AN INSIDE JOB: THE INTERSECTION OF FEDERAL COMPUTER LAW AND TRADE SECRET LAW IN CASES OF INSIDER MISAPPROPRIATION

Jenna M. Andrews*

I. Introduction

A business's greatest risk to protecting its valuable trade secrets is not outside hackers or competing firms – it is company insiders.[1] Insider misappropriation is a problem that affects all types of businesses from multinational corporations to start-ups.[2] Theft at-

* J.D. Candidate, Suffolk University Law School, 2018; Production Editor, The Journal of High Technology Law, 2017-2018; B.S. Marketing & Business Communications, Johnson & Wales University, 2012.

[1] *See* R. MARK HALLIGAN & RICHARD WEYAND, TRADE SECRET ASSET MANAGEMENT 78 (Weyand Associates, Inc., 2016) (indicating that U.S. companies report that the greatest risks to their proprietary data are employees); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 294 (2009) (noting that in the majority of trade secret theft, the misappropriator was someone the owner knew).

[2] *See* BRIAN YEH, CONG. RESEARCH SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT L. AND LEGIS. 1 (2016) (providing examples of trade secrets of a few major, multinational companies); Almeling, *supra* note 1, at 292 (recognizing that the theft of trade secrets cost companies approximately $300 billion annually); Molly Hubbard Cash, *Keep It Secret, Keep It Safe: Protecting Trade Secrets By Revisiting the Reasonable Efforts Requirement in Federal Law,* 23 J. INTELL. PROP. L. 263, 264 (2016) (highlighting that trade secret theft can have devastating impacts on small and medium sized businesses as they tend to rely heavily on trade secret protection as "an alternative to more expensive forms of intellectual property protection").

 ISSN 1536-7983.

tributed to employees, partners or other insiders accounts for 90 percent of all trade secret cases.[3] Businesses in information-based industries, such as technology, financial services, insurance, and media are particularly dependent on trade secrets, as they provide them with a competitive advantage in their respective industries and to keep potential competitors from entering the market.[4] For many modern businesses, intellectual properties, such as trade secrets, are their most substantial and valuable assets.[5] For example, a high tech company may have few physical assets, but have billions of dollars in market capitalization based on its intangible assets.[6] Additionally, it is estimated that value of trade secrets owned by publicly traded companies in the United States is 5 trillion dollars.[7] With business value dependent on the security of information assets, it is critical to these firms that laws provide adequate protection for trade secrets against their greatest threat.[8]

As trade secrets are commonly created, used, and stored on computers, they are not only protected by trade secret law, but potentially by computer law as well.[9] Before the enactment of the Defend Trade Secrets Act of 2016, which provided trade secret owners with a federal civil remedy, companies could bring lawsuits under state

[3] *See* YEH, *supra* note 2, at 14 (stipulating that owners know the misappropriator in the vast majority of trade secret cases).

[4] *See* HALLIGAN, *supra* note 1, at 18 (indicating that in the information economy, shareholder value is driven by a corporation's information assets); *see* Cash*, supra* note 2, at 264 (describing how companies in information-based industries depend on self-derived data for competitive advantages).

[5] *See* HALLIGAN, *supra* note 1, at 20 (stating that a company's value is often strongly dependent on its trade secrets).

[6] *See* HALLIGAN, *supra* note 1, at 18 (suggesting that information drives shareholder value).

[7] *See* YEH, *supra* note 2, at 13 (estimating that economic loss connected to trade secret theft in the U.S. is between 1 percent and 3 percent of the Gross Domestic Product).

[8] *See* HALLIGAN, *supra* note 1, at 23 (explaining that trade secrets can only be authenticated through litigation occurring after the information has been misappropriated).

