aspx?day=20160427&today=20170225.

to clarify conflicting state laws regarding trade secret misappropriation and to provide a new federal civil cause of action for aggrieved parties.[7] Prior to passage of the Defend Trade Secrets Act, aggrieved parties had to rely on an independent basis for federal jurisdiction or contort their claim to satisfy elements of a cause of action under the Computer Fraud and Abuse Act of 1984, the Economic Espionage Act of 1996, or general criminal statutes.

The Economic Espionage Act and general criminal statutes are often ineffective. For example, while the Economic Espionage Act "makes it a Federal criminal offense to misappropriate a trade secret that has an interstate or foreign nexus … [the Act] does not give trade secret owners a private right of action in Federal court."[8] Therefore, a party asserting a claim under the Economic Espionage Act must rely on the Federal Government to criminally prosecute the case, and "while economic espionage and the theft of trade secrets is a top priority for federal law enforcement, criminal enforcement remains a limited solution to stopping trade secret theft as the Federal Bureau of Investigation and Department of Justice are limited in the resources they can bring to bear."[9] Another option is to bring a trade secret misappropriation claim under state law. Forty-seven states and the District of Columbia have adopted some version of the Uniform Trade Secrets Act; however, state variations in the application of the Uniform Trade Secrets Act have led to inconsistent outcomes across jurisdictions.[10] This is where the Defend Trade Secrets Act becomes relevant by affording a new means for private parties to obtain federal jurisdiction. This allows them to bypass the foibles of conflicting state law without the burden of providing an independent basis for federal jurisdiction or having to use the Computer Fraud and Abuse Act, the Economic Espionage Act, or general criminal statutes.

While the contours of the Defend Trade Secrets Act are still being shaped as courts embrace this new law, two recent opinions have highlighted an interesting

[7] S. REP. NO. 114-220, at 3 (2016).

[8] *Id.*

[9] *Id.*

[10] *See* ALA. CODE § 8-27-1 (1975) et seq., ALASKA STAT. § 45.50.910 et seq., ARI. REV. STAT. ANN. § 44-401 et seq., ARK. CODE ANN. § 4-75-601 et seq., CAL. <UNIFORM TRADE SECRETS ACT CODE> § 3426 et seq., COL. REV. STAT. § 7-74-101, CONN. GEN. STAT. § 35-50 et seq., DEL. CODE ANN. tit. 6 § 2001 et seq., D.C. CODE ANN. § 48-501 et seq., FLA. STAT. ANN. § 688.001 et seq., GA. CODE ANN. § 10-1-760 et seq., HAW. REV. STAT. ANN. § 482B-1 et seq., IDAHO CODE ANN. § 48-801 et seq., Ill. ANN. STAT. ch. 140 Secs. 351-59, IND. CODE ANN. § 24-3-1-8, 1990 90 Acts, ch. 1201 Section 550.1 et seq., KAN. STAT. ANN. § 60-3320 et seq., KY. REV. STAT. ANN. § 365.880 et seq., LA. STAT. ANN. § 51:1431 et seq., ME. REV. STAT. ANN. tit. 10, § 1541 et seq., MD. CODE ANN., COMMERCIAL LAW § 11-1201 et seq., MICH. COP. LAWS ANN. § 445.1901 et seq., MINN. STAT. ANN. § 235C.01 et seq., MISS. CODE ANN. § 75-26-1 et seq., MO. ANN. STAT. § 417.467, MONT. CODE ANN. § .30-14-401 et seq., NEB. REV. STAT. ANN. § 87-501 et seq., NEV. REV. STAT. ANN. § 600A.010 et seq., N.H. REV. STAT. ANN. § 350-B:1 et seq., N.J STAT. ANN. § 56:15-1 S-et seq., N.M. STAT. ANN. § 57-3A-1 et seq., N.C. GEN. STAT. ANN. § 66-152 et seq., N.D. CENT. CODE ANN. § 25.1-01 et seq., OHIO REV. CODE ANN. § 1333.61 et seq., OKLA. STAT. ANN. tit. 78, § 86 et seq., OR. REV. STAT. ANN. § 646.461 et seq., 12 PA. STAT. AND CONS. STAT. ANN. § 5392 et seq., tit. 6 R.I. GEN. LAWS ANN. § 6-41-1 et seq., S.C. CODE ANN. § 39-8-1 et seq., S.D. CODIFIED LAWS § 37-29-1 et seq., TENN. CODE ANN. § 47-25-1701 et al., Title 6 CH 134A et al., UTAH CODE ANN. §13-24-1 et seq., VA. CODE ANN. § 59.1-336 et seq., WASH. REV. CODE ANN. § 19.108.010 et seq., W. VA. CODE ANN. § 47-22-1 et seq., WIS. STAT. ANN. § 134.90, WYO. STAT. ANN. § 40-24-101.

