St. Mary's Law Journal

Volume 45 | Number 3 Article 3

1-1-2014

The Computer Fraud and Abuse Act: An Attractive but Risky Alternative to Texas Trade Secret Law.

Paul Hanna

Matthew Leal

COMMENT

THE COMPUTER FRAUD AND ABUSE ACT: AN ATTRACTIVE BUT RISKY ALTERNATIVE TO TEXAS TRADE SECRET LAW

PAUL HANNA & MATTHEW LEAL

I. INTRODUCTION

A business hires an employee to assist in its business venture. The business authorizes the employee to use company computers for a variety of tasks, but after a brief period of employment, the employee decides he no longer wants to work for the business because he could generate more income by working for one of the business's many competitors or by simply going into business for himself. Unbeknownst to the business, and prior to terminating employment with the business, the employee uses his issued username and password to log on to his workstation and downloads several documents from the business's server. Soon after the employee downloads the information, the employee quits.[1]

Several concerns come to mind. What information did the employee have access to? Will the employee use that information to take clients from the business? What can the business do to prevent the employee from using the information to the detriment of the business? Can the business hold the employee liable for monetary damages?[2] A forensic computer analyst can provide an answer to the quandary of what information the former employee had access to,[3] and only the employee can attest to what his intentions are for the information he obtained. Guidance on the remaining two questions, possible monetary damages for lost revenue and injunctive relief, will likely require hiring an attorney.

For Texas attorneys posed with these issues, the legal landscape has

1. Hypothetical loosely based on Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *1 (N.D. Tex. Apr. 20, 2011), which involved a suit brought under the Computer Fraud and Abuse Act in which the defendant allegedly worked for the plaintiff's meat supply company as a general manager, had access to miscellaneous confidential information via the company's computers, accessed that confidential information, quit the company, and used that confidential information in an independent business venture.

2. In a recent article relating to the Computer Fraud and Abuse Act by Pamela Taylor, Comment, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 202–03 (2012), the author acknowledged that a hypothetical similar to the one addressed in this Comment raises additional questions relating more specifically to the applicability of the Computer Fraud and Abuse Act.

3. *See* Victoria A. Cundiff, *Digital Defense: Protecting Trade Secrets Against New Threats*, *in* 14th Annual Institute on Intellectual Property Law, 707, 727 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 947, 2008) ("Forensic analysis can show, in digital terms, that information has been deleted, transferred or altered . . . [and] provide circumstantial evidence of misappropriation or improper conduct.").

recently changed.[4] As of September 1, 2013,[5] Texas joined forty-six other states by adopting the Uniform Trade Secrets Act (UTSA).[6] Prior to the adoption of UTSA, known in Texas as the Texas Uniform Trade Secrets Act (TUTSA),[7] the common law tort of misappropriation of a trade secret provided one plausible avenue to hold the employee civilly liable for monetary damages[8] or to secure a permanent injunction to prevent the employee's use of the information in competition with the business.[9] TUTSA codified the common law with the intention of providing greater uniformity and an easier framework for practitioners through clear guidelines and definitions.[10] Despite the addition of TUTSA to Texas trade secret law, successfully establishing liability for the misappropriation of a trade secret still requires overcoming several common law obstacles that could prevent recovery.[11] For example, the attorney may have

4. On May 2, 2013, Governor Rick Perry signed into law the Texas Uniform Trade Secret Act (TUTSA), which became effective September 1, 2013. TEX. CIV. PRAC. & REM. CODE ANN. §§ 134A.001–.008 (West Supp. 2013). The effect of this law is to provide uniformity and modernization of the Texas common law. *See id.* § 134A.008 (announcing that the purpose of the statute is "to make uniform the law" with all other states adopting similar model language); *see also* Joseph F. Cleveland Jr. & J. Heath Coffman, *Protecting Trade Secrets Made Simple*, 76 TEX. B.J. 751, 752 (2013) ("TUTSA codifies and modernizes Texas law on misappropriation of trade secrets by providing a simple legislative framework for litigating trade secret cases.").

5. CIV. PRAC. & REM. §§ 134A.001–.008.

6. *Trade Secrets Act Enactment Status Map*, UNIFORM L. COMMISSION, http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act (last visited Nov. 6, 2013).

7. CIV. PRAC. & REM. § 134A.001.

8. *See* Calce v. Dorado Exploration, Inc., 309 S.W.3d 719, 738 (Tex. App.—Dallas 2010, no pet.) (citing Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1208 (5th Cir. 1986)) (providing factors to consider in calculating monetary damages for the misappropriation of a trade secret based on considerations the plaintiff would account for if he were to license the trade secret, which include the effect on the plaintiff's position resulting from the use of the trade secret; a price the plaintiff charged for its use in the past; the actual value of the information; the degree of past and intended future use of the information; and any other relevant factors); Rusty's Weigh Scales and Serv., Inc. v. N. Tex. Scales, Inc., 314 S.W.3d 105, 110–13 (Tex. App.—El Paso 2010, no pet.) (establishing that successful litigation of a misappropriation of trade secrets claim could lead to the plaintiff's recovery for lost profits, out-of-pocket damages, and exemplary damages in certain instances).

9. *See* Zoecon Indus. v. Am. Stockman Tag Co., 713 F.2d 1174, 1180 (5th Cir. 1983) (citing Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 778 (1958)) (affirming that a permanent injunction is a possible form of relief in a misappropriation of a trade secret claim); Mabrey v. SandStream, Inc., 124 S.W.3d 302, 310–11 (Tex. App.—Fort Worth 2003, no pet.) (reiterating the principle that a court may grant a temporary injunction where a plaintiff alleges misappropriation of a trade secret, but the injunction is not dispositive of whether a trade secret in fact exists).

10. *See* CIV. PRAC. & REM. §§ 134A.007–.008 (providing guidance as to the effect of TUTSA and its "general purpose to make uniform the law"); *see also* Joseph F. Cleveland Jr. & J. Heath Coffman, *Protecting Trade Secrets Made Simple*, 76 TEX. B.J. 751, 752 (2013) (discussing how TUTSA modernizes Texas trade secret law).

11. *Compare* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—

difficulty proving the information obtained qualifies as a trade secret,[12] or when the attorney is seeking monetary relief, that the information obtained by the employee was used or disclosed.[13] In fact, the court or jury could find that the information is not a trade secret or that the employee's subsequent actions do not qualify as use or disclosure, in which case the employer will be unable to secure any form of relief.[14]

As an alternative to Texas trade secret law, the Texas litigator could pursue liability for damages[15] and obtain an injunction under the Computer Fraud and Abuse Act (CFAA).[16] However, similar to Texas

---

Austin 2004, pet. denied) (citing IBP, Inc. v. Klumpe, 101 S.W.3d 461, 467 (Tex. App.—Amarillo 2001, pet. denied)) (recovering for misappropriation of a trade secret hinges on establishing: (1) that the information is actually a trade secret; (2) that securing the trade secret constituted a violation of a duty owed based on a relationship between parties or by other inappropriate actions; (3) that the defendant applied the trade secret in some fashion; and (4) that there was resulting injury to the plaintiff), *with* CIV. PRAC. & REM. §§ 134A.001–.008 (West Supp. 2013) (requiring plaintiffs to prove the existence of a trade secret, that a misappropriation occurred either through an acquisition by "improper means" or "disclosure or use of trade secret of another without express or implied consent," and that the plaintiff suffered damages).

12. TUTSA defines "trade secrets" as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, [or] process, [that] . . . derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use[,] and . . . is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

CIV. PRAC. & REM. § 134A.002(6).

13. *Compare Trilogy Software*, 143 S.W.3d at 463 (Tex. App.—Austin 2004, pet. denied) (citing *Klumpe*, 101 S.W.3d at 467) (stating the required elements of a misappropriation claim including the "existence of a trade secret" and "use of the trade secret"), *with* CIV. PRAC. & REM. § 134A.002(3) (delineating the definition of "misappropriation" to include "the acquisition of a trade secret" by "improper means" or the "disclosure or use of trade secret of another without express or implied consent").

14. *See* McClain v. State, 269 S.W.3d 191, 196–97 (Tex. App.—Texarkana 2008, no pet.) (finding that "backsheets were public knowledge"). The court restated, "Matters of general knowledge in an industry cannot be appropriated by one as his secret." *Id.* (quoting Wissman v. Boucher, 150 Tex. 326, 240 S.W.2d 278, 280 (1951) (internal quotation marks omitted)).

15. *See* Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *1 (N.D. Tex. Apr. 20, 2011) (providing an example of sufficient alleged facts to support a cause of action under the Computer Fraud and Abuse Act). The plaintiff alleged that the defendant worked for the plaintiff's meat supplying company as a general manager and had access to miscellaneous confidential information via the company's computers. *Id.* The defendant allegedly accessed said confidential information, subsequently quit the company, and then used said confidential information in an independent business venture. *Id.*

16. 18 U.S.C. § 1030(g) (Supp. V 2011). A plaintiff may file a CFAA claim concurrently with a TUTSA claim; however, this Comment decouples the two causes of action to determine when each would more advantageous. *See, e.g.*, Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1155 (5th Cir. 2006) (ruling on a dispute where the plaintiff "sought damages and injunctive relief under . . . the CFAA to compensate for the cost of data recovery and to prevent the defendants from continuing to

trade secret laws, there are several concerns associated with relying on the CFAA in circumstances similar to the hypothetical discussed above. Notably, there is a federal circuit court split over what type of access is considered unauthorized or beyond the scope allowed to an employee under the CFAA,[17] and Congress is considering amendments that would limit the scope of the CFAA.[18]

To demonstrate why the CFAA is a workable alternative to Texas trade secret laws and, at the same time, highlight its associated risks, it is necessary to review applicable Texas trade secret laws as well as the purpose and contemporary interpretations of the CFAA. Juxtaposing the two causes of action provides Texas litigators with a starting point to analyze which cause of action is better suited for their clients, particularly when an employee with authorized access to a computer obtains information from that computer in contemplation of competing with the employer.

II. TEXAS TRADE SECRET LAWS

A. *What Is a Trade Secret in Texas?*

While regulation of patented material falls within the jurisdiction of the federal government,[19] state laws govern trade secrets.[20] In the civil

use and disseminate [plaintiff's] trade secrets"); P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 505–07 (3d Cir. 2005) (expounding on a trade secret and a CFAA dispute between Party City and former employees who created a competing enterprise).

17. *See, e.g.*, United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (applying the intended-use analysis to determine what constitutes unauthorized access); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (interpreting the CFAA strictly to mean that unauthorized access only occurs if an employee uses a company's computer system without authorization); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (reading the CFAA liberally and holding that an unauthorized access occurs when an employee's interests are contrary to his employer's); *see also* Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (noting a split between district courts over sufficient losses to support a CFAA claim); Michael R. Greco, *CFAA Does Not Apply to Employee Data Theft According to Ninth Circuit*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/computers-office-equipment/article_Fisher-Phillips-LLP_1495924.htm (identifying a circuit court split over interpretations of the CFAA).

18. *See* S. 3342, 112th Cong. § 306 (2012) (modifying the CFAA in a proposed amendment that would limit the applicability of the CFAA).

19. 35 U.S.C. § 2 (2006) (delegating authority to the United States Patent and Trademark Office to regulate and authorize patents); *see also* Hyde Corp. v Huffines, 158 Tex. 566, 314 S.W.2d 763, 770–71 (1958) (citing Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938), Becher v. Contoure Labs, 279 U.S. 388 (1929), E. I. Du Pont de Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917)) (surveying U.S. Supreme Court precedent to confirm that trade secret claims are distinct from patent

context, most states have adopted a definition of trade secrets similar to the one found in UTSA.[21] UTSA defines "trade secrets" as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that . . . derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and . . . is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[22]

As mentioned above, Texas is now among the states that have adopted UTSA.[23] Two additional requirements of a trade secret dictated by UTSA are that the information has some "economic value" and that the information "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[24]

---

claims, that patent claims fall within the jurisdiction of the federal government, and that trade secret claims fall within the original jurisdiction of state courts, unless filed in a federal court under diversity jurisdiction).

20. *See* TEX. CIV. PRAC. & REM. CODE ANN. §§ 134A.001–.008 (West Supp. 2013); *Id.* § 16.010 (West 2006) (establishing a statute of limitation for civil suits involving the misappropriation of trade secrets under Texas law); *see also* Weightman v. State, 975 S.W.2d 621, 628 (Tex. Crim. App. 1998) (en banc) (citing Schalk v. State, 823 S.W.2d 633, 640 (Tex. Crim. App. 1991)) (discussing the requisite degree of secrecy to establish a criminal trade secret misappropriation charge and holding that "absolute secrecy is not required"). *But see* 18 U.S.C. § 18 (2006) (providing that a federal cause of action exists for the misappropriation of a trade secret, but only in certain instances). Though outside of the scope of this Comment, in the criminal context, Texas penal statutes define a trade secret as "the whole or any part of any scientific or technical information, design, process, procedure, formula, or improvement that has value and that the owner has taken measures to prevent from becoming available to persons other than those selected by the owner to have access for limited purposes." TEX. PENAL CODE ANN. § 31.05(a)(4) (West 2006) (providing a state definition for trade secret in the context of a criminal suit and declaring that theft of trade secrets qualifies as a criminal offense under state law in certain instances).

21. *Trade Secrets Act Enactment Status Map*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/Act.aspx?title =Trade%20Secrets%20Act (last visited Nov. 6, 2013); *see also* Ted Lee & Leila Ben Debba, *Backdoor Non–Competes In Texas: Trade Secrets*, 36 ST. MARY'S L.J. 483, 486 n.7 (2005) (listing the states that have adopted the Uniform Trade Secrets Act).

22. UNIF. TRADE SECRETS ACT § 1(4) (amended 1985) 14 U.L.A. 538 (2005).

23. *See* CIV. PRAC. & REM. §§ 134A.001–.008 (West Supp. 2013); *Trade Secrets Act Enactment Status Map*, UNIFORM L. COMMISSION, http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act (last visited Nov. 6, 2013).