[9] *See* Robert Milligan, *An Employee Is Stealing Company Documents…That Can't Be Protected Activity, Right?*, TRADING SECRETS (July 3, 2013), *archived at* https://perma.cc/Q3D3-2VKS (suggesting various legal actions for employee data theft); *see also* Kyle Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J. L. TECH. & POL'Y 429, 430 (2009) (noting that the use of computers for trade secret storage potentially subjects trade secrets to protection from computer misuse statutes).

trade secret law and under common law causes of action in state courts.[10] In order to gain access to federal courts, trade secret owners pursued claims under the Computer Fraud and Abuse Act ("CFAA") on its own or accessed federal courts through diversity jurisdiction.[11] Employee misappropriation actions brought under the CFAA have been met with skepticism from courts, and there is currently a circuit split regarding the extent to which the CFAA imposes liability in this context.[12] The First, Fifth, Seventh, and Eleventh Circuits have addressed this issue using a broad application of the CFAA, allowing employers to bring claims against employees who have breached a duty of loyalty by using an employer's information assets in a disloyal manner.[13] The Second, Fourth and Ninth Circuits have used a more narrow, "technical" application, limiting employers from bringing misappropriation claims under the CFAA if the employer had granted the employee access to the specific misappropriated information.[14]

In May of 2016 Congress passed the Defend Trade Secrets Act ("DTSA"), which provides broad protections against trade secret misappropriation and arguably allows employers access to federal courts without reliance on the CFAA.[15] While the extent to which

[10] *See* Defend Trade Secrets Act, 18 U.S.C.A. § 1836 (2016) (creating "appropriate injunctive relief" against trade secret violations).
[11] *See* The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2008) (denoting specific types of violations under the Act); *see also* HALLIGAN, *supra* note 1, at 146-50 (listing the civil causes of action available for misuse of trade secrets prior to the enactment of the DTSA).
[12] *See* Mark Klapow et al., *Recent Case Highlights Circuit Split on Important Computer Fraud and Abuse Act Question*, CROWELL & MORING (May 17, 2016) *archived at* https://perma.cc/UR5E-ATDF (highlighting the continued circuit split over CFAA interpretation).
[13] *See* Robert D. Sowell, *Misuse of Information Under the Computer Fraud and Abuse Act: On What Side of the Circuit Split Will the Second and Third Circuits Wind Up?*, 66 FLA. L. REV. 1747, 1751 (2015) (indicating that the First, Fifth, Seventh, and Eleventh Circuits interpret the statute broadly leading to the approaches of a contract-based theory or an agency-based theory).
[14] *See* Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 12 DUKE L. & TECH. REV. 1, *4-7 (suggesting that courts have adopted either the broad, employer-friendly interpretation of the CFAA, or the narrow interpretation that limits employers from asserting employee misconduct claims); *see also* Klapow et al., *supra* note 12 (discussing the narrow interpretation of employee misappropriation).
[15] *See* 18 U.S.C.A. § 1836 (2016) (outlining the guidelines to bring forth a trade secret claim); *see also* Claire Laporte & Emma S. Winer, *Congress Passes Sweeping*

the CFAA provides protection against the misuse of trade secrets by company insiders is unclear, the DTSA will provide an effective alternative to recovery for insider misappropriation.[16]

Part II of this note examines the Computer Fraud and Abuse Act, focusing on the elements of the statute that mirror trade secret misappropriation.[17] Part II then discusses the controversial circuit split over the interpretation of the CFAA in the insider misappropriation context.[18] Lastly, Part II provides a background on trade secret law and introduces the newly enacted Defend Trade Secret Act.[19] Part III examines several notable cases of insider misappropriation that were brought under the CFAA.[20] Part IV analyzes the two theories of interpreting the CFAA in the disloyal employee context and argues that narrow interpretation is the correct approach.[21] Finally, Part IV evaluates the DTSA as an alternative federal action to the CFAA and ultimately concludes that cases of insider trade secret misappropriation should be brought exclusively under the DTSA.[22]

II. History

A. The Computer Fraud and Abuse Act and Trade Secrets

Mainstream computer use revolutionized business by enhancing productivity, increasing connectivity, and making data mobile and readily available.[23] However, advancements in technology have

New Legislation to Protect Trade Secrets, 62 No. 3 PRAC. LAW 37-38 (June 2016) (indicating that the DTSA will provide a cause of action for a "broad variety of trade secret cases").