interplay between the Act and state non-compete policies.[11] Specifically, the remedies section of the Defend Trade Secrets Act states that an injunctive order under the Act will not conflict with state laws that prohibit restraints on trade.[12] This is important because a trade secret misappropriation claim is often brought in conjunction with a claim for violation of a non-compete agreement or is brought seeking an injunction that will operate as a constructive non-compete on the former employer—measures that amount to a restraint on trade, which may be prohibited under the Defend Trade Secrets Act. Moreover, the scope of injunctive relief sought by an aggrieved party may include restraining the employment of a separated employee. Thus, injunctive relief, a plaintiff's preferred remedy, may be harder to obtain under the Defend Trade Secrets Act even though the purported goal of the Act was to harmonize the application of trade secret law. Indeed, the principal argument made by proponents of a federal trade secret remedy was the goal of uniformity.[13] This Note argues that the Defend Trade Secret Act falls short of this goal by offering a state carve-out that limits the scope of injunctive relief available, leaving the Computer Fraud and Abuse Act as an attractive option in certain jurisdictions that disfavor or prohibit restraints on trade and in factual scenarios where the trade secret has been accessed electronically. This proposition has growing relevance, as one of President Obama's final policy initiatives was a call to action regarding the overuse and abuse of non-compete provisions.[14]

This Note is divided into two parts which detail the history, application, and interplay between various trade secret misappropriation remedies. Part I of this Note examines existing means by which to address trade secret misappropriation and the various pitfalls of each. Part I is divided into three sections. The first section of Part I examines the background and application of the Uniform Trade Secrets Act as well as its common law origins. The second section of Part I examines the background and historical application of the Computer Fraud and Abuse Act of 1984 as both an

[11] *See, e.g.*, Panera, LLC v. Nettles, 2016 U.S. Dist. LEXIS 101473, 2016 WL 4124114 (E.D. Mo. Aug. 3, 2016) (granting a temporary restraining order and concluding the plaintiff was likely to succeed on merits of DTSA claim); Henry Schein, Inc. v. Cook, 191 F.Supp.3d 1072 (N.D. Cal. June 2016) (denying in part a preliminary injunction on basis that injunctive relief would violate California policy disfavoring restraints on trade).

[12] 18 U.S.C.A. § 1836(3)(A)(i)(I-II) (2016) ("In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may…grant an injunction…to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not …prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or… otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business...").

[13] *See, e.g.*, David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769 (2009) ("The dominant failure of a state-based trade secret regime is that trade secret law differs from state to state. Consequently, the most obvious benefit of [a federal trade secret statute] is that it will instantly accomplish what the common law, Restatement, UTSA, and Economic Espionage Act have all failed to achieve-- uniformity, both substantive and procedural.").

[14] Press Release, The White House, Office of the Press Sec'y, FACT SHEET: The Obama Administration Announces New Steps to Spur Competition in the Labor Market and Accelerate Wage Growth, (Oct. 25, 2016) ("Today, the Administration put out a call to action and set of best practices for state policymakers to enact reforms to reduce the prevalence of non-compete agreements that are hurting workers and regional economies.").

anti-hacking statute and as a means of federal jurisdiction for trade secret misappropriation claims when the information alleged to have been misappropriated was done so by electronic means. Lastly, the third section of Part I examines the background and application of the Economic Espionage Act of 1996.

Part II of this Note transitions to a discussion of the Defend Trade Secrets Act. Specifically, Part II is divided into two sections, which detail the background of the Defend Trade Secrets Act, recent application of the Act, and interaction between the Act and state non-compete provisions. I conclude by arguing that the Computer Fraud and Abuse Act may be a more attractive remedy for trade secret misappropriation claims considering recent state and federal trends disfavoring non-compete covenants and in light of the state non-compete carve out provisions of the Defend Trade Secrets Act.

I. EXISTING MEANS BY WHICH TO ADDRESS TRADE SECRET MISAPPROPRIATION

A. Background and Application of the Uniform Trade Secrets Act

Forty-seven states and the District of Columbia have enacted some version of the Uniform Trade Secrets Act. States that have not adopted the Uniform Trade Secrets Act follow common law principles that are similar to the general principles expressed in the Act. As background, the common law principles regarding trade secret misappropriation are best identified in the Restatement (Third) of Unfair Competition.[15] In a common law district, a plaintiff must establish three elements to prevail on a trade secret misappropriation claim: (1) a plaintiff must establish the existence of a trade secret; (2) a plaintiff must establish that the defendant has acquired knowledge of the trade secret as a result of a confidential relationship with the plaintiff; and (3) a plaintiff must establish that the defendant has made unauthorized use or disclosure of the trade secret.[16]

With respect to the first element of a common law trade secret claim, drafters of comment B to § 757 of the Restatement of Torts acknowledged it was not possible to come up with an exact definition. Instead, they listed six factors courts typically consider when evaluating whether something is a trade secret:

> (1) [t]he extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

[15] RESTATEMENTS (THIRD) OF UNFAIR COMPETITION 39 (AM. LAW INST. 1995) ("A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.").

[16] *Id.*

This is not a dispositive test but rather a list of factors courts can and do consider when establishing the first element of a trade secret claim—whether there was a proper trade secret to protect in the first place. The Restatement § 757 factors are important because they have continued to be referenced by courts in jurisdictions that have adopted the Uniform Trade Secrets Act.[17] One reason courts may continue to rely on the Restatement factors is the inherent difficulty of defining trade secrets in an increasingly complex technological landscape. A second reason may be that the Uniform Trade Secrets Act definition is simply lacking. Indeed, the Uniform Trade Secrets Act defines "trade secret" 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.[18]

Although this definition incorporates aspects of the Restatement § 757 factors, it does not provide as many independent factors for a court to consider and rely upon. Under the Uniform Trade Secrets Act, a trade secret must have independent economic value and be subject to reasonable security measures. A Uniform Trade Secrets Act trade secret definition does not afford judges the same comfortable amount of leeway as that provided under the Restatement.