24. CIV. PRAC. & REM. § 134A.002(6)(A),(B); *see also* Joseph F. Cleveland Jr. & J. Heath Coffman, *Protecting Trade Secrets Made Simple*, 76 TEX. B.J. 751, 753 (2013) (discussing the "expansive definition of protectable trade secrets" that TUTSA now provides). TUTSA lists the subparts of what constitutes a "trade secret" to include information that:

> [D]erives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use[,] and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Prior to the adoption of TUTSA, Texas case law provided an alternative definition for trade secrets in the context of civil liability, relying heavily on the *Restatement (First) of Torts* section 757.[25] This definition was "any formula, pattern, device[,] or compilation of information which is used in one's business and presents an opportunity to obtain an advantage over competitors who do not know or use it."[26] Additionally, at common law, there was a requirement that "a substantial element of secrecy" surround the information.[27] This secrecy element was satisfied when the owner showed that the information would be secure, unless acquired by "improper means."[28] As will be discussed below, understanding the differences between the common law and TUTSA provides a useful framework to estimate how TUTSA will be interpreted and applied by courts.[29]

To determine whether civil liability attaches to the actions of the employee in the hypothetical presented above and to explore the differences between pursuing liability under the CFAA and Texas trade secret law, it is necessary to go beyond the established definition of a trade secret. The following section delineates the cause of action for misappropriation of trade secrets in Texas, focusing on recent changes resulting from the passage of TUTSA.

CIV. PRAC. & REM. § 134A.002(6)(A), (B).

25. Computer Assocs. Int'l, Inc. v. Altai, Inc., 918 S.W.2d 453, 455 (Tex. 1994) (citing Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 766 (1958) (quoting RESTATEMENT (FIRST) OF TORTS § 757 (1939))) (providing a definition of trade secret in the context of a civil action).

26. *In re* Goodyear Tire & Rubber Co., 392 S.W.3d 687, 692 (Tex. App.—Dallas 2010, no pet.); *accord* Altai, 918 S.W.2d at 455 (citing *Huffines*, 314 S.W.2d at 766 (quoting RESTATEMENT (FIRST) OF TORTS § 757 (1939))) (defining a trade secret and weighing whether to apply the discovery rule to toll the two-year state of limitations applicable for a misappropriation of trade secrets claim at that time); *see also* Am. Precision Vibrator Co. v. Nat'l Air Vibrator Co., 764 S.W.2d 274, 276 (Tex. App.—Houston [1st Dist.] 1988, no writ) (restating the definition of a trade secret and finding that customer lists fall within the scope of that definition).

27. Astoria Indus. of Iowa, Inc. v. SNF, Inc., 223 S.W.3d 616, 634 (Tex App.—Fort Worth 2007, pet. denied).

28. McClaine v. State, 269 S.W.3d 191, 195 (Tex. App.—Texarkana 2008, no pet.) (citing Q-Co Indus., Inc. v. Hoffman, 625 F. Supp. 608 (S.D.N.Y. 1995)).

29. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995) ("The original Act or its 1985 revision has been adopted in a majority of the states . . . . *Except as otherwise noted*, the principles of trade secret law described in this Restatement *are applicable to actions under the [UTSA] as well as to actions at common law*." (emphasis added)); *see, e.g.*, Tex. Dep't of Pub. Safety v. Cox Tex. Newspapers, LP, 343 S.W.3d 112, 126 n.5 (Tex. 2011) (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39, 40–41 (1995)) (relying on the Restatement to support its definition of a trade secret); *In re* Bass, 113 S.W.3d 735, 740 (Tex. 2003) (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995)) (concurring with the Restatement's position and acknowledging it as the majority view—that all six-factors do not need to be satisfied for information to meet the definition of a trade secret).

B. *The Tort of Misappropriation of a Trade Secret*

Prior to TUTSA, a plaintiff–employer seeking monetary damages was required to show four elements to establish the tort of misappropriation of a trade secret against a former employee.[30] The plaintiff had to demonstrate that: (1) the information in dispute qualified as a trade secret, (2) there was a "breach of a confidential relationship or improper discovery of a trade secret," (3) the defendant used the trade secret, and (4) the plaintiff suffered damages.[31] TUTSA does not lessen the common law burden when the plaintiff–employer is seeking monetary damages.[32]

It is important to note, however, that prior to TUTSA, Texas common law allowed former employers to seek injunctive relief by merely showing the information had been obtained through improper means.[33] TUTSA also allows plaintiffs to enjoin a former employee without a showing of use or disclosure.[34] Although it is beyond the scope of this Comment, the enactment of TUTSA left a lingering question in Texas trade secret law[35]—whether a former employer may enjoin a former employee from commencing employment under the doctrine of "inevitable disclosure."[36]

---

30. *See* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—Austin 2004, pet. denied) (citing IBP, Inc. v. Klumpe, 101 S.W.3d 461, 476 (Tex. App.—Amarillo 2001, pet. denied)) (reiterating the common law elements for misappropriation of a trade secret in a suit between a plaintiff–employer and a former employee who, after dismissal, secured employment with a client of the plaintiff–employer).

31. *Trilogy Software*, 143 S.W.3d at 463 (citing *Klumpe*, 101 S.W.3d at 476).

32. *Compare Trilogy Software*, 143 S.W.3d at 463 (delineating the common law elements of a misappropriation of trade secrets claim), *with* TEX. CIV. PRAC. & REM. CODE ANN. §§ 134A.002–.004 (West Supp. 2013) (providing that a plaintiff must prove the following elements for a TUTSA claim to recover monetary damages: (1) the information must meet the definition of a trade secret; (2) the defendant or respondent must have misappropriated the trade secret; and (3) the misappropriation must have caused actual damages).

33. *See* Rugen v. Interactive Bus. Sys., Inc., 864 S.W.2d 548, 552 (Tex. App.—Dallas 1993, no writ) (enjoining a former employee from disclosing trade secrets to a new employer, although no use or disclosure had yet occurred); Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 762 (2013) (citing *Rugen*, 864 S.W.2d at 552) (identifying the *Rugen* doctrine to be a modification of the inevitable disclosure doctrine).

34. *See* CIV. PRAC. & REM. § 134A.002(3) (allowing a misappropriation claim to not only be based on "the disclosure or use of a trade secret," but also the "*acquisition* of a trade secret . . . by improper means" (emphasis added)).

35. Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 762 (2013) ("In the end, the Legislature's decision to leave this issue open will likely lead to more litigation until the courts reach a consensus and either expressly adopt or reject the inevitable disclosure doctrine . . . .").

36. *See* PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1271 (7th Cir. 1995) (concluding that a former PepsiCo employee, Redmond, should be temporarily enjoined from working for the competitor, Quaker, because his position would lead to the inevitable disclosure of PepsiCo trade secrets); Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 758 (2013) (describing the inevitable disclosure doctrine as a vehicle for employers to prevent former employees from working for a competitor

1. The First Obstacle to Recovery—Establishing the Existence of a Trade Secret

Under the common law, Texas relied on the *Restatement (First) of Torts* section 757 definition of a trade secret.[37] Though a new definition has been provided by TUTSA,[38] examining the previous meaning offers a supplemental analysis for determining what business information qualifies as a trade secret.[39] This will continue to be true, as other states that have adopted UTSA continue to look to the Restatement for additional guidance.[40] Comment b to section 757 clarifies that not all information used for conducting business qualifies as a trade secret.[41] For example, information known by the public, information known within a particular industry, and information that is evident about a product from its use does not qualify as a trade secret.[42] Yet, trade secret protections are not limited to information known only to employers.[43]

---

merely because of the anticipated or future threat that the former employee might inevitably disclose the trade secret during the course of their employment).

37. *See* Computer Assocs. Int'l, Inc. v. Altai, Inc., 918 S.W.2d 453, 455 (Tex. 1994) (citing Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 776 (quoting RESTATEMENT (FIRST) OF TORTS § 757 (1939))) (adopting the RESTATEMENT (FIRST) OF TORTS definition for trade secrets).

38. CIV. PRAC. & REM. § 134A.002(6).

39. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (clarifying, in comment b, the definition of a trade secret).

40. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995) (discussing the doctrinal development of the RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995)).

> In 1979, the National Conference of Commissioners on Uniform State Laws promulgated the Uniform Trade Secrets Act. The Prefatory Note states that the "Uniform Act codifies the basic principles of common law trade secret protection." The original Act or its 1985 revision has been adopted in a majority of the states. . . . *Except as otherwise noted, the principles of trade secret law described in this Restatement are applicable to actions under the Uniform Trade Secrets Act as well as to actions at common law.* The concept of a trade secret as defined in this Section is intended to be consistent with the definition of "trade secret" in § 1(4) of the Act.

Id. (emphasis added); *see, e.g.*, Tex. Dep't of Pub. Safety v. Cox Tex. Newspapers, LP, 343 S.W.3d 112, 126 n.5 (Tex. 2011) (recognizing the RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39, 40, 41 (1995) as a source that Texas courts reference to guide their analysis of what constitutes a trade secret and what appropriate remedies are available); *In re* Bass, 113 S.W.3d 735, 740 (Tex. 2003) (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995)) (agreeing with the Restatement and the majority of jurisdictions who, at the time, followed the six-factor test with the understanding that a party did not have to prove all six factors to meet the definition of a trade secret).

41. *Cf.* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (elaborating on the characterization of a trade secret by clarifying that a trade secret "differs from other secret information in a business" because of its usefulness on a continuous basis such as where "a code for determining discounts" is distinct from the particular "terms of a secret bid for a contract" that will not be reused).

42. *See id.* (stating in comment b. that "[m]atters of public knowledge or of general knowledge

Though not an exhaustive list, the *Restatement (First) of Torts* provides the following examples of trade secrets, which are still valid under UTSA:[44] information only used for a single transaction, such as the price associated with a contract for service or specialized terms included in a proposal; information used to ascertain end results in manufacturing processes; and information that relates to the ongoing conduct of the business, such as customer lists, pricing data, and administration of the internal affairs of the business.[45]

As mentioned above, many states that have adopted UTSA still look to the *Restatement (First) of Torts* to supplement their determination of whether a trade secret exists.[46] Additionally, the *Restatement (Third) of Unfair Competition*, which is widely considered to be an update to UTSA, clarifies that the original six-factor test outlined in the *Restatement (First) of Torts* section 757[47] is still highly relevant to determining whether a trade secret exists.[48] The six factors consist of:

> (1) the extent to which the information is known outside [the] business;
> (2) the extent to which the information is known by employees and others involved in [the] business;
> (3) the extent of the measures taken by [the business] to guard the secrecy of the information;
> (4) the value of the information to [the business] and to [its] competitors;
> (5) the amount of effort or money expended by [the business] in developing the information; [and]
> (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[49]

---

in an industry . . . [and matters] which are completely disclosed by the goods which one markets" are not trade secrets).

43. *See id.* (attempting to clarify the constructs of a trade secret by suggesting that there is no requirement "that only the proprietor of the business know [of the secret]").

44. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995) (discussing how the current version of the RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. B (1995) incorporates the common law and the RESTATEMENT (FIRST) OF TORTS § 757 cmt. b, and to the extent applicable, is compatible with the provisions of UTSA).

45. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (elaborating on various examples of trade secrets and what does not qualify as a trade secret).

46. *See, e.g.*, *In re* Bass, 113 S.W.3d 735, 739–42 (Tex. 2003) (holding in a challenge over mineral rights that the RESTATEMENT (FIRST) OF TORTS is controlling on the issue of whether a trade secret exists, and that it is appropriate to evaluate the six-factor test outlined in the Restatement in concurrence with the characteristics of the disputed information).

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

48. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995) ("[T]he principles of trade secret law described in this Restatement are applicable to actions under the Uniform Trade Secret Act as well as to actions at common law.").

49. *Bass*, 113 S.W.3d at 739 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)).

Although the factors provide clarity to the question of whether a trade secret exists, Texas courts have inserted a degree of ambiguity into the application of this test by recognizing that all six factors do not have to be satisfied by the party asserting that a trade secret exists[50] and by acknowledging that the six-factor list is not exhaustive.[51]

Whether establishing the existence of a trade secret under TUTSA or the six-factor test, practitioners must be aware that, at its basic level, the definition of a trade secret can be broken down into three essential elements: (1) the information must not be generally known;[52] (2) it must have some economic value;[53] and (3) the plaintiff must have expended reasonable efforts to maintain its secrecy.[54]

Returning to the employment hypothetical presented above, if the plaintiff–employer is unable to prove that the information obtained from company computers is a trade secret, either plainly under TUTSA or with the help of Texas's six-factor test, the employer will be unable to recover monetary damages or secure injunctive relief under Texas trade secret laws.[55] However, as discussed below, the employer may still have an opportunity to recover under the CFAA because it does not condition recovery on the nature of the information obtained.[56]

---

50. *See Bass*, 113 S.W.3d at 740 (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995)) (emphasizing that "the party claiming a trade secret should not be required to satisfy all six factors because trade secrets do not fit neatly into each factor every time").

51. *See Bass*, 113 S.W.3d at 740 (suggesting that numerous considerations may be relevant to a judicial inquiry into whether a trade secret exists).

52. *See* TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(6) (West Supp. 2013) (providing the definition of a trade secret); *Bass*, 113 S.W.3d at 739 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (providing six factors to consider to determine whether information should be deemed a trade secret).

53. *See* CIV. PRAC. & REM. § 134A.002(6)(A) (requiring that a trade secret "derives independent economic value" from its clandestine nature); *Bass*, 113 S.W.3d at 739 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (including "the value of the information" as a factor to consider in "determining whether given information is [a] trade secret").

54. CIV. PRAC. & REM. § 134A.002(6)(B) (necessitating that the information be the "subject of efforts that are reasonable under the circumstances to maintain its secrecy" in order to meet the second prong of TUTSA's definition of a trade secret); *see Bass*, 113 S.W.3d at 739 n.1 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (listing "the extent of measures taken [by the secret owner] to guard the secrecy of the information" as a factor to be considered in determining whether the information in question qualifies as a trade secret).

55. *See* Tex. Integrated Conveyor Sys., Inc. v. Innovative Conveyor Concepts, Inc., 300 S.W.3d 348, 370–74 (Tex. App.—Dallas 2009, pet. denied) (considering whether summary judgment is appropriate when the issue of whether a trade secret exists is unresolved).