[16] *See* Laporte & Winer, *supra* note 15, at 37 (discussing the importance of broader alternative solutions to trade secret misappropriation).

[17] *See infra* Part II.A.

[18] *See infra* Part II.B.

[19] *See infra* Part II.C.

[20] *See infra* Part III.

[21] *See infra* Part IV.

[22] *See infra* Part IV.

[23] *See* Sarah Boyer, *Current Issues in Public Policy: Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?,* 6 RUTGERS J.L. & PUB. POL'Y 661, 663-64 (Spring 2009) (indicating that technology has drastically changed the way businesses operate); *see* Pamela Taylor, *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, 204 (Apr. 17, 2012) (noting that employees can easily access company data from virtually any location).

significantly increased the risk of information theft and misuse.[24] The Computer Fraud and Abuse Act was first enacted as a criminal statute to cover a broad spectrum of computer crimes, particularly hacking and espionage.[25] The CFAA's criminal sanctions have since been expanded from covering government and financial institution computers to covering computers in the private sector.[26] The CFAA was further amended to allow civil actions to be brought by any person who suffers loss from a violation of the CFAA resulting in damages of $5,000 or more.[27] As the protective scope of the statute expanded, the CFAA became a tool for companies to privately litigate the theft of trade secrets and information assets.[28]

Sections 1030 (a)(2) and 1030(a)(4) of the CFAA mirror trade secret misappropriation in the context of an employee taking proprietary information from their employer through the use of a computer.[29] Section 1030 (a)(2) of the CFAA prohibits the act of (1) intentionally

[24] *See* Boyer, *supra* note 23, at 664 (summarizing the risks arising from advancements in technology).

[25] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009) (identifying that the legislative intent behind the CFAA was to "enhance the ability to prosecute computer crimes" and "target hackers who accessed computers to steal data or disrupt computer functionality"); *See* Kelsey T. Patterson, *Narrowing it Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 492-93 (describing the CFAA as a criminal statute enacted to address hacking). *See also* Taylor, *supra* note 23, at 207 (indicating that Congress aimed to create a broad statute to cover a broad range of computer crimes).

[26] *See* S. REP. NO. 104-357, at 7 (1996) (proposing an extension of the CFAA to include potentially any computer used in interstate or foreign commerce or communication).

[27] *See* The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2017) (allowing for private civil actions against conduct that violates the CFAA).

[28] *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012) [hereinafter *WEC Carolina Energy*] (rejecting the imposition of liability against authorized users and emphasizing the CFAA should be interpreted to protect companies from unauthorized users); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (disseminating company data after terminating an employment relationship constitutes unauthorized access and therefore is actionable under the CFAA); Ef Cultural Travel Bv v. Explorica, 274 F.3d 577, 581-82 (1st Cir. 2001) (discussing how even after termination, disseminating information in violation of a confidentiality agreement constitutes use which exceeds authorization).

[29] *See* Brenton, *supra* note 9, at 432-50 (suggesting that sections of the CFAA parallel trade secret law, albeit they lack the evidentiary safeguards found in trade secret law).

accessing a computer without authorization or by exceeding authorized access, (2) obtaining information from that protected computer, and (3) causing loss in excess of $5,000.[30] Additionally, section 1030(a)(4) prohibits (1) accessing a protected computer without authorization or exceeding authorized access, (2) with intent to defraud, and (3) furthering fraud by obtaining anything with a value in excess of $5,000.[31] These provisions of the CFAA appear to impose broad liability for obtaining valuable information from a computer to which the individual did not have access.[32] Unlike trade secret laws, the

[30] *See* 18 U.S.C. § 1030(a)(2).