In order for a Uniform Trade Secrets Act claim to be actionable, there must have been a "misappropriation." The Uniform Trade Secrets Act describes several types of conduct and defines "misappropriation" as:

> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.[19]

[17] *See, e.g.*, Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 722 (7th Cir. 2003) ("Although the Act explicitly defines a trade secret…Illinois courts frequently refer to six common law factors (which are derived from § 757 of the Restatement (First) of Torts) in determining whether a trade secret exists.").

[18] Uniform Law Commission Annual Conference, *The Uniform Trade Secrets Act With 1985 Amendments*, Uniform Law Commission, (Aug. 2-9, 1985). http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.

[19] *Id*. at 3-4

The Uniform Trade Secrets Act definition of "misappropriation" does not define "improper means." However, courts applying the Uniform Trade Secrets Act have generally held improper means to include: misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, theft, and bribery. In a comment to the Act, the drafters defined "proper means" as independent invention, reverse engineering, discovery under a license from the owner of the trade secret, observation of the item in public use or on public display, and obtaining the trade secret from published literature.[20]

The Uniform Trade Secrets Act was completed by the Uniform Law Commission in 1979 and amended in 1985.[21] The goal of the Uniform Law Commission members is "to research, draft and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical."[22] Ironically, the goal of the Uniform Trade Secrets Act was to address gaps in the common law and to provide uniform remedies across state lines.[23] Unfortunately, this goal was thwarted over the years by variances in judicial interpretation and application of the law. This lack of uniformity has caused problems for attorneys litigating trade secret claims and businesses seeking to protect valuable trade secrets in their ordinary course of business. David Almeling, an IP attorney for the law firm O'Melveny & Myers, wrote an article in 2009 advocating for a federal trade secrets law. In his article, Almeling noted the following critiques about the Uniform Trade Secrets Act, "among the forty-six states that have enacted it, differences remain because legislatures in those states have modified the Uniform Trade Secrets Act and courts in those states have adopted different interpretations."[24] Almeling goes on to explain that:

> [t]hese modifications and interpretations…include fundamental differences about what constitutes a trade secret, what is required to misappropriate it, and what remedies are available. Finally, even in instances where states have enacted the Uniform Trade Secrets Act, many state courts continue to rely on their own common law instead of…the Uniform Trade Secrets Act.[25]

Ironically, the point of Almeling's article is to advocate for a federal trade secret law to provide the uniformity lacking with the adoption of the Uniform Trade Secrets Act he so deftly critiques. Unfortunately, as will be explored, the newly enacted Defend Trade Secrets Act leaves much to be desired in this regard.

---

[20] *Id*. at 5-6.

[21] *About the ULC*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/Narrative.aspx?title=About%20the%20- ULC (explaining that the Uniform Law Commission is a coalition of "practicing lawyers, judges, legislators and legislative staff and law professors, who have been appointed by state governments as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands").

[22] *About the ULC*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/Narrative.aspx?title=About%20the%20- ULC

[23] *Why States Should Adopt the UTSA*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/Narrative.aspx?title=Why%20States%20Should%20Adopt%20UTSA.

[24] Almeling, *supra* note 13, at 773-74.

[25] *Id*. at 774.

B. Background and Historical Application of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act of 1984 (CFAA) was passed by Congress to address concerns in the 1980s regarding the cyber security of federal computers and information networks.[26] Importantly, the Computer Fraud and Abuse Act is *not* a trade secret law and was never intended to serve as a federal corollary to the Uniform Trade Secrets Act. However, in the initial years after passage, the law was amended multiple times. These amendments were always limited to the narrow scope of the law's original intent—to protect computers, "involving a compelling federal interest."[27]

However, in 1994 Congress amended the law to allow, "any person who suffered damage by a statutory violation to 'maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.'"[28] This set of amendments was codified at 18 U.S.C. 1030(g) and provided a new federal civil remedy.[29] Additionally, 18 U.S.C. 1030(a)(5) was amended to protect computers and computer systems from both outside *and* inside actors.[30] Specifically, the section prohibited an individual who "intentionally accesses a Federal interest computer without authorization, and…alters, damages, or destroys information in any such Federal interest computer…."[31]

In 1996, the Act was amended again to broaden the scope of the law. For example, "[while the] 1994 version of 18 U.S.C. § 1030(a)(5)(A), included the phrase 'through means of a computer used in interstate commerce or communications'; this qualifying phrase was deleted in a 1996 amendment."[32] Additionally, the phrase "federal interest computer" was replaced with "protected computer."[33] These amendments are consistent with a general broadening of the law to include all computers, not just those with a federal interest, as originally designated under the Act.

Consistent with the legislative intent of the Act, the law was originally used to address hacking and computer crime. However, as the Act evolved to fit the rapidly changing technological landscape it also became a means of federal subject matter jurisdiction for trade secret misappropriation when that misappropriation occurred by electronic means.[34] Using the Act as a vehicle for federal subject matter jurisdiction

[26] Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*,174 A.L.R. Fed. 101 (2001).

[27] *Id*.

[28] *Id*.

[29] 18 U.S.C. 1030(g).