56. *See* 18 U.S.C. § 1030(a)(2) (2006 & Supp. V 2011) (providing civil liability where a party "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer," but omitting any reference to the nature or value of the information obtained).

2. The Second Obstacle to Recovery—Establishing a Relationship of Confidence

Once the employer in the hypothetical described above establishes that a trade secret exists, the employer will encounter the second obstacle to recovery—demonstrating that a breach of confidence resulted from the use or disclosure of the trade secret.[57] Demonstrating such a breach is uniquely relevant to actions between an employer and former employee because agency principles establish a relationship of confidence between the parties.[58]

According to agency principles, a relationship of confidence exists between an employee and an employer as an extension of the employee's duty to refrain from using information in contradiction to her obligations as an employee or in a manner that competes with or harms the employer.[59] This includes information the employer provided to the employee in confidence or discovered by the employee as a result of her employment.[60] The duty owed by the employee to the employer exists without regard to whether there was an express agreement to refrain from using the information obtained as an employee.[61] Although the presence of a relationship of confidence is readily established in the employee–

57. *See* CIV. PRAC. & REM. § 134A.002(2)–(3) (allowing action to be taken against those who acquire, disclose, or use a trade secret without authorization or through improper means, either of which would constitute a breach of an employee's duty of loyalty); Twister B.V. v. Newton Research Partners, LP, 364 S.W.3d 428, 437–38 (Tex. App.—Dallas 2012, no pet.) (identifying the elements of a misappropriation of a trade secret claim and, in doing so, acknowledging the requisite breach of a relationship of confidence between parties); *see also* RESTATEMENT (FIRST) OF TORTS § 757 (1939) (expressing that liability for unprivileged use of a trade secret occurs where there is a breach of a confidential relationship from said use).

58. *See* Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 769 (1958) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. j (1939)) ("The chief example of a confidential relationship under [the rule on liability for disclosure or use of another's trade secret] is the relationship of principal and agent . . . ."); *see also* RESTATEMENT (SECOND) OF AGENCY § 395 (1958) (establishing a duty not to disclose information learned through employment and prohibiting use of information learned through employment in competition with or to the detriment of the employer).

59. *See* RESTATEMENT (SECOND) OF AGENCY § 395 (1958) (placing a fiduciary duty to not compete or act contrary to the interests of the agent's principal).

60. *See id.* ("[A]n agent is subject to a duty to the principal not to use or to communicated information confidentially given him . . . or acquired by him during the course of or on account of his agency or in violation of his duties as agent, in competition with or to the injury of the principal . . . .").

61. *See* Am. Derringer Corp. v. Bond, 924 S.W.2d 773, 777 (Tex. App.—Waco 1996, no writ) (citing *Huffines*, 314 S.W.2d at 763) (reiterating that, in the context of a suit to establish liability "between an employer and an employee," the plaintiff does not need to prove that an express agreement exists between the parties to prove a misappropriation of a trade secret claim based on a confidential relationship).

employer context because of agency principles, the plaintiff–employer still must prove a breach of that relationship.[62]

Revisiting the hypothetical above, if the information taken by the employee was accessible by every employee and did not contain any warnings clearly labeling the information as secret, proving a breach of duty might prove challenging for the employer. This is not only because the information, stored in such an innocuous manner, might not meet the requirement that the information be reasonably protected,[63] but also because the employee's action might not contain the requisite scienter to establish a breach of duty.[64]

3. The Third Obstacle to Recovery—Establishing Disclosure or Use

Texas courts agree that a relationship of confidence exists between employers and employees.[65] Furthermore, TUTSA[66] and Texas common law acknowledge that a breach of confidence occurs when an employee uses or discloses a trade secret.[67] However, when a plaintiff–employer seeks monetary damages, if the defendant did not disclose or use the trade

62. *See* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—Austin 2004, pet. denied) (citing IBP, Inc. v. Klumpe, 101 S.W.3d 461, 467 (Tex. App.—Amarillo 2001, pet. denied)) (restating the common law elements for misappropriation of a trade secret in regard to a suit between the employer and a former employee, who obtained a position with the previous employer's client after dismissal).

63. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(6)(B) (West Supp. 2013); *In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)).

64. *See* CIV. PRAC. & REM. CODE § 134A.002(3) (delineating that a trade secret be either acquired through improper means, or disclosed or used "without the express or implied consent" of its owner); *see also* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991) (Posner, J.) (discussing the dual nature associated with the requirement that reasonable efforts be taken to protect a trade secret and identifying that the requirement serves "both [an] evidentiary and remedial significance"); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) (requiring the "actor [know] or [have] reason to know" that the action taken to procure the trade secret was improper).

65. *See Huffines*, 314 S.W.2d at 769 (citing RESTATEMENT (SECOND) OF AGENCY § 395–96 (1958)) (emphasizing that the relationship of an employer and employee is the primary example of a relationship of confidence).

66. *See* CIV. PRAC. & REM. § 134A.002(3)(B)(ii)(b), (c) (suggesting that in order to establish "misappropriation" in the context of "disclosure or use[,]" it is imperative to include instances in which the trade secret was "acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or derived from or through a person who owed a duty to the person seeking relief").

67. *See Huffines*, 314 S.W.2d at 769 (referencing RESTATEMENT (FIRST) OF TORTS § 757 (1939) to explain that liability for misappropriation of a trade secret occurs where the secret is disclosed or used); *see also* Atl. Richfield Co. v. Misty Prods., Inc., 820 S.W.2d 414, 422 (Tex. App.—Houston [14th Dist.] 1992, writ denied) (holding that the defendant did not use the formula, which the plaintiff claimed qualified as a trade secret, where the defendant could not understand the formula and the product produced by the defendant consisted of a compound readily found in the open market).

secret, two problems arise. First, the plaintiff will be unable to establish damages, a requisite for recovery.[68] Second, the plaintiff might fail to establish a breach of a relationship of confidence;[69] although, this concern is minor because, as noted above, acquisition by improper means in itself is likely sufficient to show a breach of loyalty.[70]

Several courts have wrestled with what constitutes "use."[71] Some Texas courts define use as "commercial use" whereby a "party seeks to profit from the use of the secret."[72] Thus, the tort of misappropriation does not occur where a party merely contemplates use of the information.[73]

In the hypothetical described above, the use or disclosure component of a misappropriation claim may bar civil relief in the form of monetary damages because there is no evidence that the employee used or disclosed the information in question. Though, if a plaintiff–employer seeks to enjoin a former employee before the employee has an opportunity to disclose the information, TUTSA provides a cause of action.[74] This

68. *See* CIV. PRAC. & REM. §§ 134A.003–.005 (West Supp. 2013) (delineating the list of remedies to include injunctive relief, actual damages (which include the actual loss "and the unjust enrichment caused by [the] misappropriation"), exemplary damages, and attorney's fees); Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1205 (5th Cir. 1986) (opining on the dual importance of establishing use in a suit where the plaintiff claimed that a former employee provided crucial information for a process of manufacturing, but the defendant had not yet incorporated the process to secure a benefit).

69. *See Metallurgical Indus.*, 790 F.2d at 1205 (noting the dual importance of demonstrating use in a complaint where the employer claims that a former employee conveyed critical information regarding a manufacturing process, but his process had not yet been incorporated).

70. *See* CIV. PRAC. & REM. § 134A.002(3) (West Supp. 2013) (defining misappropriation to include "acquisition of a trade secret" through improper means, or disclosure or use "without the express or implied consent" of its owner).

71. *Compare Metallurgical Indus.*, 790 F.2d at 1205 ("[W]hile the nature of the use may be relevant in determining the proper extent of damages, its existence must also be shown to establish wrongdoing in the first place."), *with* Garth v. Staktek Corp., 876 S.W.2d 545, 548 (Tex. App.—Austin 1994, writ dism'd w.o.j.) (finding that use occurred where the defendant attempted to secure a patent and financing to manufacture a product but had not yet actually produced a final product).

72. *See, e.g.*, Global Water Grp. v. Atchley, 244 S.W.3d 924, 930 (Tex. App.—Dallas 2008, pet. denied) ("Use of the trade secret means commercial use by which the offending party seeks to profit from the use of the secret." (citing *Metallurgical Indus.*, 790 F.2d at 1205)).

73. *See id.* ("Actual use or disclosure of a trade secret is a required element of the tort."); *Metallurgical Indus.*, 790 F.2d at 1205 (discussing the necessity of use to hold the defendant liable for the trade secret gained).

74. *See* CIV. PRAC. & REM. § 134A.002(3)(A) (allowing mere acquisition by improper means to satisfy the definition of misappropriation); *Id.* §§ 134A.001–.003 ("Actual or threatened misappropriation may be enjoined."); *see also* Rugen v. Interactive Bus. Sys., Inc., 864 S.W.2d 548, 552 (Tex. App.—Dallas 1993, no writ) (enjoining a former employee who possessed confidential information, where it was probable the former employee would use the information for "her benefit and to the detriment of [her former employer]"). *But see* Joseph F. Cleveland Jr. & J. Heath Coffman,

attribute might be seen as an advantage of TUTSA over the CFAA because, although the CFAA does not require that the defendant use the information to establish liability, the claim will fail if the plaintiff does not meet the requisite showing of damages.[75] In other words, the minimum damage requirement effectively limits plaintiffs from bringing a claim under the CFAA when damages have yet to occur.[76]

4. The Fourth Obstacle to Recovery—Establishing Damages

As discussed above, TUTSA provides plaintiffs the opportunity to enjoin former employees prior to any use or disclosure of a trade secret.[77] Though the recent enactment of TUTSA created uncertainty about the showing of damages a plaintiff must make, TUTSA does clearly indicate that "actual or threatened misappropriation may be enjoined."[78] Also certain is that prior to TUTSA, some appellate courts achieved a similar result by applying the *Rugen* doctrine.[79] The *Rugen* doctrine allows a plaintiff to temporarily enjoin a former employee from using a trade secret by proving the individual is in possession of the secret and the circumstances indicate that it is more likely than not the former employee will disclose it.[80] It is important to note that the *Rugen* doctrine has been criticized as "inconsistent with more recent case law,"[81] though the doctrine is still heavily cited by trade secret plaintiffs.[82] Furthermore, it remains to be seen if Texas will apply TUTSA's anticipatory language[83] to achieve a result similar to the *Rugen* doctrine, or if it will go so far as to interpret such language as an adoption of the inevitable disclosure

Protecting Trade Secrets Made Simple, 76 TEX. B.J. 751, 752 (2013) (setting forth the uncertainty of whether Texas will adopt the inevitable disclosure doctrine).

75. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (Supp. V 2011).

76. *Id.*

77. CIV. PRAC. & REM. § 134A.003; *see id.* § 134A.002(3)(A) (permitting the acquisition of a trade secret by improper means to support a claim of misappropriation).

78. *Id.* § 134A.003(a).

79. *See* Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 762 (2013) (citing *Rugen*, 864 S.W.2d at 552) (clarifying the doctrine to be a modification of the inevitable disclosure doctrine).

80. *See Rugen*, 864 S.W.2d at 552 (allowing an employer to enjoin preemptively a former employee from using disclosing trade secrets).

81. Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 759 (2013).

82. *Id.* at 762 (discussing that despite the possible inconsistencies between the *Rugen* doctrine and current case law and its limited reach, "trade secrets plaintiffs continue to cite *Rugen*"); *see* Reliant Hosp. Partners, LLC, v. Cornerstone Healthcare Grp. Holdings, Inc., 374 S.W.3d 488, 502 (Tex. App.—Dallas 2012, no pet.) (disregarding the plaintiff's reliance on *Rugen*).

83. *See* CIV. PRAC. & REM. § 134A.003(a) (West Supp. 2013) ("Actual *or threatened* misappropriation may be enjoined." (emphasis added)).

doctrine.[84] The inevitable disclosure doctrine holds that "a plaintiff may prove a claim of trade secret misappropriation by demonstrating that [the] defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets."[85] If Texas chooses to adopt the inevitable disclosure doctrine, it would be a significant departure from the common law,[86] though Texas would be among other states that, after adopting UTSA, held its language to be an adoption of the doctrine.[87]

At common law, with the rare exception of the *Rugen* doctrine discussed above, a plaintiff–employer seeking injunctive relief, even if only temporary, was required to produce evidence in support of the full cause of action for misappropriation, which included evidence of disclosure or use.[88] If the employer prevailed at trial on the misappropriation claim, the court had the discretion to grant a permanent injunction from use of the trade secret if damages would be difficult to calculate.[89] If, however, damages were calculable, recovery might have been limited to lost profits, out-of-pocket damages, and exemplary damages in certain instances.[90]

---

84. *See* Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 762 (2013) (commenting that the legislature's decision to leave the question open "will likely lead to more litigation until the courts reach a consensus and either expressly adopt or reject the inevitable disclosure doctrine").

85. PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995).

86. Cardinal Health Staffing Network v. Bowen, 106 S.W.3d 230, 241–42 (Tex. App.—Houston [1st Dist.] 2003, no pet.) ("We have found no Texas case expressly adopting the inevitable disclosure doctrine, and it is unclear to what extent Texas courts might adopt it or might view it as relieving an injunction applicant of showing irreparable injury."); Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 759 (2013) ("[N]o Texas court has endorsed the inevitable disclosure doctrine . . . .").

87. *See, e.g.*, Triumph Packaging Grp. v. Ward, 834 F. Supp. 2d 796, 808–09 (N.D. Ill. 2011) (discussing the applicability of the inevitable disclosure doctrine and distinguishing the facts of the record before it from *PepsiCo, Inc.*); Interbake Foods, LLC v. Tomasiello, 461 F. Supp. 2d 943, 973 (N.D. Iowa 2006) (concluding "that the inevitable disclosure doctrine is just one way of showing a threatened disclosure . . . ."). *See generally* Brandy L. Treadway, *An Overview of Individual States' Application of Inevitable Disclosure: Concrete Doctrine or Equitable Tool?*, 55 SMU L. REV. 621, 626–632 (2002) (providing a thorough review of which states adopted the inevitable disclosure doctrine).