> (a) Whoever—. . . .
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> (B) information from any department or agency of the United States; or
> (C) information from any protected computer;

Id. See also Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1032 (N.D. Ill. 2008) (clarifying that "any protected computer" refers to any computer providing access to the internet). In addition to computers used exclusively by the federal government or financial institutions, a protected computer may refer to any computer "used in interstate or foreign commerce or communication . . . ." *Id.*

[31] *See* 18 U.S.C.S. § 1030 (a)(4).

> (a) Whoever . . . .
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

Id.

[32] *See* 18 U.S.C.S. § 1030 (a)(2) (barring the unauthorized access of valuable information); *see also* 18 U.S.C.S. § 1030 (a)(4) (prohibiting individuals from obtaining information from the fraudulent access of computer).

CFAA focuses solely on the conduct of the defendant and does not place any qualifying characteristics on the accessed information.[33]

B. The Circuit Court Split

Employers have used the civil action available through the CFAA against former employees who have used company computers to take trade secrets or other information assets in order to form their own company or to join a competing firm.[34] However, courts have struggled with application of the CFAA in the disloyal employee context.[35] The vague language of the statute has left Federal Circuits divided over the meaning of "without authorization" and "exceeds authorized access" and whether employees should be held liable for the misuse of their employer's information assets under the CFAA.[36] The First, Fifth, Seventh, and Eleventh Circuits have taken an expansive view of the application of the CFAA in the disloyal employee context.[37] These courts have held that under the CFAA, an action arises when an employee permissibly accesses information on a com-

[33] *See* Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 335 (2015) (explaining that the CFAA contains several provisions that can be invoked by trade secret plaintiffs, although the misappropriated information is not required to qualify as a trade secret); *see also* Brenton, *supra* note 9, at 431 (suggesting that the employment of the CFAA to litigate trade secret theft in federal court ignores the policies underlying trade secret law).

[34] *See* James Juo, *Split Over the Use of the CFAA Against Disloyal Employees*, THE FED. LAW 51 (2014) (stating that the CFAA has been used by employers against disloyal employees who have misappropriated computer data).

[35] *See id.* (indicating division over the scope of the CFAA in the employee context).

[36] *See id.* (explaining that a circuit split exists regarding the scope of liability under the CFAA); *see also* Taylor, *supra* note 23, at 210 (indicating that two opposing approaches to the CFAA have developed, thus creating a split in the Federal Circuits).

[37] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (setting out the "agency theory" of interpreting authorization under the CFAA); Ef Cultural Travel BV v. Explorica, Inc., 274 F.3d 578, 581 (1st Cir. 2001) (holding "that because of the broad confidentiality agreement appellants actions' 'exceeded authorized access,' and so [the court does] not reach the more general arguments made about statutory meaning, including whether use of a scraper alone renders access unauthorized.") s*ee also* Pollaro, *supra* note 14, at *1 (summarizing the holding in *Citrin* as establishing that access is unauthorized when an employee decides to act inconsistently with his employer's interest).

puter, but uses the information in a manner inconsistent with the employer's policies.[38] The Seventh Circuit adopted an "agency theory" interpretation, holding that an employee's authorization terminates when he acts against the interest of the employer.[39] This theory considers authorization to be defined by the agency relationship between the employer and employee, rather than the technical authorization to access a computer, such as log in credentials.[40] For example, an employer may act against the interests of his employer when he supplies a competing company with a compiled list of his firm's acquisition targets.[41] The broad interpretation applied by these courts is beneficial to employers because it merely requires them to establish that the employee's actions were adverse to the employer in order to show that the employee did not have authorization under the CFAA.[42]

Conversely, the Second, Fourth and Ninth Circuits have rejected the "agency theory" and applied a narrow interpretation of the CFAA.[43] These courts have considered the legislative history of the

[38] *See* Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155, 163 (2008) (maintaining that under the agency theory, an employee loses authorization when the employee is acting with a disloyal purpose).

[39] *See Citrin*, 440 F.3d at 420 (explaining that the employee's access rights were terminated when he breached his duty of loyalty); *see also* Juo, *supra* note 34, at 51 (specifying that the Seventh Circuit relied on the agency relationship between an employer and employee in establishing the existence of authorization).