[30] Buckman, *supra* note 26.

[31] 18 U.S.C. § 1030(a)(5)(A) (1994).

[32] *See* Buckman, *supra* note 26.

[33] *See* Buckman, *supra* note 26.

[34] Although at first glance this seemingly conflicts with the purported goal of the newly passed Defend Trade Secrets Act, the means by which to address trade secret misappropriation under the Computer Fraud and Abuse Act *required* that the trade secret misappropriation occur by electronic means. While this was a growing means by which trade secrets were misappropriated it nevertheless still left physical misappropriation of trade secrets by more conventional means without a federal remedy, thereby creating the need for the Defend Trade Secrets Act.

for trade secret misappropriation highlighted the evolving dichotomy between "inside" and "outside" actors with respect to the original intent of the law. Historically, the Computer Fraud and Abuse Act was viewed as an "anti-hacking" statute[35] and therefore applied to *outside* actors who "exceeded authorized access" or acted "without access" under the terms of the statute.[36] Specifically, the statute uses the phrase "without access" ten times and the phrase "exceeds authorized access" four times to refer to actors in violation of the statute.[37] However, in the trade secret context, most claims involve a departing employee. Thus, the question became whether or not the Computer Fraud and Abuse Act covered internal misappropriation of trade secrets by electronic means or only outside actors who fit the more traditional description and legislative intent of preventing hackers. One case that explores this question is *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*[38]

In *Shurgard Storage*, the District Court for the Western District of Washington held that "employees were 'without authorization' to access information from their employer's computers when they began to appropriate the employer's trade secrets for the benefit of the competitor."[39] In that case, Shurgard sued Safeguard under the Computer Fraud and Abuse Act for trade secret misappropriation when Eric Leland, a departing Shurgard employee, "sent e-mails to the defendant [Safeguard] containing various trade secrets and proprietary information belonging to the plaintiff [Shurgard]."[40] Leland went on to accept employment with Safeguard. Shurgard argued for purposes of the statute that although Leland had access to the information while employed by Shurgard, he "exceeded" this access when he became an agent for Safeguard. Conversely, Safeguard claimed that Leland could not "exceed" access when it was already granted to him by Shurgard as part of his normal employment with Shurgard.[41] The court accepted Shurgard's interpretation of "exceeds authorized access" and in the process laid the early framework for a circuit split regarding how courts interpret when an employee exceeds authorized access.[42] Regarding application of the Computer Fraud and Abuse Act in *Shugard*, Deborah Buckman said,

> The court applied principles of agency law to conclude that the employees' authorized access to the employer's computers ended at the moment when they became agents of the competitor and began appropriating information from the employer's computer for the competitor's benefit. The court also rejected the defendants' argument that the Act applied only to "outsiders" or "hackers" and was inapplicable to inside employees, noting that its express language refers to anyone who intentionally

[35] *See* e.g., H.R. Rep. No. 98-894 (1984).

[36] *See* 18 U.S.C. § 1030 (1994).

[37] *See* 18 U.S.C. § 1030.

[38] Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[39] Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*,174 A.L.R. Fed. 101 (2001).

[40] Shurgard Storage, 119 F. Supp. 2d at 1123.

[41] *Id*.

[42] *Id.* at 125 ("Under this rule, the authority of the plaintiff's former employees ended when they allegedly became agents of the defendant. Therefore, for the purposes of this 12(b)(6) motion, they lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail.").

> accesses a protected computer. The court acknowledged that the original scope of the statute may have been interpreted as so limited, but pointed out that its subsequent amendments broadened the scope sufficiently to cover the behavior alleged in this case.[43]

The *Shurgard* court highlighted the dichotomy between inside and outside employees and broadened the scope of the Computer Fraud and Abuse Act to apply not just as an anti-hacking statute for outside actors but also to internal, departing employees. This distinction was further emphasized in a subsequent case, *Int'l Airport Ctrs., LLC v. Citrin*.[44]

In *Citrin*, Jacob Citrin served as an employee for International Airport Centers ("International Airport"), a real estate development corporation involved in the acquisition of airport real estate.[45] Citrin decided to leave International Airport and start a competing business. While in the process of leaving International Airport, Citrin deleted all the data off his company-issued laptop before handing in the computer. The Court of Appeals for the Seventh Circuit drew on the agency principles espoused by the *Shurgard Storage* court when it said, "Citrin's breach of his duty of loyalty terminated his agency relationship…and with it his authority to access the laptop, because the only basis of his authority had been that relationship."[46] This judicial trend toward applying agency principles to determine when an employee "exceeded authorized access" or acted "without access" was not meant to last. In 2012, the Ninth Circuit rejected *Citrin* in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) ("*Nosal"*). In the *Nosal* case, David Nosal was an employee of Korn Ferry – a Los Angeles-based executive search and advisory firm. Nosal decided to leave Korn Ferry and start his own competing firm.[47] After leaving Korn Ferry, Nosal convinced some of his former colleagues who were still working for Korn Ferry to help him start a competing business. Nosal's fellow employees used their Korn Ferry computer login information to access and download source lists, names and contact information from a confidential database on the company's computer system, and then transferred that information to Nosal to help start the competing business.[48] In that case, the employees who were still working for Korn Ferry were authorized to access the database, but Korn Ferry had a policy that prohibited disclosing confidential information.[49] Nosal was indicted on twenty counts, including trade secret theft. Using *Citrin*, the court could have applied agency principles and reasoned that misappropriation had taken place under the Computer Fraud and Abuse Act because the employees Nosal solicited had stopped acting for Korn Ferry when they surreptitiously conveyed confidential information to Nosal in breach of their duty of loyalty. Instead,

[43] *See* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*,174 A.L.R. Fed. 101 (2001).