88. *See* IAC, Ltd. v. Bell Helicopter Textron, Inc., 160 S.W.3d 191, 197–200 (Tex. App.—Fort Worth 2005, no pet.) (noting that a relationship of confidence exists as a product of the employer–employee relationship and that information taken as a result of this relationship may qualify as a trade secret eligible for a temporary injunction).

89. *See* Zoecon Indus. v. Am. Stockman Tag Co., 713 F.2d 1174, 1180 (5th Cir. 1983) (citing Hyde Corp. v. Huffines, 314 S.W.2d 763, 778 (Tex. 1958)) (affirming that a permanent injunction is a possible form of relief in a misappropriation of a trade secret claim).

90. *See* Rusty's Weigh Scales and Serv., Inc. v. N. Tex. Scales, Inc., 314 S.W.3d 105, 110–13 (Tex. App.—El Paso 2010, no pet.) (establishing that if a plaintiff successfully litigates a claim for misappropriation of a trade secret, the plaintiff might recover lost profits, out-of-pocket damages, and exemplary damages in certain instances); Calce v. Dorado Exploration, Inc., 309 S.W.3d 719, 738 (Tex. App.—Dallas 2010, no pet.) (citing Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1208 (5th Cir. 1986)) (outlining factors to consider in calculating monetary damages for the

TUTSA essentially codifies the common law in regard to economic damages.[91] Additionally, TUTSA makes clear that plaintiffs may be awarded exemplary damages "[i]f [willful] and malicious misappropriation is proven by clear and convincing evidence . . . not exceeding twice any [actual damages]."[92] Although this specific cap on exemplary damages is contrary to the common law, the limitation of exemplary damages is not novel in Texas.[93] TUTSA also allows plaintiffs to recover attorney's fees when: (1) a cause of action was brought in bad faith, (2) a motion to dismiss an injunction was "made or resisted in bad faith," or (3) the misappropriation involved "[willful] and malicious" conduct.[94] On the other hand, the CFAA limits plaintiffs to economic, injunctive, and compensatory damages.[95]

C. *Placing the Tort in Context*

It is clear that when an employee accesses a work computer with the intention of taking information for use in a competing enterprise, the employer can pursue civil liability through Texas trade secret laws.[96] To

misappropriation of a trade secret); *see also* Glatty v. Air Starter Components, Inc., 332 S.W.3d 620, 631 (Tex. App.—Houston [1st Dist.] 2010, pet. denied) (quoting ERI Consulting Eng'rs, Inc. v. Swinnea, 318 S.W.3d 867, 878–99 (Tex. 2010)) (reasoning that the party claiming lost profits must provide "reasonably certain evidence of lost profits" and holding that the plaintiff failed to meet the requirement).

91. Joseph F. Cleveland Jr. & J. Heath Coffman, *Protecting Trade Secrets Made Simple*, 76 TEX. B.J. 752, 754 (2013) ("There are no differences between existing Texas common law and TUTSA regarding the economic damages available for trade-secret misappropriation."). *Compare* TEX. CIV. PRAC. & REM. CODE ANN. § 134A.004(a) (West Supp. 2013) (including, in addition to injunctive relief, damages amounting to "actual loss caused by misappropriation and the unjust enrichment caused by misappropriation . . . . [D]amages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret"), *with* Carbo Ceramics, Inc. v. Keefe, 166 Fed. App'x 714, 722 (5th Cir. 2006) (providing a thorough discussion of the types of damages a plaintiff can recover for a misappropriation of a trade secret), *and Calce*, 309 S.W.3d at 738 (discussing damages for royalties in terms of "what a fair licensing price would have been had the parties agreed").

92. CIV. PRAC. & REM. § 134A.004(b) (allowing plaintiffs to recover exemplary damages up to twice the amount of actual damages).

93. *See id.* § 41.008(b) (limiting exemplary damages to "an amount equal to the greater of" either "two times the amount of economic damages; plus . . . any noneconomic damages . . . not to exceed $750,000[,] or $200,000").

94. *Id.* § 134A.005 (West Supp. 2013) ("The court may award reasonable attorney's fees to the prevailing party if: (1) a claim of misappropriation is made in bad faith; (2) a motion to terminate an injunction is made or resisted in bad faith; or (3) [willful] and malicious misappropriation exists.").

95. 18 U.S.C. § 1030(g) (Supp. V 2011) (limiting damages to "compensatory damages and injunctive relief," specifying that "[d]amages for a violation involving only conduct described in [the] subsection [most applicable to private employers] are limited to economic damages").

96. CIV. PRAC. & REM. § 134A.002(6) (West Supp. 2013); *In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)).

bring a successful claim, however, the plaintiff's attorney must overcome several obstacles to recovery. First, the attorney must prove that the material acquired is in fact a trade secret.[97] As noted above, Texas courts will use a six-factor test to determine the existence of a trade secret,[98] but establishing that a trade secret exists could require substantial litigation because no single factor is dispositive of the existence of a trade secret.[99] Second, the attorney will have to prove the existence of a relationship of confidence.[100] While it will be easy for the attorney to establish a relationship of confidence where there is an employer–employee relationship based on agency principles,[101] proving a breach of the relationship can be more difficult.[102] Finally, the attorney must address the issues of use, disclosure, and damages. If the employee has merely accessed the information but proof of its use or disclosure has not manifested itself, it will be unlikely that the plaintiff can recover monetary damages;[103] although, TUTSA allows the possibility of injunctive relief for

97. CIV. PRAC. & REM. § 134A.002(6); *see also In re* Cooper Tire & Rubber Co., 313 S.W.3d 910, 915 (Tex. App.—Houston [14th Dist.] 2010, no pet.) (acknowledging that the burden for establishing whether a trade secret exists falls on the party asserting the existence of a trade secret and that Texas relies on a six-factor test "[t]o determine whether a trade secret exists").

98. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995) ("[T]he principles of trade-secret law described in this Restatement are applicable to actions under the Uniform Trade Secret Act as well as to actions at common law."); *see also Bass*, 113 S.W.3d at 739 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (listing the six-factor test used to determine what constitutes a trade secret).

99. *See In re* XTO Res. I, LP, 248 S.W.3d 898, 901 (Tex. App.—Fort Worth 2008, no pet.) ("The party claiming a trade secret is not required to satisfy all six factors because trade secrets do not fit neatly into each factor every time, and other circumstances may be relevant . . . .").

100. *See* Twister B.V. v. Newton Research Partners, LP, 364 S.W.3d 428, 437–38 (Tex. App.—Dallas 2012, no pet.) (listing the required elements of a misappropriation claim and determining that the second element is a requisite "breach of a confidential relationship or . . . discover[y] by improper means"); *see also* RESTATEMENT (FIRST) OF TORTS § 757 (1939) (providing that liability for an employee's unprivileged use of a trade secret occurs where "his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him").

101. *See* Nat'l Plan Adm'rs, Inc. v. Nat'l Health Ins. Co., 235 S.W.3d 695, 700 (Tex. 2007) (recognizing that an employer–employee relationship is an example of an agency relationship). *But see* Winter v. Morgan, 256 S.W. 342, 344 (Tex. Civ. App.—Amarillo 1923, no writ) ("The law never presumes agency; it is always a fact to be proved, and the person who alleges it has the burden of proving it by a preponderance of the evidence.").

102. *See* CIV. PRAC. & REM. § 134A.002(3) (detailing that for misappropriation to occur, the individual must either acquire the trade secret through improper means or use or disclose it without permission); *see also* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991) (Posner, J.) (discoursing the function of the requirement that a trade secret be reasonably kept secure); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) (placing the burden upon a plaintiff to prove that the information was taken with less-than-innocent intentions).

103. *See* Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 769 (Tex. 1958) ("[L]iability [attaches] if his disclosure or use of another's trades secret is a breach of the confidence reposed in

"[a]ctual or threatened misappropriation."[104] Keeping these limitations on recovery in mind while examining the elements of a claim under the CFAA provides insight as to why the CFAA is a workable alternative to Texas trade secret laws.

III. THE COMPUTER FRAUD AND ABUSE ACT

Although Texas trade secret laws provide one avenue for an employer to pursue relief against a former employee, the Texas litigator can also seek to pursue civil liability through the federal Computer Fraud and Abuse Act (CFAA).[105] The CFAA is a workable alternative because, unlike Texas trade secret laws, it does not require proving that the information obtained qualifies as a trade secret.[106] However, Texas businesses and litigators who contemplate relying on the CFAA should note that several factors make it a risky alternative: (1) a split among federal circuit courts over the proper interpretation and application of the CFAA in civil complaints between an employee and employer;[107] (2) congressional scrutiny that could lead to limiting applicability of the CFAA in the employer–employee

him by the other in disclosing the secret to him." (quoting RESTATEMENT (FIRST) OF TORTS § 757 (1939))); Atlantic Richfield Co. v. Misty Prods., Inc., 820 S.W.2d 414, 422 (Tex. App.—Houston [14th Dist.] 1992, writ denied) ("Use of the trade secret means commercial use by which the offending party seeks to profit from the use of the secret.").

104. CIV. PRAC. & REM. § 134A.003(a) (West Supp. 2013).

105. 18 U.S.C. § 1030 (2006 and Supp. V 2011).

106. *See id.* § 1030(a)(2) (Supp. V 2011) (creating a cause of action where a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) *information* from any protected computer" (emphasis added)).

107. *See, e.g.*, Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (finding that a "breach of his duty of loyalty terminated his . . . authority to access the laptop"). *Compare* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (examining allegations made in a complaint alleging a violation of the CFAA and holding that "without authorization" means accessing a computer "without approval," whereas "exceeds authorized access" means that the actor "has approval to access a computer, but uses his access to obtain or alter information that falls outside the bound of his approved access"), *and* United States v. Nosal, 676 F.3d 854, 857–58 (9th Cir. 2012) (en banc) (adopting a restrictive view of the CFAA and holding that "without authorization" and "exceeds authorized access" are dependent upon the classification of the actor as an "outside hacker" or an "inside" hacker), *with* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (reaffirming the "intended-use analysis" doctrine that focuses on the "relationship . . . between computer owner and the user" to determine whether a use of a computer is authorized), *and* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (agreeing with the court below that a violation of the CFAA occurred where the defendant accessed the computer for personal reasons).

context;[108] and (3) an internal Fifth Circuit district court split over calculation of recoverable damages under the CFAA.[109]

A. *An Introduction to the Act*

The CFAA, as it stands today, is a descendent of the 1984 Counterfeit Device and Computer Fraud and Abuse Act.[110] In the original statute, Congress attempted to protect government computers from what many refer to as "classic hacking," or situations where the actor clearly did not have permission to use the computer.[111] Although the original language of the CFAA did not provide for civil remedies based on a private cause of

108. *See* S. 3342, 112th Cong. § 306 (2012) (as placed on S. Leg. Calendar under General Orders. Calendar No. 438, June 28, 2012) (modifying 18 U.S.C. § 1030(e)(6) (2006) in order to clarify that the CFAA is not violated by acting contrary to a use agreement).

109. *See* Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (noting a split between the Northern and Southern Federal District Courts for the state of Texas). *Compare* Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *3 (N.D. Tex. Apr. 20, 2011) (finding sufficient loss to maintain a suit based on "lost revenue that could amount to over $5,000 over the course of one year"), *with* Alliantgroup, LP, v. Feingold, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011) (holding that the plaintiff failed to "allege or present evidence of any cognizable losses" and could not maintain suit based on the CFAA), M–I, LLC v. Stelly, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010) (determining that "lost profits, loss of customers and loss of future business opportunities" are insufficient to maintain suit under the CFAA because the loss must be a "result of investigation or interruption of computer service"), *and* Quantlab Tech. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010) (concluding that the plaintiff failed to allege proper facts to support a claim under the CFAA because the plaintiff did "not allege an interruption of service as a result of [defendant's] actions, nor any investigation or response to [defendant's] alleged access of the computer").

110. *See Miller*, 687 F.3d at 201 (explaining the evolution and application of the CFAA in a case where an employer alleged that a former employee violated four sections of the act); *see also* Pierre Grosdidier, *Court Decisions Could Remove Ambiguity About Unauthorized Employee Computer Access*, MARTINDALE (Feb. 9, 2012), http://www.martindale.com/litigation-law/article_Haynes-Boone-LLP_1441238.htm (reporting on the evolution of the CFAA into a "broad and powerful weapon in computer–related . . . civil litigation" since enactment); *cf.* Computer Fraud and Abuse Act of 1986, H.R. 4718, 99th Cong. § 100 (1986) (codified as amended at 18 U.S.C. § 1030 (1984)) (modifying previous state attempts to criminalize hacking).

111. *See, e.g.*, *Nosal*, 676 F.3d at 858 ("Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking."); *see also* Pierre Grosdidier, *Court Decisions Could Remove Ambiguity About Unauthorized Employee Computer Access*, MARTINDALE (Feb. 9, 2012), http://www.martindale.com/litigation-law/article_Haynes-Boone-LLP_1441238.htm (reporting on the purpose of the statute at its inception, "to target hackers"); *cf.* Jeffrey D. Neuburger, *Ninth Circuit Ruling Trimming CFAA Claims for Misappropriation Reminds Employers that Technical Network Security is the First Defense*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/internet-law/article_Proskauer-Rose-LLP_1495998.htm (providing background on the intent of Congress to address "classical hacking" in an era during which computers were not used by typical businesses).

action,[112] Congress subsequently amended the language of the statute to incorporate provisions that provide for a private cause of action in civil suits.[113] In addition to permitting civil suits, most commentators recognize that congressional amendments to the CFAA broadened its scope and applicability.[114]

18 U.S.C. § 1030 (the CFAA) now prohibits seventeen specific acts under § 1030(a) or § 1030(b),[115] one of which the civil litigant must allege that the defendant committed.[116] Of the seventeen acts, § 1030(a)(2)(C) has the broadest application.[117] This makes it an attractive provision for employers to bring suit against former employees.[118] Under § 1030(a)(2)(C), a violation of the CFAA occurs whenever an individual "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected

112. *See* Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 471 (1990) (noting that shortly after the passage of the CFAA in 1984, interested parties called for revision of the statute to provide for a private cause of action).

113. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1131 (9th Cir. 2009) (providing that 18 U.S.C. § 1030(g) "creates a right of action for private persons injured by" one of the violations found elsewhere in the statute); A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009) (reviewing whether the private plaintiff properly established the element of damages to maintain civil suit under 18 U.S.C. § 1030(g)); P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 511 (3d Cir. 2005) (recognizing that through 18 U.S.C. § 1030(g) the CFAA provides a cause of action and remedies for civil suits); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 n.8 (1st Cir. 2001) (noting that 18 U.S.C. § 1030(g) permits civil suits where it is linked to a violation of the CFAA under § 1030(a)(4)).

114. *See* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 41 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (noting amendments to the CFAA "in 1986, 1996, 2001, and 2008" and asserting that today the act has multiple interpretations and broad applicability).

115. *See* 18 U.S.C. §§ 1030(a)(1)–(a)(7)(C) (2006 & Supp. V 2011) (providing for seventeen violations of the law that result in civil and criminal liability).

116. *Id.* § 1030(g) (Supp. V 2011) (mandating that civil actions seeking "compensatory damages and injunctive relief" require allegations that the violation involves a factor found in 18 U.S.C. § 1030(c)(4)(A)).

117. *Id.* § 1030(a)(2) (assigning civil liability where a party "intentionally accesses a [protected] computer without authorization" and conditioning recovery on damages resulting from access of computers, but not from use or disclosure of the information obtained); *see also* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 42 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (calling 18 U.S.C § 1030(a)(2)(c) "the broadest provision" of the act).

118. *See* United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (noting that under § 1030(a)(2)(C) the plaintiff is not required to demonstrate an intent to defraud).

computer."[119] Because the language "obtains information"[120] applies to all information regardless of its value and because all computers qualify as "protected computer[s],"[121] the only real obstacle for the civil plaintiff's attorney to overcome is demonstrating that the individual exceeded authorized access[122] and that the misappropriation caused at least $5,000 in damages.[123]

B. *Fifth Circuit CFAA Cases*

One of the most significant obstacles to recovery in civil actions is proving that the individual acted "without authorization"[124] or "exceeded authorized access."[125] While federal circuit courts disagree on the

119. 18 U.S.C. § 1030(a)(2)(C) (Supp. V 2011); Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 42 (2011) (quoting 18 U.S.C. § 1030(a)(2)(C) (Supp. V 2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/ viewcontent.cgi?article=1003&context=faculty_testimony.

120. 18 U.S.C. § 1030(a)(2)(C) (Supp. V 2011).

121. *Id.*

122. *See Nosal*, 676 F.3d at 859 (noting that all computers connected to the Internet are "protected computers" within the meaning of the statute); Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 42 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University)), *available at* http://scholarship.law.gwu.edu/cgi/ viewcontent.cgi?article=1003&context=faculty_testimony (describing the definition of protected computers and concluding that because nearly all computers are protected and "the statute does not require the information be valuable or private," liability "hinges largely on the first element").

123. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (Supp. V 2011) (requiring that claims show a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value"); *see also id.* §§ 1030(c)(4)(A)(i)(I)–(VI) (Supp. V 2011) (listing the five factors, one of which must be established to maintain a civil suit: a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value"; interference with treatment or medical processes; "physical injury to any person"; "threat[s] to public health or safety"; damage to government security devices; or damage affecting at least 10 protected computers); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201 n.1 (4th Cir. 2012) (noting that the plaintiff properly alleged losses in a single year that met the requisite threshold amount in § 1030(c)4(A)(i)(I) to maintain a civil suit under the CFAA); Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1157 (5th Cir. 2006) (recognizing that § 1030(g) permits civil actions where one of the five factors are involved).

124. *Id.* § 1030(a)(2) (Supp. V 2011) ("Whoever . . . (2) intentionally accesses a computer without authorization or exceeds authorized access . . . shall be punished as provided in subsection (c) of this section.").

125. *Id.*; *accord* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 43 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003& context= faculty_testimony; *see also Miller*, 687 F.3d at 204 (defining the term "without authorization" as "gain[ing] admission to a computer without approval").

meaning and application of these two terms,[126] Fifth Circuit precedent is clear on the matter.[127] The following is a description of the Fifth Circuit's interpretation of the CFAA that the court established through criminal suits and an example of how district courts within the Fifth Circuit use that interpretation to establish civil liability in cases between an employer and a former employee.

In *United States v. Phillips*,[128] the Fifth Circuit Court's first attempt to clarify the meaning of authorization under the CFAA, the court determined that defining the scope of authorization requires identifying the intended use for which authorization was given and the "nature of the relationship established between the computer owner and the user."[129] However, because of the court's relatively brief discussion, *Phillips* left many questions unanswered.[130] To address the unanswered questions, the court revisited and expanded the meaning of "unauthorized access" in *United States v. John*.[131] At issue in the case was whether a former employee of Citigroup exceeded authorized access when she printed

126. *See Miller*, 687 F.3d at 203–04 (holding that the term "without authorization" refers to instances where an individual had no authorization to access the computer and "exceeds authorized access" refers to instances where the individual had authority to access the computer for limited purposes but the person uses that access to access information they are not authorized to access); *Nosal*, 676 F.3d at 856–59 (en banc) (linking the definition of "exceeds authorized access" to the context of whether the actor is classified an "outside" or "inside hacker"); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (determining that the policy prohibiting access for certain purposes was determinative of whether a violation of the CFAA act occurs in certain instances); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (concluding that the duty of loyalty is controlling in the question of whether an actor is acting without authorization or exceeded authorization); *cf.* Michael R. Greco, *CFAA Does Not Apply to Employee Data Theft According to Ninth Circuit*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/computers-office-equipment/article_ Fisher-Phillips-LLP_1495924.htm (acknowledging the split between the federal courts on the meaning of "without authorization" and "exceeded authorized access"). *See generally* Pamela Taylor, Comment, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 209–26 (2012) (noting a broad and narrow view of the CFAA and arguing for the application of the narrow view).

127. *See* United States v. John, 597 F.3d 263, 269–71 (5th Cir. 2010) (affirming the intended-use rule established in a prior suit brought under the CFAA); United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (noting that the intended-use for which authorization is granted controls on the matter of whether a user exceeded authorized access or acted without authorization).

128. United States v. Phillips, 477 F.3d 215 (5th Cir. 2007).

129. *Id.* at 219 (addressing whether a defendant's use of the University of Texas computer system to recover social security numbers and other encrypted data constituted unauthorized use where the defendant had general authorization to use the computer system).

130. *Id.*

131. United States v. John, 597 F.3d 263 (5th Cir. 2010) (clarifying the meaning of the CFAA in a suit where a former employee of Citigroup argued that she had not violated the CFAA by downloading customer information later used to commit fraud because she had authorization to access the information at the time she downloaded it).

corporate account information and gave the information to a friend.[132] The defendant argued that a violation of the CFAA only occurs where a person "us[es] authorized access to obtain information that she is not entitled to obtain or alter[s] information that she is not entitled to alter."[133] Therefore, because she had authorization to access the information as part of her duties as an employee, she did not access the information without authorization or exceed her authorized access by accessing the information. In rejecting the defendant's restrictive view of the CFAA, the court reasoned that exceeding authorized access could occur in two instances.[134] First, similar to the defendant's argument, the court reasoned that exceeding authorized access occurs where a person is authorized to access only a limited range of data on a computer and the individual accesses data beyond the scope of that limited range.[135] Second, exceeding authorized access to a computer also occurs where the individual has authorization to access the computer, but the individual "exceed[s] the purposes for which" the grantor authorized access.[136]

Under this expansive view of the CFAA prohibitions, the "intended-use" for which authorization was granted is crucial to determining whether a party exceeded authorized access.[137] In further solidifying its position on the correct interpretation of the CFAA, the court went on to assert that an employer may define the scope of authorized use through employment

132. *See id.* at 269 (detailing the defendant's employment with Citigroup and the defendant's employment related authorization to access customer information through the company's computer system).

133. *Id.* at 271.

134. *See id.* (reading "[t]he statute at issue [to] prohibit[] both accessing a computer 'without authorization' and 'exceed[ing] authorized access' to obtain specified information" (quoting 18 U.S.C. § 1030(a)(2)(A) (2006))).

135. *See id.* (confirming in part the defendant's interpretation of the CFAA through a hypothetical in which an authorized user is permitted to use a computer, but the authorized user exceeds his authorized use by accessing password protected information where the user had not been given the password).

136. *See id.* at 272 (pointing out that the facts of the situation at hand, where an employee had authorization to access customer information but not to use that information for unlawful purposes, demonstrate an example of the second prohibition established by the CFAA). This interpretation is analogous to the improper means standard defined in both the RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) and the UNIF. TRADE SECRET ACT § 1(1) (amended 1985) 14 U.L.A. 537 (2005). *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) ("One is subject to liability for the appropriation of another's trade secret if: (a) the actor acquires by means that are improper . . . ."); UNIF. TRADE SECRET ACT § 1(1) (amended 1985) 14 U.L.A. 537 ("'Improper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means . . . .").

137. *See John*, 597 F.3d at 271 (quoting United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007)) (noting the importance of the computer owners expectations in determining the scope of the intended authorized uses).

agreements.[138] Therefore, Citigroup authorized John to access the customer information on Citigroup's computers, but when John accessed the information and disclosed it to a friend in violation of corporate policies, John exceeded her authorized access.[139]

In both of the Fifth Circuit's decisions, the court addressed the applicability of the CFAA in criminal suits.[140] To date, the Fifth Circuit has not addressed the CFAA in terms of civil liability, but federal district courts within the state of Texas apply the same intended-use analysis adopted at the appellate level in criminal cases.[141] For example, in *Meats by Linz, Inc. v. Dear*,[142] the Federal District Court for the Northern District of Texas considered whether an employer adequately stated a claim under the CFAA to survive a motion to dismiss.[143] According to the allegations made in the complaint, the former employee, Dear, worked for the plaintiff, Meats by Linz, Inc. (MBL), as a general manager.[144] In furtherance of his duties, MBL authorized Dear to access confidential information used by the company.[145] MBL protected the information by requiring a password to access it, and MBL further sought to protect the information by requiring Dear to sign an agreement that prohibited him from disclosing the information, competing with the company, soliciting

138. *See id.* at 272 (relying on EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001) (holding that the intended-use analysis is aided by the existence of an employment agreement).

139. *See id.* (finding that the defendant violated the CFAA).

140. *See id.* at 269 (opining on the applicability of the CFAA in a criminal suit brought by the government against a former employee of Citigroup who "accessed and printed information pertaining to at least seventy-six corporate customer accounts and provided it to" a person not employed by Citigroup); *Phillips*, 477 F.3d at 217 (hearing the appeal from a criminal conviction secured against Christopher Andrew Phillips, a former University of Texas at Austin student, for violating the CFAA).

141. *See* Barnstormers, Inc. v. Wing Walkers, LLC, No. EP-10-CV-261-KC, 2011 WL 1671641, at *9 (W.D. Tex. May 3, 2011) (mem. op. not designated for publication) (declaring that the plaintiff stated a sufficient basis for recovery where the defendant "exceed[ed] the purposes for which" the authorized computer access was granted); Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *2 (N.D. Tex. Apr. 20, 2011) (finding that the intended-use analysis is controlling on the question of whether a violation of the CFAA occurred).

142. Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, (N.D. Tex. Apr. 20, 2011).

143. *See id.* at *2 (considering a defendant's motion to dismiss in an action brought under the CFAA because the defendant claimed he had authorization to access the information and therefore could not exceed his authorized access).

144. *See id.* at *1 (describing the relationship between the plaintiff and defendant prior to the filing of the claim under the CFAA).

145. *See id.* (listing the specific information that the former employee, Dear, had access to while working for MBL as a general manager, which included customer contact information and data relating to the price of goods sold).

customers of MBL, or attempting to usurp MBL's corporate opportunities in any other way.[146]

According to MBL's allegations, Dear accessed MBL's confidential information through a computer and then, within a few hours of accessing the information, Dear submitted his resignation.[147] MBL alleged that, shortly after resigning, Dear began soliciting MBL customers found in the information Dear downloaded prior to resigning.[148] In response to the suit filed by MBL, Dear filed a motion to dismiss for failure to state a "plausible claim under the CFAA."[149] Dear's argument for dismissal relied on the assumption that the CFAA does not establish liability where the defendant had authorization to access the information.[150] To determine whether MBL could bring a suit under the CFAA where the defendant had authorization to access the information, the court relied heavily on the Fifth Circuit Court's decision in *John*.[151] Ultimately, the court held that MBL adequately stated a cause of action because the company did not intend for Dear to use the information to compete with the business.[152]

---

146. *See id.* (restating the four elements of the restrictive covenant that the defendant allegedly signed prior to receiving access to the information purportedly accessed in violation of the CFAA).

147. *See id.* (reviewing the allegations made by a plaintiff–employer in a suit brought under the CFAA).

148. *See id.* at *3 (outlining the allegations made by the plaintiff, which if true, support the damages component of a claim filed under the CFAA).

149. *See id.* at *2 (discussing the court's initial inquiry upon consideration of defendant's motion).

150. *See id.* (acknowledging that the motion to dismiss filed by the plaintiff rests on two primary grounds: (1) that the defendant could not have violated the CFAA where "he had authorization to access" the information at the time the information was accessed; and (2) the plaintiff failed to allege damages necessary to maintain a suit under the CFAA).

151. United States v. John, 597 F.3d 263 (5th Cir. 2010); *see also* Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *2 (N.D. Tex. Apr. 20, 2011) (evaluating the holding in *United States v. John* to determine whether a viable claim under the CFAA occurs in the context of a civil suit when the defendant had authorization to access the information but the defendant exceeded their authorized use).

152. *See Meats*, 2011 WL 1515028, at *3 ("[The plaintiff] has pleaded a plausible CFAA claim . . . because it has alleged . . . [the defendant] accessed the [plaintiff's] computer system . . . and then used it, in violation of the restrictive covenant agreement without [plaintiff's] express consent, to compete directly with [the plaintiff]."); Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ ("[B]ecause Dear accessed the information in violation of the restrictive covenants and, therefore, not in furtherance of its intended-use, his access was unauthorized.").