[40] *See* Brenton, *supra* note 9, at 437 (indicating that a broad interpretation considers "authorization" as defined by agency law instead of defining authorization in a technical sense).

[41] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (opining that the employee lost authorization to access company computers and the contained data when he sent his employer's proprietary information to a competitor via email).

[42] *See* Juo, *supra* note 34, at 51 (illustrating that the broad approach adopted by the Fifth, Seventh, and Eleventh Circuits find liability when an employee merely violates the computer use policy of the employer).

[43] *See* United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015) (indicating that the agency theory only considers the culpable behavior at issue and fails to recognize the implications of a broad CFAA interpretation on the conduct engaged in by millions of people); *WEC Carolina Energy*, 687 F.3d 199, 206 (4th Cir. 2012) (declining to follow the agency theory of *Citrin*). "Although an employer might choose to rescind an employee's authorization for violating a use policy, we do not think Congress intended an immediate end to the agency relationship and, moreover, the imposition of criminal penalties for such a frolic." *Id.*; LVRC Holding LLC v.

CFAA and determined that the law was aimed exclusively at penalizing external data theft, such as hacking.[44] Under the narrow interpretation, unauthorized access occurs when an individual does not have physical or technological access to a computer, such as access to a company laptop or a password to enter into a company network.[45] For example, when a former employee purposefully breaches a firm's internal network after the employee's log in credentials have been revoked and accesses the firm's internal database, he is acting without authorization.[46] These courts have also determined that the violation of a company's use policies, resulting in non-permissive use of information, does not qualify as exceeding authorization under the CFAA.[47] This approach limits employers because it does not impose liability upon a former employee who misuses trade secrets to which he was given access to in the course of his work.[48]

Brekka, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (stating that the court is not persuaded by the reasoning in *Citrin*, primarily because the court did not want to impose criminal liability for violating employer-placed limits).

[44] *See Valle*, 807 F.3d at 525 (suggesting that the "computer crime[s]" referred to in the statutes are understood to mean hacking or trespassing into a computer system); *see also* Brenton, *supra* note 9, at 438 (indicating that in considering the legislative history of the CFAA, courts find that the statute was intended to apply to outside hackers instead of disloyal employees abusing their access).

[45] *See WEC Carolina Energy*, 687 F.3d at 204-05 (indicating that an employee using information in an impermissible manner does not "exceed authorized access" under the CFAA if the employee has a password and username allowing him to access that information); *see also* Brenton, *supra* note 9, at 438 (stating that narrow interpretation jurisdictions use physical or technological access, such as a password, as an indication of authorization).

[46] *See* United States v. Nosal, 844 F.3d 1024, 1029 (9th Cir. 2016) [hereinafter *Nosal II*] (determining that a former employee's conduct of accessing a company database through the use of a current employee's login credentials was a breach of a technological barrier and therefore qualified as "without authorization" under the CFAA).

[47] *See WEC Carolina Energy*, 687 F.3d at 207 (arguing that Congress did not intend to criminalize the use of information in a manner that is not authorized, but rather to criminalize the misuse of information that one is not authorized to access).

[48] *See* Juo, *supra* note 34, at 52 (emphasizing that the ability of an employer to use the CFAA against disloyal employees is limited in jurisdictions that apply the narrow interpretation).

C. Trade Secret Law

1. State Trade Secret Law

Trade secrets are commercially valuable information that provide a competitive advantage by virtue of not being generally known to the public.[49] They can result from years of research and development, time-consuming compilation, and expensive production costs.[50] Unlike other forms of intellectual property, there is no formal procedure for obtaining and registering a trade secret; they can only be preserved through litigation.[51] Prior to the enactment of a federal trade secret law, civil relief for trade secret misappropriation was available exclusively under common law and state law.[52]

---

[49] *See* UNIF. TRADE SECRETS ACT § 1 (NAT'L CONF. OF COMM'RS ON UNIF. ST. LAWS 1985) (defining trade secret).