[44] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[45] *Id*. at 419.

[46] *Id*. at 420–21 (quoting Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d at 1123, 1125).

[47] United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012).

[48] *Id*.

[49] *Id*.

the Ninth Circuit Court of Appeals held that, "[T]he CFAA does not cover an employee-hacker or an insider that takes data and uses it in an anticompetitive manner after leaving the company." [50] The *Nosal* ruling laid the groundwork for a circuit split.

Three months later, the Fourth Circuit agreed with the Ninth Circuit *Nosal* opinion in *WEC Carolina Energy Solutions LLC v. Miller* ("*WEC"*).[51] In *WEC*, defendant Mike Miller worked for WEC – a specialty welding company in South Carolina. WEC brought suit against Miller and his assistant for downloading confidential information to a personal laptop in preparation for a planned departure to a WEC competitor.[52] In that case, the court held that "the CFAA is not violated unless an employee lacks *any* authorization to obtain or alter the data when he or she was employed." [53] Conversely, "the First, Fifth, Seventh, and Eleventh circuits take the opposite view and support the concept that an employee-hacker violates the CFAA whether he or she uses the data with or without financial gain."[54]

Thus the circuit split regarding an employee's scope of "authorization" and whether it applies to inside and outside actors equally evolved from these cases and remains in controversy. This uncertainty and un-reconciled disparity regarding interpretation of the Computer Fraud and Abuse Act is one of the main limiting factors associated with using the Computer Fraud and Abuse Act as a vehicle for remedying trade secret misappropriation. However, as is discussed in Part III of this Note, the Computer Fraud and Abuse Act still has significant advantages over the Defend Trade Secrets Act despite this limitation.

C. History and Application of the Economic Espionage Act of 1996

The Economic Espionage Act of 1996 ("EEA") is divided into two sections.[55] The law created two new federal criminal offenses for the theft of trade secrets. First,

[50] Robert C. Kain, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, but Illegal in Miami, Dallas, Chicago, and Boston*, 87 FLA. BAR J. 36 (2013).

[51] 687 F.3d 199 (4th Cir. 2012).

[52] *Id*. at 201-02.

[53] 687 F.3d 199 (4th Cir. 2012).

[54] *Id.*

[55] Specifically, 18 U.S.C. § 1831 states: "'(a) IN GENERAL- Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly-'(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;'(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;'(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;'(4) attempts to commit any offense described in any of paragraphs (1) through (3); or '(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both. '(b) ORGANIZATIONS- Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000." Meanwhile, Section 1832 states, "'(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly-- '(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; '(2) without authorization copies,

"[s]ection 1831 of the EEA, titled "Economic Espionage," criminalizes acts done with the intent to benefit any foreign government, instrumentality, or agent."[56] Meanwhile, "[s]ection 1832 of the EEA, titled 'Theft of Trade Secrets,' pertains to domestic acts and makes the same conduct described in section 1831 a crime regardless of whether the theft is meant to benefit a foreign government."[57] Importantly, "[s]ection 1832 differs from section 1831 by including stipulations that the goal of the misappropriation is to harm the owner of the trade secret and to economically benefit someone other than the owner of the trade secret."[58] Significantly, the Economic Espionage Act of 1996 as introduced was solely a federal criminal statute; therefore, the only party that had standing to bring a suit under the Economic Espionage Act of 1996 was the Federal Government. This was perhaps the main limitation (although there were others[59]) regarding use of the Economic Espionage Act of 1996 to redress trade secret misappropriation. Regardless, the law was passed to address a growing concern by the government that foreign actors were committing economic espionage against U.S. companies and was meant to (again) standardize application of trade secret misappropriation law.[60] Recognizing the limitations of the Economic Espionage Act of 1996 to adequately address trade secret misappropriation, the Defend Trade Secrets Act emerged as a means to yet again standardize application of trade secret misappropriation law and provide a new, private federal cause of action for aggrieved parties.

duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; '(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; '(4) attempts to commit any offense described in paragraphs (1) through (3); or '(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both. '(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

[56] Spencer Simon, *The Economic Espionage Act of 1996*, 13 BERKELEY TECH. L.J. 305, 310 (1998).

[57] *Id.*

[58] *Id.*

[59] *See id.* ("The EEA does not protect trade secrets related to services (as opposed to goods), negative know-how, or reverse engineering. Furthermore, it does not address the needs of U.S. corporations operating abroad from trade secret theft. It also fails to adequately address the rights of victims for monetary loss sustained as a result of the theft and misappropriation of their trade secrets. To qualify under section 1832, trade secrets must be "related to or included in a product that is produced for or placed in interstate or foreign commerce." Because trade secrets explicitly must be embodied in a product in the stream of commerce, protection is limited if the trade secret relates to a rendering of services rather than a produced ware that contains or uses the secret.").