C. *Advantages of CFAA Claims*

A comparison of the CFAA, as interpreted by the Fifth Circuit, with Texas trade secret laws demonstrates why a suit filed under the CFAA can be advantageous to civil plaintiffs. As stated above, a civil claim under the CFAA merely requires demonstrating that (1) the individual exceeded his authorized access and (2) obtained information from the protected computer.[153] Exceeding authorized access occurs where the individual uses the computer in a manner contrary to the intended purpose for which the computer owner granted authorization.[154] Exceeding authorized access may also be a violation of TUTSA;[155] however, under TUTSA and Texas common law, the owner of the information must establish that the information obtained is a trade secret.[156] Herein lies the first advantage of suits filed under the CFAA: proving the value or nature of the information obtained is not a required element of a claim under the CFAA.[157] Second, the Texas trade secret law requires proving that a relationship of confidence existed and a breach of that relationship occurred as a result of the disclosure or use of the trade secret.[158] Much like the first requirement of a misappropriation of a trade secret claim, the second requirement demonstrates another advantage to filing suit under the CFAA. CFAA claims do not require establishing a relationship of confidence,[159] but this is only a slight advantage because a relationship of confidence is easy to establish in the employer–employee context.[160]

---

153. *See* 18 U.S.C. § 1030(a)(2) (Supp. V 2011) (providing civil liability where a party "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer" and conditioning recovery on damages resulting from access but not from use or disclosure of the information obtained).

154. *See John*, 597 F.3d at 269–71 (affirming the intended-use rule established in a prior suit brought under the CFAA); United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (noting that the intended use for which authorization is granted controls on the matter of whether a user exceeded authorized access or acted without authorization).

155. *See* TEX. CIV. PRAC. & REM. CODE ANN. §§ 134A.001–.002(2) (West Supp. 2013) (defining improper as to include "breach or inducement of a breach of a duty to maintain secrecy").

156. *See id.* § 134A.002(6); *see also* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—Austin 2004, pet. denied) (citing IBP, Inc. v. Klumpe, 101 S.W.3d 461, 467 (Tex. App.—Amarillo 2001, pet. denied)) (listing the "existence of a trade secret" as the first element of the cause of action for misappropriation of a trade secret)).

157. *See* 18 U.S.C. § 1030(a)(2) (Supp. V 2011) (providing civil liability where a party "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer," but not making recovery in the civil context dependent upon the value or nature of the information obtained).

158. *See Trilogy Software*, 143 S.W.3d at 463 (citing *Klumpe*, 101 S.W.3d at 467) (listing "breach of a confidential relationship" and "use of the trade secret" as the second and third elements of the cause of action for misappropriation of a trade secret).

159. *See* 18 U.S.C. § 1030(a)(2) (Supp. V 2011) (providing civil liability where a party

IV. CFAA: A RISKY ALTERNATIVE TO TEXAS TRADE SECRET LAW

A. *Federal Circuit Court Split*

There is a split amongst federal appellate courts over the application of the CFAA where the suit involves an employer attempting to hold an employee civilly liable.[161] Thus far, five federal circuit courts have interpreted the statute, and each one has developed a slightly different interpretation.[162] In *WEC Carolina Energy Solutions LLC v. Miller*,[163] the Fourth Circuit reviewed the CFAA in light of the alternative interpretations presented by the Seventh and Ninth Circuits.[164] The court in *Miller* determined that the term "without authorization" is only applicable to instances where an individual had no authorization, or approval, to access the computer.[165] Alternatively, the court determined that "exceeds authorized access" refers to instances where a person's grant of authority extends to accessing the computer for limited purposes, but the person uses that access to obtain information on the computer that they were not authorized to access.[166] Although it is a subtle distinction,

---

"intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (C) information from any protected computer," but not making recovery dependent on the scope of authorization rather than specifically requiring a relationship of confidence).

160. *See* Nat'l Plan Adm'rs, Inc. v. Nat'l Health Ins. Co., 235 S.W.3d 695, 700 (Tex. 2007) (drawing a connection between employer–employee relationships and agency relationships because an employer–employee relationship is an example of an agency relationship). *But see* Winter v. Morgan, 256 S.W. 342, 344 (Tex. Civ. App.—Amarillo 1923, no writ) (noting that agency is not presumed).

161. *See* Jeffrey D. Neuburger, *Ninth Circuit Ruling Trimming CFAA Claims for Misappropriation Reminds Employers that Technical Network Security Is the First Defense*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/internet-law/article_Proskauer-Rose-LLP_1495998.htm (discussing that in the context of employee–employer civil actions based on the CFAA, the Ninth Circuit, unlike the Seventh Circuit, holds that "exceeding authorized access" does not encompass situations where the employee merely uses accessed documents in completion with the employer).

162. *See* Michael R. Greco, *CFAA Does Not Apply to Employee Data Theft According to Ninth Circuit*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/computers-office-equipment/article_Fisher-Phillips-LLP_1495924.htm (reporting that the Fifth, Seventh, Ninth, and Eleventh Circuits provide interpretations of the CFAA).

163. WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012).

164. *See id.* at 203 (acknowledging that the Seventh and Ninth Circuits provide two distinct views of what constitutes "without authorization" and "exceeds authorized access" under the CFAA); Wayne C. Heavener, *Fourth Circuit Court of Appeals Finds Computer Fraud and Abuse Act Provides No Remedy for Employer, Whose Former Employee Misappropriated Company Information*, MARTINDALE (Aug. 3, 2012), http://www.martindale.com/computer-software/article_Semmes-Bowen-Semmes-A-Professional_1563086.htm (delineating a review of the pertinent facts of the case).

165. *See Miller*, 687 F.3d at 204 (providing the Fourth Circuit's definition of "without authorization" after a detailed review of the terms meanings adopted by other federal circuit courts).

166. *See id.* (stating the Fourth Circuit's opinion as to when a CFAA violation has occurred).

the court clarifies that "exceeding authorized access" does not depend on the use to which the person puts the information obtained.[167] Instead, "exceeding authorized access" depends on the improper use of access to obtain information for which there was no grant of authority to access.[168] Therefore, based on its interpretations of the CFAA, the Fourth Circuit determined that a former employee did not violate the CFAA when he accessed proprietary information and used it to secure customers for a competitor because the employee had authorization to access the proprietary information he obtained, even if company policies prohibited using the information in that manner.[169] It is noteworthy that under TUTSA, similar facts would be actionable as a disclosure in violation of a duty of confidence.[170] Additionally, by divorcing the improper use of obtained information from improper use of access to obtain information beyond the scope of the authorized access, the court determined that a misappropriation claim is distinct from a claim based on the CFAA.[171]

As justification for this restrictive interpretation of the CFAA, the court focused on the CFAA's dual applicability to both criminal and civil actions.[172] According to the court, a more liberal interpretation in civil cases could result in criminalizing activities, like checking social networking sites if an employer's use-policy prohibits such activities.[173]

The Ninth Circuit, in *United States v. Nosal*,[174] provided a similar

167. *See id.* (noting that definitions for "without authorization" and "exceeds authorized access" do not encompass the "improper *use* of information validly accessed").

168. *See id.* (stressing that the resulting improper use of information obtained is not relevant to determining whether a party acted without authorization or exceeded authorized use).

169. *See id.* at 207 (concluding that to state a valid civil claim under the CFAA, the plaintiff should have alleged that the employee did not have authorization to access the computer or authorization to access the specific information accessed on the computer).

170. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(3) (West Supp. 2013) (delimiting the elements of a misappropriation to include "(A) acquisition of a trade secret . . . by improper means; or (B) disclosure or use . . . without express or implied consent"); *see also id.* § 134A.002(2) (defining improper means to encompass acts that are a "breach or inducement of a breach of a duty to maintain secrecy, to limit use, or to prohibit discovery").

171. *See Miller*, 687 F.3d at 207 (applying the court's reasoning to determine that the defendant may be liable for misappropriation claims but not for violating the CFAA); *see also* Wayne C. Heavener, *Fourth Circuit Court of Appeals Finds Computer Fraud and Abuse Act Provides No Remedy for Employer, Whose Former Employee Misappropriated Company Information*, MARTINDALE (Aug. 3, 2012), http://www.martindale.com/computer-software/article_Semmes-Bowen-Semmes-A-Professional_1563086.htm (reporting on the court's distinction between a misappropriation claim and a CFAA claim).

172. *See Miller*, 687 F.3d at 204 (citing United States v. Lanier, 520 U.S. 259, 266 (1997)) (reiterating that where a criminal statute is interpreted, strict construction rules apply).

173. *See id.* at 206 (warning that alternate interpretations of the CFAA advanced by other circuit courts could criminalize acts that Congress had no intention to criminalize).

174. United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).

restrictive interpretation of exceeds authorized access and echoed similar concerns—that a broad interpretation of the term could lead to criminalizing many Americans' routine computer use.[175] But, while *Nosal* is fairly indistinguishable from *Miller*, the Ninth Circuit went one step further. To maintain focus on the statute's original intent—addressing the issue of hacking—the court clarified the meanings of "without authorization" and "exceeds authorized access" by linking the terms to "inside" and "outside" hackers.[176] According to the court, "'[w]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)."[177]

Regardless of whether the Fourth and Ninth Circuits correctly ascertained Congress's intent, Supreme Court precedent supports using a restrictive approach where a criminal statute is ambiguous.[178]

Unlike the Fourth and Ninth Circuits, the Seventh and Eleventh Circuits adopted an approach similar to the intended-use approach utilized by the Fifth Circuit. In *International Airport Centers, LLC v. Citrin*,[179] the Seventh Circuit concluded that authorization to use an employer's computers terminates when an employee acts or decides to act "in violation of the duty of loyalty that agency law imposes on an employee."[180] Likewise, the Eleventh Circuit attempted to interpret the meaning of "exceeds authorized access" in a manner that seems to

175. *See id.* at 856–63 (holding that there are two possible interpretations of "exceeds authorized access"; that under the correct meaning of the phrase "exceeding authorized access" occurs when "one [who is] authorized to access only certain data or files . . . accesses unauthorized data or files;" that more expansive interpretations of the statute could lead to criminalizing "innocuous behavior;" and that the statute was not intended to address misappropriation claims); *see also* Jeffrey D. Neuburger, *Ninth Circuit Ruling Trimming CFAA Claims for Misappropriation Reminds Employers that Technical Network Security Is the First Defense*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/internet-law/article_Proskauer-Rose-LLP_1495998.htm (stating an argument for a restricted interpretation of the CFAA by recognizing that under the liberal approach criminal prosecution for violations of social networking user agreements could occur).

176. *See Nosal*, 676 F.3d at 858 (attempting to clarify the meaning of the CFAA by inserting the terms "inside" and "outside").

177. *Id.*

178. *See* United States v. Kozminski, 487 U.S. 931, 949 (1988) (favoring a restricted interpretation of a criminal statute where the alternative could result in criminalizing a multitude of routine activities).

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

180. *See id.* at 420–21 (holding that once the employee decides to act contrary to the interests of his employer "his authority to access the [computer]" terminates).

compliment the Fifth Circuit's viewpoint.[181] In *United States v. Rodriguez*,[182] the defendant's authorization permitted him to access agency databases for limited purposes, but when the defendant accessed the database for explicitly prohibited purposes, the court determined the defendant exceeded authorized access.[183] However, the decision is distinct from the Fifth Circuit decisions because exceeding authorization resulted as a violation of agency policy rather than merely as a result of intending to use the information for nefarious purposes.[184]

The split of authorities over the proper interpretation of the terms "without authorization" and "exceeds authorization" in the CFAA presents three problems for the civil litigant planning to rely on the Fifth Circuit's intended-use analysis.

First, the Fifth Circuit Court of Appeals could choose to ignore its precedent in light of a changed understanding of the law involved if presented an opportunity to revisit the CFAA in the context of a civil suit between an employee and a former employer. The court last affirmed its adoption of the intended-use analysis in 2010.[185] The two courts adopting similar lines of analysis to the Fifth Circuit adopted their approaches concurrently with or before the Fifth Circuit decision.[186] However, since adopting the intended-use analysis, the Fourth and Ninth Circuits have had the opportunity to adopt alternative interpretations of the CFAA that severely limit its applicability in the employee–employer context and to articulate justifications for rejecting the approach adopted by the Fifth Circuit, which could encourage the Fifth Circuit to reexamine its decision to apply the intended-use analysis.[187]

---

181. *See* United States v. Rodriguez, 628 F.3d 1258, 1258 (11th Cir. 2010) (addressing whether a federal employee exceeded authorized access when he violated agency policy by accessing a computer to obtain information for nonbusiness purposes).

182. United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).

183. *See id.* at 1263–64 (determining that the policy prohibiting access for certain purposes is determinative of whether a violation of the CFAA act occurs in certain instances).

184. *See id.* at 1263 (distinguishing between the facts at hand and the issues addressed by the Fifth Circuit).

185. *See* United States v. John, 597 F.3d 263, 269–71 (5th Cir. 2010) (affirming the intended-use rule established by the court in 2007).

186. *See Rodriguez*, 628 F.3d at 1263 (finding that a violation of the CFAA occurs where the actor "obtained [information] for a nonbusiness reason"); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that "[v]iolating the duty of loyalty" results in termination of authorization to access a computer).

187. *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (arguing that the CFAA only applies where there was no authorization to access the information in question and arguing for strict construction where criminal penalties are at issue to prevent unintentionally criminalizing activities); *see also* United States v. Nosal, 676 F.3d 854, 858 (9th Cir.

Second, the Fifth Circuit Court of Appeals could choose to ignore its precedent in light of a change in the facts involved if presented an opportunity to revisit the CFAA in the context of a civil suit between an employee and a former employer. When the court adopted and affirmed the intended-use analysis, it was in the context of criminal suits.[188] The court has not yet addressed the matter in the context of civil suits.

Third, the split amongst federal appellate courts makes the issue ripe for review by the Supreme Court, and the Supreme Court could accept the restrictive approach adopted by the Fourth and Ninth Circuits because the statute is a criminal statute.[189]

B. *Possible Amendment of the CFAA*

In 2011, Congress heard calls from interested parties to limit the applicability of the CFAA during a subcommittee meeting of the United States House of Representatives Committee on the Judiciary.[190] Professor Orin Kerr of George Washington University Law School, a former member of the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice, testified that under the current statutes all computers qualify as "protected computers," and mere violations of user website agreements could result in criminal prosecution.[191] Although Kerr did not specifically address the

---

2012) (en banc) (concluding that authorization is not dependent upon intended-use and distinguishing between inside and outside actors).