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

Id. at 5; *see also* Peter J. Riebling, et al., *Landmark Trade Secrets Law Creates New Federal Civil Cause of Action and Compliance Obligations for All Employers*, THE NAT'L L. REV. 1, 1 (2016) (listing common examples of trade secrets). Trade secrets may include "customer lists, customer contract details, data, business plans, business strategies, formulas, methods, software codes, processes, procedures and techniques." *Id.*

[50] *See* Cash, *supra* note 2, at 267 (noting that "a trade secrets scan be the result of years of research and development and millions of dollars in production costs"); *see also* HALLIGAN, *supra* note 1, at 11-13 (listing examples of trade secrets and how they are developed). Trade secrets may exist in the area of research, development, engineering, marketing, sales, finance, accounting and also may include "negative know-how," such as what formulations or processes do not work. *Id.*

[51] *See* HALLIGAN, *supra* note 1, at 23 (highlighting that trade secrets can only be validated through litigation). Unlike patents, which are certified and the owner is presumed to have valid rights, trade secret owners, can only establish rights to their information by filing a suit for misappropriation. *Id.*

[52] *See* Riebling, *supra* note 49, at 1 (indicating that companies previously sought relief for trade secret misappropriation under state trade secret law).

Forty-seven states have adopted a version of the Uniform Trade Secret Act (UTSA), providing a unified standard for qualifying trade secrets and establishing misappropriation.[53]

In trade secret litigation under the UTSA, the first consideration is whether the information at issue meets the definition of a trade secret, first evaluating if the information derives economic value.[54] Secondly, it must be shown that the information is not generally known.[55] Thirdly, it must be established that the information is not readily ascertainable by proper means.[56] Lastly, the owner must show that reasonable precautions were undertaken in order to maintain the secrecy of the information.[57]

The trade secret owner must also establish that the trade secret was misappropriated, which can occur through either of two modes of conduct.[58] First, misappropriation can occur when an individual acquires a trade secret through conduct that breaches a contract or other obligation to keep the trade secret confidential.[59] Secondly,

---

[53] *See* Riebling, *supra* note 49, at 1 (stating that forty-seven states have adopted some form of the Uniform Trade Secret Act).

[54] *See* UNIF. TRADE SECRETS ACT § 1, *supra* note 49, at 5 (stating the requirement that information "derives independent economic value, actual or potential, from not being generally known to . . . . other persons who can obtain economic value from its disclosure or use"). *See also* Andrew Beckerman-Rodau, *Trade Secrets – The New Risks to Trade Secrets Posed by Computerization*, 28 RUTGERS COMPUTER & TECH L. J. 227, 243-44 (2002) (identifying economic value as a key requirement for a trade secret to exist).

[55] *See* UNIF. TRADE SECRETS ACT § 1, *supra* note 49, at 5-6 (explaining that "[t]he language 'not being generally known to and not being readily ascertainable by proper means by other persons' does not require that information be generally known to the public for trade secret rights to be lost").

[56] *See* UNIF. TRADE SECRETS ACT § 1, *supra* note 49, at 5 (establishing that trade secrets information may not be "readily ascertainable by proper means by, [to] other persons who can obtain economic value from its disclosure or use").

[57] *See* UNIF. TRADE SECRETS ACT § 1, *supra* note 49, at 5 (indicating that trade secrets must be subject to reasonable efforts to maintain the information's secrecy).

[58] *See* Beckerman-Rodau, *supra* note 54, at 251-53 (affirming that a trade secret action requires the owner to demonstrate that the information was improperly acquired or disclosed).

[59] *See* UNIF. TRADE SECRETS ACT § 1, *supra* note 49, at 4-5 (defining misappropriation).