[60] *See e.g., id.* ("The problem of foreign economic espionage has grown significantly since the end of the Cold War. Testifying before joint hearings by the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology, and Government Information for the EEA's passage in early 1996, Federal Bureau of Investigation Director Louis Freeh stated that the Bureau's investigations of economic espionage cases had doubled in the previous year from 400 to 800, and twenty-three countries had been involved. He claimed that foreign governments are actively targeting U.S. industry and the U.S. government to steal "critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage." According to Freeh and other law enforcement officials, former military spies have been redeployed by foreign governments to the commercial world, presumably ready to use their skills in other ways. The loss to U.S. industry from foreign economic espionage is estimated at nearly $100 billion per year.) (internal quotation marks and citations omitted).

II. THE BACKGROUND AND APPLICATION OF THE DEFEND TRADE SECRETS ACT AND INTERPLAY WITH STATE NON-COMPETE PROVISIONS

A. Background and Legislative Intent

According to the United States Senate Report, the Defend Trade Secrets Act (DTSA) was passed in order to harmonize variances in state application of trade secret law.[61] Forty-seven states and the District of Columbia have passed some version of the Uniform Trade Secrets Act (UTSA).[62] However, state application of the Uniform Trade Secrets Act has been anything *but* uniform. Inconsistent application of the Uniform Trade Secrets Act by the states has led to a confusing landscape for businesses and employers to navigate an economy that is increasingly unbound by traditional geographic limitations. For example, the Senate Report acknowledged the impact of this variation among state law versions of the Uniform Trade Secrets Act stating,

> [a]lthough the differences between State laws and the UTSA are generally relatively minor, they can prove case-dispositive: they may affect which party has the burden of establishing that a trade secret is not readily ascertainable, whether the owner has any rights against a party that innocently acquires a trade secret, the scope of information protectable as trade secret, and what measures are necessary to satisfy the requirement that the owner employ ''reasonable measures'' to maintain secrecy of the information.[63]

Practitioners and academics alike have long advocated for a federal trade secret law to clarify this confusing landscape and provide parity with other forms of intellectual property already afforded federal protection.[64] Indeed, the Defend Trade Secrets Act is not a revolutionary concept; it is the product of decades of advocacy and a rapidly changing technological landscape that has led to increasing theft of U.S. trade secrets. Moreover, the Defend Trade Secrets Act achieves its goal of providing a federal remedy by paying homage to, and incorporating, the legislative efforts of previous trade secret laws. Specifically, the Defend Trade Secrets Act amends the Economic Espionage Act to provide a civil remedy and bases its definition of "trade secret" off the Uniform Trade Secrets Act.

In short, the Defend Trade Secrets Act is both new and old—an amalgamation of existing law with a new federal application. There are five key differences between the Uniform Trade Secrets Act and the Defend Trade Secrets Act. First, the Defend Trade Secrets Act definition of "trade secret" builds on the Uniform Trade Secrets Act definition by stating that trade secrets means all forms and types of financial,

---

[61] S. REP. NO. 114-220 (2016).

[62] *See supra* note 10.

[63] S. REP. NO. 114-220, at 2 (2016).

[64] *See e.g.*, Christopher Rebel J. Pace, *The Case for A Federal Trade Secrets Act*, 8 HARV. J.L. & TECH. 427 (1995); *see generally*, Almeling, *supra* note 13.

business, scientific, technical, economic, and engineering information.[65] The definition section of the Defend Trade Secrets Act also makes clear that trade secrets can be tangible or intangible regardless of how they are stored, compiled, or memorialized, whether that is physically, electronically, graphically photographically, or in writing.[66] Secondly, the term "improper means" expressly excludes certain conduct under the Defend Trade Secrets Act (reverse engineering, independent derivation or any other lawful means of acquisition).[67] Third, the Defend Trade Secrets Act provides for an *ex parte* civil seizure order.[68] Fourth, while the Defend Trade Secrets Act is not to be construed as pre-empting or displacing civil or criminal remedies under either federal or state law, the Uniform Trade Secrets Act expressly displaces other state law regarding trade secrets or misappropriation.[69] Finally, although the Defend Trade Secrets Act provides for similar remedies as those afforded by the Uniform Trade Secrets Act, the Defend Trade Secrets Act expressly states that no injunction can "prevent a person from entering into an employment relationship."[70] This Note focuses on this final distinction and is arguably why the Computer Fraud and Abuse Act may be a more attractive means to address trade secret misappropriation.

B. Recent Application of the Defend Trade Secrets Act and its Interplay with State Non-Compete Provisions

Two recent cases highlight the evolving judicial interpretation of the newly enacted Defend Trade Secrets Act. To contrast treatment of injunctive relief by the courts and to highlight the dichotomy that is already developing, this section examines one case from California, a state that prohibits restraints on trade,[71] and one case from Missouri, a state that does not prohibit restraints on trade. [72] Finally, this section examines a newly filed case in the Northern District of California and explores how that case may fit into the developing DTSA landscape.

The first court to enter a written opinion under the DTSA was the Northern District of California in *Henry Schein, Inc. v. Cook*.[73] In that case, Henry Schein Inc.

[65] 18 U.S.C. § 1836(3) (2016).

[66] *Id.*

[67] 18 U.S.C. § 1836(6) (2016).