188. *See John*, 597 F.3d at 269–71 (opining on the application of the CFAA in a criminal suit brought against a former employee of a bank); United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (considering the applicability of the CFAA in a criminal suit brought against a former student of the University of Texas).

189. *See* United States v. Kozminski, 487 U.S. 931, 949 (1988) (preferring a restricted interpretation of a criminal statute where the alternative could result in criminalizing a multitude of routine activities); United States v. Wiltberger, 18 U.S. 76, 90–91 (1820) ("In criminal cases, a strict construction is always to be preferred; and if there be doubt, that is of itself conclusive."). *But see* Sedima, S.P.R.L. v. Imrex Co., Inc., 473 U.S. 479, 491 (1985) (announcing that merely because "the offending conduct is described by reference to criminal statutes does not mean that its occurrence must be established by criminal standards or that the consequences of a finding of liability in a private civil action are identical to the consequences of a criminal conviction").

190. *See* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 41 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (arguing that the CFAA should be amended to restrict its broad application).

191. *See id.* (internal quotation marks omitted) (concluding that the term "protected computer" "appears to include all computers" and that under current interpretations of exceeds authorized access violating the terms of websites such as Google and Match.com could result in criminal liability).

CFAA in the context of civil actions, the changes he recommended would have a significant impact on the ability of employers to successfully litigate civil suits.[192] For example, Kerr suggested that Congress amend 18 U.S.C. § 1030(a)(2) by limiting its ability to obtaining information that has a value greater than $5,000 or is of a "sensitive or private nature."[193] The sensitive or private nature language would bring the CFAA closer to Texas trade secret claims because it would place greater responsibility on the court to scrutinize the value or nature of the disputed information.[194]

As a counterweight to the arguments for restricting the CFAA's applicability, Congress also heard testimony from federal administrative agency officials charged with prosecuting criminal violations of the CFAA.[195] Government testimony acknowledged the broad application of statutory provision in the CFAA, but they argued that narrowly tailoring the language of the act would prevent adequate enforcement as unforeseen technological advances occur and "make it difficult or impossible to deter and punish serious threats from malicious insiders."[196] More specifically, one government official argued that restrictions to the definition of what exceeds authorized access would undermine employer confidence that the government could seek prosecution when employees exceed authorized access for nefarious purposes.[197]

Despite calls to refrain from restricting the CFAA, the United States Senate signaled a desire to limit the scope of what qualifies as

192. *See id.* (focusing on whether suggested alterations of the statute would prevent "prosecutions based on violations of Terms of Service and Terms of Use").

193. *See id.* at 46 (suggesting a possible amendment to 18 U.S.C. § 1030(a)(2) (Supp. V 2011) that adopts a "significant harm" requirement).

194. *Compare In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003) (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939)) (stating that the six factors a court shall consider in determining whether information qualifies as a trade secret are "(1) the extent to which the information is known . . . (3) the extent of the measures taken by him to guard the secrecy of the information (4) the value of the information to him and his competitors (5) the amount of money . . . expended"), *with* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 47 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (suggesting a possible amendment to 18 U.S.C. § 1030(a)(2) (Supp. V 2011) that adopts a "significant harms" requirement consisting of a monetary value threshold for filing suit or an inquiry into the "sensitive or private" nature of the information obtained).

195. *See* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 6 (2011) (Statement of Richard W. Downing, Deputy Section Chief) (expressing concerns that limiting the CFAA would impede and frustrate the ability to prevent and punish insider threats).

196. *Id.*

197. *Id.*

"unauthorized" in the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, commonly referred to as the Cybersecurity Act of 2012.[198] If adopted, the amended language would force the Fifth Circuit to reexamine the intended-use analysis currently employed because the bill amends § 1030(e)(6) to clarify that unauthorized use must be based on something more than accessing a computer where it is prohibited by "a contractual obligation or agreement."[199] While the act states that violations of an acceptable use policy are not sufficient to independently establish that unauthorized access occurred, it provides no guidance on whether a violation of the duties owed from agent to employer occurring concurrently with a violation of the employer's use policy is sufficient to establish unauthorized use.[200]

Although the Cyber Security Act was unlikely to become law in 2012,[201] the fact that § 1030 was addressed in several other proposed bills suggests that interested parties wishing to restrict the applicability of § 1030 in civil suits will have an abundance of legislative opportunities to amend the statute in future meetings of Congress.[202] The possible amendment of the CFAA to include measures that would focus on the nature of the information obtained means that the prospective plaintiff–

198. *See* S. 3342, 112th Cong. § 306 (2012) (limiting the meaning of unauthorized use in civil actions by amending 18 U.S.C. § 1030(e)(6) (2006)).

199. *See id.* (amending 18 U.S.C. § 1030(e)(6) (2006) to read: "[unauthorized use] does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with . . . [a] non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized").

200. *See id.* (attempting to clarify the meaning of "unauthorized use" in the civil context but failing to provide a sufficient framework to determine which other factors independent of a violation of a computer use policy are sufficient to establish unauthorized use).

201. *See* Mike McCarter, *Cybersecurity Secure It Act Offers Best Chance for Improved Cybersecurity, Senate Republicans Say*, HSTODAY.US (Aug. 15, 2012), http://www.hstoday.us/index.php?id=483&cHash=081010&tx_ttnews%5Btt_news%5D=25445 (suggesting that it was unlikely the Cybersecurity Act would pass during the remainder of the 112th Congress because the House of Representatives refused to consider similar legislation earlier in the year); *see also* J.C. Boggs & Lauren M. Donoghue, *Cybersecurity Legislation Unlikely to Pass During Lame Duck*, KING & SPALDING: WASHINGTON INSIGHT (Oct. 5, 2012), http://www.kslaw.com/library/newsletters/WashingtonInsight/2012/Oct5/article5.html (proposing that the Cybersecurity Act is unlikely to pass in 2012 based on comments by Senator Joe Lieberman but noting that the President considers legislation on the matter an issue of significant importance to the nation's security).

202. *See* S. 3569, 112th Cong. § 306 (2012) (attempting to amend 18 U.S.C. § 1030 (Supp. V 2011) to provide for a civil and criminal offense for unauthorized access of a cloud computing service or account); S. 3074, 112th Cong. (2012) (creating an offense under 18 U.S.C. § 1030 (Supp. V 2011) for employers that encourage an employee to access a protected computer without authorization).

employer should be wary of relying on the CFAA act in lieu of Texas trade secret laws in the immediate future.

C. *Internal Split over Damages and Loss Calculations*

In addition to the split amongst federal appellate courts over what constitutes without authorization and exceeds authorized access, there is an internal federal district court split in Texas over damage and loss calculations[203] under § 1030(c)(4)(A)(i)(I).[204] According to § 1030(g), a party may use the CFAA to hold another civilly liable "if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."[205] Specifically, civil suits are appropriate only where the act of obtaining information includes:

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
> (II) the modification or impairment or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
> (III) physical injury to any person;
> (IV) a threat to public health or safety;
> (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; . . . .[206]

In the hypothetical discussed in the Introduction of this Comment, where the suit is between a typical non-governmental employer and a former employee, § 1030(c)(4)(A)(i)(I) is the most relevant.[207]

---

203. *See* Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (discussing in detail the split amongst district courts in Texas over sufficient losses); *see also* Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *3 (N.D. Tex. Apr. 20, 2011) (deciding that aggregated losses to the plaintiff resulting from lost sales were sufficient to meet the requisite $5,000 damages component); M–I LLC v. Stelly, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010) (determining that the plaintiff–employer, M–I LLC, failed to adequately state a claim under the CFAA against the company's former employees because the damages and losses alleged by the plaintiff were insufficient).

204. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I) (Supp. V 2011) (working in conjunction with § 1030(g) to provide a basis for civil liability where there is "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value").

205. *Id.* § 1030(g).

206. *Id.* §§ 1030(c)(4)(A)(i)(I)–(V).

207. *See id.* § 1030(c)(4)(A)(i)(I) (establishing civil liability in five instances that relate to a variety

Section 1030(c)(4)(A)(i)(I) refers to "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value,"[208] and § 1030(e)(11) defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[209]

In *Meats by Linz, Inc. v. Dear*,[210] the U.S. District Court for the Northern District of Texas considered whether the plaintiff properly claimed sufficient damages under the CFAA.[211] The plaintiff claimed that the damage resulting from lost revenues was sufficient to bring an action under the CFAA, but the defendant asserted that lost revenues alone were insufficient.[212] The court agreed with the plaintiff's assertion that the lost revenues alleged were a sufficient basis for claiming damages.[213] This holding directly conflicts with the previous holdings of the Federal District Court for the Southern District of Texas.[214] According to the Southern District Court, "'loss' encompasses only two types of harm: costs to investigate and respond to an offense, and costs incurred because of a

---

of related occurrences that could result from or occur contemporaneously with the unauthorized access of computers); Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (arguing that most "business related civil claims brought under the [CFAA] are brought pursuant to subsection (c)(4)(A)(i)(I)").

208. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (Supp. V 2011).

209. *Id.* § 1030(e)(11) (2006).

210. Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *3 (N.D. Tex. Apr. 20, 2011).

211. *See id.* (determining that the plaintiff "pleaded a plausible CFAA claim" because the facts presented were sufficient to infer the defendant exceeded authorization when he used the plaintiff's information to compete directly with the plaintiff); Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (providing a description of the case and evaluating the decision of the court).

212. *See Meats*, 2011 WL 1515028, at *3 (evaluating the lost revenues resulting from a loss in the sale of meat products directly related to the defendant acting in competition with the plaintiff).

213. *See id.* (reaching the conclusion that the plaintiff stated sufficient damages where the plaintiff alleged lost revenue "aggregate[ed] in at least $5,000 in value").

214. *See* Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (providing detailed analysis of the difference between the two federal district court holdings).

service interruption."[215] Until this important issue is settled, the benefit of stating a claim under the CFAA to a plaintiff–employer in Texas, in lieu of a misappropriation of a trade secret claim, remains a risky proposition because the employer may be severely limited in its recovery of monetary damages. Regardless of which view ultimately prevails, what is certain is that the CFAA requires plaintiffs to establish damages of at least $5,000.[216] TUTSA, in contrast, does not have a minimum damage requirement.[217] In fact, TUTSA might allow a plaintiff to obtain injunctive relief where damages have yet to occur.[218]

V. CONCLUSION

Several issues are raised when an employee authorized to access a Texas employer's computer system uses the system to obtain information for an enterprise that directly competes with the employer's business. However, the most pertinent question is whether there is an avenue for the employer to recover monetary damages caused by the former employee and to prevent future use of the information. For the Texas litigator posed with client questions on this distressing matter, two avenues for recovery are readily available. The litigator could file a complaint based on Texas trade secret law, which consists of TUTSA[219] and Texas common law.[220] In the alternative, the Texas litigator could pursue civil liability through use of the CFAA.[221]

---

215. *See id.* (citing Alliantgroup, LP v. Feingold, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011)) (noting that some courts within Texas provide a narrow view of "loss" that does not encompass misappropriated information presented as lost revenue); *see also* Alliantgroup, LP v. Feingold, 803 F. Supp. 2d 610, 614 (S.D. Tex. 2011) (delivering an opinion adverse to the plaintiff in a cause of action filed to recover monetary damages under the CFAA where the defendant "took customer lists and confidential or proprietary information and disclosed that information" to a subsequent employer); Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 775–76 (S.D. Tex. 2010) (concluding that the plaintiff failed to properly state a complaint under the CFAA because the alleged losses did not result from "costs associated with that examination").

216. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (Supp. V 2011) (requiring that claims show a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value").

217. *See* TEX. CIV. PRAC. & REM. CODE ANN. § 134A.004 (West Supp. 2013) (allowing a plaintiff to recover economic damages without specifying a minimum damage amount).

218. *Id.* § 134A.003(a) (permitting injunctive relief where there is mere "threatened misappropriation").

219. *Id.* §§ 134A.001–.008.

220. *See* Simplified Telesys, Inc. v. Live Oak Telecom, LLC, 68 S.W.3d 688, 690 (Tex. App.—Austin 2000, pet. denied) (outlining the common law elements of a misappropriation of a trade secret claim through a restatement of the plaintiffs allegations).

221. *See* 18 U.S.C. § 1030(a)(2) (Supp. V 2011) (creating a federal offense where an actor "intentionally accesses a computer without authorization"); *Id.* § 1030(c)(4)(A)(i)(I) (limiting recovery under the CFAA in civil actions to instances where the "loss" exceeds $5,000); *Id.* § 1030(g)

Generally speaking, Texas trade secret laws have some distinct advantages. First, Texas trade secret laws are well settled through ample case law;[222] although TUTSA may create ambiguity in some nuanced areas.[223] Second, under TUTSA, a plaintiff does not have to meet any minimum showing of damages.[224] Third, injunctive relief is available for "actual or threatened misappropriation," meaning that a former employer may enjoin an employee before any damages occur.[225] Finally, a plaintiff can recover exemplary damages[226] and attorney's fees.[227]

Conversely, a detailed review of the CFAA demonstrates that the CFAA remains a workable alternative.[228] Whereas a misappropriation claim requires proving that the information obtained qualifies as a trade secret,[229] such an inquiry is not required for the CFAA.[230] Similarly,

---

(clarifying that the CFAA is available to plaintiffs in a civil action "to obtain compensatory damages and injunctive relief" and providing for a two-year statute of limitations).

222. *See* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—Austin 2004, pet. denied) (identifying the four elements of the tort of misappropriation of a trade secret as a "common-law tort cause of action"); *see also In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003) (clarifying that Texas continues to follow the six-factor test "to determine whether a trade secret exists" that was found in the RESTATEMENT OF TORTS § 757 regardless of the fact that it no longer appears in the revised RESTATEMENT (SECOND) OF TORTS); Computer Assocs. Int'l v. Altai, Inc., 918 S.W.2d 453, 455 (Tex. 1994) (citing Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 766 (1958) (referencing RESTATEMENT (FIRST) OF TORTS § 757 (1939)) (establishing the definition of trade secrets that Texas adheres to in the context of civil suits).