[68] The most contentious and arguably the most significant change from the UTSA to the DTSA is the inclusion of an *ex parte* civil seizure order which provides, "for expedited relief on an ex parte basis in the form of a seizure of property from the party accused of misappropriation, a remedy available under extraordinary circumstances where necessary to preserve evidence or prevent dissemination of a trade secret." S. REP. NO. 114-220, at 3 (2016). The *ex parte* basis allows for a claimant to petition the court unchallenged for an injunctive order to prevent the dissemination of a trade secret. This is a radical departure from the equitable relief available under the UTSA.

[69] Unif. Trade Secrets Act § 7(a) (1985) (stating that "[e]xcept as provided in subsection (b), this [Act] displaces conflicting tort, restitutionary, and other law of this State.".

[70] 18 U.S.C. § 1836(b)(3) (2016).

[71] *See generally*, David R. Trossen, *Edwards and Covenants Not to Compete in California: Leave Well Enough Alone*, 24 BERKELEY TECH. L.J. 539 (2009).

[57] *See e.g.*, *Whelan Sec. Co. v. Kennebrew*, 379 S.W.3d 835, 841 (Mo. 2012) ("Missouri courts generally enforce a non-compete agreement if it is demonstratively reasonable." (internal citations omitted)).

[73] 2016 LEXIS 81369 (N.D. Cal. June 22, 2016). *See generally*, Vann Pierce and Matthew Ingles, *Early Returns (Part 3 of 3): California Federal Court First to Rule Under New Defend Trade Secrets Act of 2016*, ORRICK

("HSI"), a medical, dental, and veterinary supplies company originally sought a Temporary Restraining Order ("TRO") against a former employee, Ms. Jennifer Cook, before filing a complaint alleging trade secret misappropriation under the DTSA.[74] In the TRO proceeding, HSI alleged that before Ms. Cook left HSI to work for a competitor, she stole confidential information in violation of state and federal trade secret laws and in contravention of employment agreements she signed while employed with HSI.[75] The court granted the TRO which, "enjoined [Cook] from, directly or indirectly, soliciting, continuing to solicit, initiating contact with, or accepting business from, any HSI customers whose accounts were assigned to her while she was employed by HSI."[76] Two weeks later on June 22, 2016, the court granted HSI a preliminary injunction but repealed the customer contact restrictions on Ms. Cook in recognition of California case law and statutory law disfavoring restraints on trade, despite finding that HSI demonstrated a likelihood of success on the merits regarding misappropriation of trade secrets under the DTSA.[77]

Conversely in July of 2016 in the Eastern district of Missouri, Panera sought and was granted a TRO to enjoin a former employee from working for a competitor based largely on that employee's knowledge and potential use of Panera trade secrets.[78] In that case, Panera, a corporation that owns and operates "bakery-café" stores sought to enjoin a former employee from working for the pizza company Papa John's.[79] Panera alleged that Michael Nettles, as Vice President of Architecture in Panera's Information Technology department, had access to valuable and confidential information, including Panera trade secrets.[80] Panera sought a TRO to enjoin Nettles from employment with Papa John's to prevent the disclosure of valuable trade secrets.[81] The court found that, "Panera [was] likely to succeed on the merits of several of its claims, including … its request for injunctive relief in order to protect the disclosure of its confidential information and trade secrets."[82] The scope of the injunctive relief granted in the TRO by the court barred Nettles from employment with Papa John's, because, "Nettles' immediate employment with Papa John's is likely to lead to such disclosure [of trade secrets].[83]

The difference between *Panera* and *Henry Schein* is clear. In states that disfavor or prohibit the enforcement of non-compete provisions, one of the most valuable and sought after remedies by plaintiffs is potentially unavailable—injunctive relief that acts as a constructive restraint on trade. Companies may prefer equitable relief in this

TRADE SECRET WATCH BLOG, (June 30, 2016), http://blogs.orrick.com/trade-secrets-watch/2016/06/30/california-federal-court-first-to-rule-under-new-defend-trade-secrets-act-of-2016/.

[74] *See generally*, Henry Schein, Inc. v. Cook, 191 F. Supp. 3d 1072 (N.D. Cal. 2016).

[75] *Id.*

[76] *Id.* at 1079–80.

[77] 2016 LEXIS 81369, at *6-7.

[78] Panera, LLC v. Nettles, No. 4:16-CV-1181-JAR, 2016 WL 4124114, at *1 (E.D. Mo. Aug. 3, 2016).

[79] *Id.*

[80] *Id.*

[81] Importantly, the court did not directly analyze the trade secret misappropriation claim under the DTSA framework but instead noted that, "[a]lthough the Court's analysis has focused on Panera's Missouri trade secrets claim, an analysis under the Defend Trade Secrets Act would likely reach a similar conclusion." *Id.* at 4, n. 2.

[82] *Id.* at 2.

[83] *Id.* at 4.

form because it most clearly represents the original intent of the restrictive covenant entered into by the departing employee or most effectively protects the valuable trade secret information imperiled by the departing employee. Often, a restraint on trade is the *only* way of preventing the inevitable disclosure[84] of highly confidential and highly profitable trade secrets. If a company is denied the availability of injunctive relief, they are denied the most effective tool available. This is why the Computer Fraud and Abuse Act, which does not contain a carve-out for states that disfavor or prohibit restraints on trade, may be a more effective tool for combating trade secret misappropriation—as it leaves open the option of injunctive relief in the form of a constructive restraint on trade.

A recently filed case in the Northern District of California serves as an exemplar of the confusing landscape wrought by the various trade secret laws and the myriad considerations counsel must take into account when seeking both venue and remedy for an alleged trade secret misappropriation. On February 23, 2017, Waymo, LLC ("Waymo") filed suit against Uber Technologies Inc. ("Uber"), alleging violation of both the DTSA and the California UTSA.[85] Waymo, a Google Inc. subsidiary, specializes in driverless car technology.[86] In its complaint against Uber, Waymo alleges that in January of 2016, Anthony Levandowski, a former manager at Waymo, stole confidential, proprietary information and trade secrets before departing Waymo to form his own company that would eventually be bought by Uber for $680 million.[87] Waymo alleges that. "[i]n December 2015, Mr. Levandowski specifically searched for and then installed specialized software onto his company-issued laptop in order to access the server that stores these particular files. Once Mr. Levandowski accessed this server, he downloaded the 14,000 files, representing approximately 9.7 GB of highly confidential data."[88] Waymo further alleges that, "[a] number of Waymo employees subsequently also left to join Anthony Levandowski's new business, downloading additional Waymo trade secrets in the days and hours prior to their departure. These secrets included confidential supplier lists, manufacturing details and statements of work with highly technical information."[89]

These allegations are important for several reasons. First, although Waymo did not discover the alleged misappropriation until some months later and is not pursuing a claim under the Computer Fraud and Abuse Act, the allegation that Levandowski had to install specialized software to access the files he allegedly stole could be a basis for "exceeding authorized access" under the CFAA in jurisdictions that recognize the CFAA as a means of redress for trade secret misappropriation by internal employees. Had Waymo discovered the alleged misappropriation sooner and filed for a TRO, Levandowski could have potentially been enjoined from forming his new company and using the allegedly misappropriated trade secrets. Unfortunately, this route would have been rife with challenges because this suit is being brought in the

[84] For a discussion on the inevitable disclosure doctrine, *see* PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).

[85] Waymo LLC v. Uber Technologies, Inc. et al, No. 3:17-cv-00939, (N.D. Cal. filed Feb. 23, 2017).

[86] *See generally*, WAYMO, https://waymo.com/.

[87] *See generally*, Plaintiff's Complaint ("Pl's Compl."), ECF No. 1 at ¶¶ 1-8.

[88] *Id.* at ¶ 4.

[89] *Id*. at ¶ 6.

Northern District of California, in which case *Nosal* controls. Because *Nosal* and the Ninth Circuit interpretation of the CFAA controls, it would prevent interpretation of the CFAA to apply to internal employee hacking as a means to redress trade secret misappropriation. Thus, even though the trade secrets at issue here were allegedly accessed by electronic means, and even though using the CFAA would allow Waymo to file suit in California without having to consider California's prohibition on restraints of trade, counsel for Waymo is limited to the UTSA and DTSA because of the unresolved circuit split and the Ninth Circuit's decision to not allow the CFAA to be applied to internal employees when they exceed authorized access.

Moreover, because this suit is being brought in the Northern District of California for violation of the Defend Trade Secrets Act, counsel for Waymo will be constrained by the DTSA provision which prevents any injunction from "conflict[ing] with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business…").[90] As examined in the discussion on *Panera*, this is not a consideration in states that do not prohibit restraints on trade. Thus, while the DTSA provides federal subject matter jurisdiction in this case, it is arguably undercut by the venue's prohibition on restraints of trade.

CONCLUSION

The purported goal of the Defend Trade Secrets Act was to bring order to chaos, to harmonize the variances in judicial interpretation of the Uniform Trade Secrets Act, and to empower private litigants with a new federal cause of action. This goal is severely curtailed by the state non-compete carve-out, which hamstrings a plaintiff's use of injunctive relief where it might run afoul of state non-compete provisions. *Henry Schein, Inc. v. Cook* demonstrates how seriously limiting state policies disfavoring non-competes can be on the efficacy of injunctive relief when pursued under the Defend Trade Secrets Act. Given recent trends and White House initiatives (discussed *supra*) to persuade state lawmakers to oppose enforcement of non-compete provisions, the Defend Trade Secret Act could end up being as ineffective at unifying trade secret law as previous attempts at standardization have been.

Moreover, given business's increasing reliance on electronic storage, it is likely that most future trade secret misappropriation cases will involve electronic access. Therefore, it may be preferable when bringing an action in a state that prohibits or disfavors enforcement of non-compete provisions to proceed under the Computer Fraud and Abuse Act rather than run the risk of potentially losing injunctive relief under the Defend Trade Secrets Act. However, as examined in the counterfactual situation with the ongoing *Waymo* lawsuit, even this may not be a viable option until

[90] *See* 18 U.S.C. § 1836(3)(A)(i)(I-II) (2016), which states: "In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may … grant an injunction … to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not … prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or … otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business…."

the Supreme Court reconciles the circuit split regarding whether an internal employee can be liable for violation of the CFAA when accessing trade secrets.

As more cases are decided under the Defend Trade Secrets Act and more states join the trend of prohibiting or disfavoring enforcement of non-compete provisions, it may exacerbate the potential irrelevance of the Defend Trade Secrets Act as a viable means for employers to prohibit the post-employment actions of its former employees and protect valuable trade secrets which encourage innovation and propel our economy forward.