223. *See* Alex Harrell, *Is Anything Inevitable?*, 76 TEX. B.J. 757, 762 (2013) (discussing how the adoption of TUTSA has left open the question of whether Texas will adopt the inevitable disclosure doctrine, specifically noting that only further litigation will flesh out the issue). *But see* Joseph F. Cleveland Jr. & J. Heath Coffman, *Protecting Trade Secrets Made Simple*, 76 TEX. B.J. 751, 755 (2013) ("TUTSA moderniz[ed] the law of misappropriation of trade secrets in Texas by providing a consistent and predictable statutory framework for the protection of trade secrets and litigating trade secret cases.").

224. *See* CIV. PRAC. & REM. § 134A.004 (West Supp. 2013) (permitting recovery of "actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss," but nowhere limiting recovery for damages beyond a particular threshold).

225. *See id.* § 134A.003(a).

226. *Id.* § 134A.004(b) ("If [willful] and malicious misappropriation is proven by clear and convincing evidence, the fact finder may award exemplary damages in an amount not exceeding twice any award made under Subsection (a).").

227. *Id.* § 134A.005 ("The court may award reasonable attorney's fees to the prevailing party if: (1) a claim of misappropriation is made in bad faith; (2) a motion to terminate an injunction is made or resisted in bad faith; or (3) [willful] and malicious misappropriation exists.").

228. *Compare* 18 U.S.C. § 1030(a)(2) (Supp. V 2011) (articulating the three elements of a CFAA claim), *with* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—Austin 2004, pet. denied) (providing the elements of a misappropriation claim).

229. *See* H.E. Butt Grocery Co. v. Moody's Quality Meats, Inc., 951 S.W.2d 33, 35–36 (Tex. App.—Corpus Christi 1997, writ denied) (evaluating the "five-element process for [producing] beef fajitas" and determining that because "[the] process gave him a competitive [advantage]" and "the

while monetary damages for the misappropriation of a trade secret hinge upon use of the trade secret, merely obtaining the information in question is sufficient to trigger liability under the CFAA;[231] although this distinction is severely hampered by the CFAA's $5,000 minimum pleading requirement.[232]

While the differences between the two causes of action become clearer from a comparison of the elements for each cause of action, the Texas litigator should be aware of three risks associated with filing a claim under the CFAA in the Fifth Circuit.

First, the meaning of the terms "without authorization" and "exceeds authorization" under the CFAA remains contested.[233] However, it is

marinating process was not available to the general public" it qualified as a trade secret); *see also In re* Bass, 113 S.W.3d 735, 741–42 (Tex. 2003) (applying the "six-factor test to determine whether [plaintiff's] geological seismic data" was a trade secret and finding that the value of the information in question qualifies the information as a trade secret).

230. *See* 18 U.S.C. § 1030(a)(2) (listing violations of the CFAA); *see also* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (focusing on whether a former employee exceeded authorized access when he downloaded information rather than whether the downloaded information had intrinsic value to justify a claim under the CFAA); United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (en banc) (maintaining focus on whether Nosal had authorization to access the computer rather than focusing on whether the executive search firm's data met a value threshold necessary to maintain suit under 18 U.S.C. § 1030 (2006 & Supp. V 2011)); United States v. John, 597 F.3d 263, 271–73 (5th Cir. 2010) (opining that a violation of the CFAA occurs where the defendant acted without authorization and not making that holding dependent on the nature of the information obtained by the defendant); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (emphasizing the importance of authorization to a CFAA claim in concluding that the defendant's conviction was maintainable); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (investigating the relationship between the plaintiff and the defendant and the purpose of the defendant's actions in a suit filed under the CFAA, rather than the nature of the information the defendant accessed).

231. *Compare* 18 U.S.C. § 1030(a)(2) (making recovery dependent upon whether the information is "obtain[ed]"), *with* Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1205 (5th Cir. 1986) (evaluating the use requirement in misappropriation claims and concluding that "while the nature of the use may be relevant in determining the proper extent of damages, its existence must also be shown to establish wrongdoing in the first place").

232. 18 U.S.C. § 1030(c)(4)(A)(i)(I).

233. *See Miller*, 687 F.3d at 207 (finding that the defendant, a former employee of the plaintiff, did not violate the CFAA because the defendant was authorized to access the information stored on the computers, despite the fact that the defendant's use of the information was prohibited by a computer use policy between the defendant and the plaintiff); *Nosal*, 676 F.3d at 864 (affirming the decision of the court below to dismiss a CFAA claim based on a narrow reading of the statute because, according to the court, the "CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*"); *John*, 597 F.3d at 271–73 (emphasizing a prior interpretation of the CFAA and concluding that, despite authorization to access the computer, the defendant exceeded authorized access); *Rodriguez*, 628 F.3d at 1263 (finding a violation of the CFAA based on the use policy between employee and employer); *Citrin*, 440 F.3d at 420 (acknowledging a violation of the CFAA in a suit between an employer and an employee); *see also* Pamela Taylor, Comment, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on*

clear the scope of authorization is dependent upon the intended use for which the employer granted authorization.[234] Thus, where the employee accessed the computer data to compete directly with the employer in the initial hypothetical, there is no doubt that the employee acted without authorization.[235] Precedents established by two sister circuit courts tend to support this conclusion.[236] However, from the perspective of other federal appellate circuit courts, a violation of the CFAA would not occur in the hypothetical addressed in this Comment unless the information obtained by the employee was that which may have been on the computer, but the employee was not authorized to access.[237] The Fifth Circuit adopted the "intended-use analysis" before the adoption of contrary interpretations maintained by the other circuits,[238] and in the context of criminal suits.[239] This suggests that a change in understanding of the law

---

Employers, 49 HOUS. L. REV. 201, 209–26 (2012) (writing about the distinctions between various federal appellate court interpretations of the CFAA); Michael R. Greco, *CFAA Does Not Apply to Employee Data Theft According to Ninth Circuit*, MARTINDALE (Apr. 13, 2012), http://www.martindale.com/computers-office-equipment/article_Fisher-Phillips-LLP_1495924.htm (elaborating on interpretations of the CFAA advanced by various federal appellate courts prior to the release of the Ninth Circuit's 2012 decision).

234. *See John*, 597 F.3d at 271–73 (affirming the jurisdiction's adherence to the "intended-use analysis" when comparing allegations to the constructs of the CFAA); United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (adopting the "intended-use analysis" as it relates to violations of the CFAA); *see also Meats*, 2011 WL 1515028, at *3 (applying the "intended-use analysis" to determine that the plaintiff stated a cause of action under the CFAA).

235. *See Meats*, 2011 WL 1515028, at *1 (considering whether a former employee who accessed the plaintiff's computer system to obtain information and who then used the information to compete with the plaintiff violated the CFAA).

236. *Rodriguez*, 628 F.3d at 1263 (finding a violation of the CFAA based on a use agreement between the parties); *Citrin*, 440 F.3d at 420 (examining the defendant's actions from the perspective of the actions in relation to duties owed to a principal).

237. *See Miller*, 687 F.3d at 199 (holding that a violation of the CFAA did not occur where the former employee "downloaded company's proprietary information and used it in making presentation to customer on behalf of competitor"); *Nosal*, 676 F.3d at 857 (construing the statute narrowly to avoid "transform[ing] the CFAA from an anti–hacking statute into an expansive misappropriation statute").

238. *Compare Miller*, 687 F.3d at 207 (affirming a restrictive interpretation to the CFAA in 2012), *and Nosal*, 676 F.3d at 864 (adopting a restrictive interpretation of the CFAA in 2012), *with John*, 597 F.3d at 271–73 (emphasizing the importance of the "intended-use" to find the defendant breached the CFAA prohibitions through its decision in 2010), *Rodriguez*, 628 F.3d at 1263 (interpreting the facts alleged to find a breach of the CFAA where an employer policy prohibiting the defendant's use of the computer existed in 2010), *and Citrin*, 440 F.3d at 420 (clarifying when violations of the CFAA occur). *But see* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (addressing when violations of the CFAA occur and finding "that authorization to use a computer [does not cease] when an employee resolves to use the computer contrary to the employer's interest").

239. *See John*, 597 F.3d at 271–73 (addressing the applicability of the CFAA in the context of a criminal suit brought by the United States government); *Phillips*, 477 F.3d at 219 (adopting the

and the facts involved could warrant adopting the more restrictive approach that would bar recovery; hence, possible revaluation of the "intended-use" approach makes reliance on Fifth Circuit precedent an uncertain proposition.

Second, reliance on the CFAA as it exists in statute today is risky because the statute is the subject of ongoing congressional scrutiny.[240] If the federal government adopts the proposed changes to the CFAA, the nature of the information obtained could become a new obstacle for the Texas litigator to overcome.[241] Amending the statute to focus on the nature of the information obtained eliminates the clear advantage of the CFAA over misappropriation of trade secrets because the mere act of obtaining information would no longer trigger liability.[242] Finally, reliance on the CFAA by Texas litigators and employers is risky because the matter of sufficient damages to file suit under the CFAA is unsettled in the federal district courts of Texas.[243] Depending upon the court where the

"intended-use analysis" approach in a criminal suit).

240. *See* S. 3342, 112th Cong. § 306 (2012) (proposing an amendment to the CFAA that would affect civil suits brought under the CFAA); Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 41 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (discussing justifications for amending the CFAA at a congressional hearing); Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 11–13 (2011) (statement of Richard W. Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice) (arguing against amendment of the CFAA at a congressional hearing).

241. *See* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 46 (2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (recommending "significant limits on the kind of information that can trigger liability under" the CFAA such as through a requirement that the information obtained have a "value of more than $5,000" rather than cause merely cause a loss of $5,000 or that the information be of a "sensitive or private" nature).

242. *Compare* 18 U.S.C. § 1030(a)(2)(c) (Supp. V 2011) (creating a violation where any information is obtained), *with* Trilogy Software, Inc. v. Callidus Software, Inc., 143 S.W.3d 452, 463 (Tex. App.—Austin 2004, pet. denied) (making recovery in a misappropriation claim dependent upon whether the information appropriated qualifies as a trade secret).

243. *See* Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (noting a split between the Northern and Southern Federal District Courts for the state of Texas over sufficient damages to maintain a suit under the CFAA). *Compare* Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *3 (N.D. Tex. Apr. 20, 2011) (finding sufficient loss to maintain a suit based on "lost revenue that could amount to over $5,000 over the course of one year"), *with* Alliantgroup, LP v. Feingold, 803 F. Supp. 2d 610, 630 (S.D. Tex. 2011) (holding that

suit is heard, consequential losses in revenue unrelated to investigations of unauthorized access may be insufficient.[244]

Ultimately, the differences between Texas trade secret law, including TUTSA, and the CFAA can be best illustrated by returning to the initial hypothetical.[245] By providing two alternate versions of the hypothetical, each lending facts toward a particular claim, it is possible to discern when Texas trade secret law or the CFAA would be more appropriate.

A claim under Texas trade secret law would be ideal in the following situation: (1) there is business information that is reasonably protected and derives value from its secretive nature; (2) an employee acquires the information to compete with the employer and quits; (3) the former employee discloses the information to his new employer; and (4) the former employer suffers damages from the disclosure.[246]

While on the other hand, a claim under the CFAA would be well-suited in the following situation: (1) some business information exists on an employer's computer; (2) an employee either intentionally accesses the information without permission or has permission, but accesses it in a way that exceeds the employee's authorization; (3) the employee obtains the information; and (4) the employer suffers damages in excess of $5,000.[247]

---

the plaintiff failed to "allege or present evidence of any cognizable losses" and could not maintain suit based on the CFAA), M–I LLC v. Stelly, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010) (determining that "lost profits, loss of customers and loss of future business opportunities" occurring independently are insufficient to maintain suit under the CFAA because the loss must be "a result of investigation or interruption of computer service"), *and* Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010) (concluding that the plaintiff failed to allege proper facts to support a claim under the CFAA because the plaintiff did "not allege an interruption of service as a result of [defendant's] actions, nor any investigation or response to [defendant's] alleged access of the computer").

244. *See* Shawn E. Tuma, *New "Employment" Computer Fraud and Abuse Act Case . . . but with a Twist!*, COMPUTER, DATA BREACH PRIVACY, SOCIAL MEDIA, L. BLOG (Apr. 25, 2011, 10:41 PM) http://shawnetuma.com/2011/04/25/new-employment-computer-fraud-and-abuse-act-case-but-with-a-twist/ (evaluating the loss provisions of the CFAA and providing insight on which types of loss have been deemed sufficient to support damages in Texas district courts).

245. *See supra* endnote 1.

246. *See* TEX. CIV. PRAC. & REM. §§ 134A.001–.008 (West Supp. 2013) (codifying Texas trade secret common law to provide uniformity and modernization); *Trilogy Software*, 143 S.W.3d at 463 (Tex. App.—Austin 2004, pet. denied) (calling attention to the four elements of a misappropriation claim); *see also In re* Bass, 113 S.W.3d 735, 739 (Tex. 2003) (asserting that the six-factor test "to determine whether a trade secret exists" that was found in the *Restatement (First) of Torts*, but does not appear in the revised *Restatement (Second) of Torts)*, is still looked to by Texas); Computer Assocs. Int'l v. Altai, Inc., 918 S.W.2d 453, 455 (Tex. 1994) (citing Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 766 (1958) (referencing RESTATEMENT (FIRST) OF TORTS § 757 (1939)) (providing the definition of a trade secret).

247. *See* 18 U.S.C. § 1030 (2006 & Supp. V 2011) (providing a federal cause of action for the misappropriation of information for protected computers if obtained improperly that causes damages

As apparent, determining which of these causes of actions is more advantageous is highly fact-specific.

over $5,000); *see also* Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. 42 (2011) (quoting 18 U.S.C. § 1030(a)(2)(C) (Supp. V 2011) (written statement of Orin S. Kerr, Professor of Law, George Washington University), *available at* http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1003&context=faculty_testimony (delineating the elements of a CFAA claim).