> (2) "Misappropriation" means:
> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

misappropriation occurs when a trade secret is acquired through conduct deemed commercially improper.[60] Under UTSA, "improper means" may include illegal conduct such as theft, bribery or misrepresentation, but may also include otherwise legal conduct that exceeds the bounds of commercial reasonableness.[61]

2. Federalizing Trade Secret Law

The Economic Espionage Act (EEA) of 1996 is a federal statute that criminalized trade secret theft.[62] The statute implemented similar requirements for establishing a trade secret and a similar definition of misappropriation as the UTSA, only expanding the definition slightly to make it more applicable to modern technologies.[63]

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

Id.

[60] *See* Ronald Coleman et al., *Trade Secrets – The Basic Principals and Issues*, ABA 6 (2014) (identifying acquisition through improper means as a key element of misappropriation).

[61] *See* UNIF. TRADE SECRETS ACT § 1, *supra* note 49, at 4 (setting forth examples of "improper means" such as, "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means").

[62] *See* Economic Espionage Act, 18 U.S.C. § 1831 (2013) (outlining the elements of economic espionage); *see also* HALLIGAN, *supra* note 1, at 146 (describing the EEA as a federal criminal statute targeting trade secret theft).

[63] *See* 18 U.S.C. § 1839 (2016).

> (3) [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering in-

However, as a criminal statute, an EEA charge can only be brought by a federal prosecutor and does not provide private companies with a remedy for trade secret theft.[64] Consequently, less than a dozen EEA prosecutions occur nationwide every year in comparison with thousands civil trade secret lawsuits brought in state courts under the UTSA.[65]

Following the circuit split in employee misappropriation cases under the CFAA, many lawmakers, legal scholars, and businesses lobbied for a federal law covering trade secret misappropriation.[66] House Representative Jerrold Nadler (NY-D) argued,

> [A] fifty-state system does not work well in our increasingly mobile and globally interconnected world. Former employees and industrial spies are likely to

> formation, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information . . . .

Id.

[64] *See* HALLIGAN, *supra* note 1, at 146 (indicating that the protection provided by the EEA is not available to private businesses). Private companies seek remedies such as monetary damages and injunctive relief, while criminal statutes punish defendants with imprisonment and fines. *Id.*

[65] *See* HALLIGAN, *supra* note 1, at 146 (comparing the amount of EEA prosecutions to the amount of civil trade secret actions brought each year). The minimal amount of EEA cases are a result of the high standard of proof (beyond reasonable doubt) required in criminal cases and limited resources available to federal prosecutors. *Id.*

[66] *See* HALLIGAN, *supra* note 1, at 150 (describing the proposal made in 2008 for two amendments to the EEA providing solutions to some of the issues in trade secret law); *see also* YEH, *supra* note 3, at 18-19 (stating that supporters of the DTSA argued that a federal trade secret law would provide a solution to variations in statutory text and state court interpretations).

> carry or transfer secret information across state borders or overseas. The limited jurisdiction of the state court system makes it more difficult to obtain discovery or to act quickly enough to enforce an order that might stop the immediate loss of company secrets.[67]

In May of 2016, the Defend Trade Secrets Act was passed, providing federal courts with original jurisdiction over civil trade secret misappropriation.[68] The DTSA expanded the Economic Espionage Act to provide a civil remedy for owners of trade secrets related to products used in interstate or foreign commerce that have been misappropriated.[69] The new law adopts the same substantive standards for establishing a trade secret, as well as the same definition of misappropriation and improper means as the UTSA, signifying that UTSA precedent will apply to the new law.[70] The remedies available under the DTSA include monetary damages, injunctive relief and attorney's fees.[71]

Unlike the UTSA, the DTSA provides trade secret owners with access to federal courts without reliance on diversity jurisdiction or the CFAA.[72] Federal court is a more advantageous forum for businesses because federal courts have jurisdiction over patent and other types of intellectual property disputes and are generally experienced

---

[67] *See* Press Release, Rep. Nadler on Protecting Trade Secrets of Am. Companies (June 24, 2014), *archived at* https://perma.cc/ML6R-ADSW (advocating for changes in trade secret legislation).

[68] *See* Defend Trade Secret Act, 18 U.S.C. § 1836 (2016) (establishing civil and criminal protections of trade secrets in federal court); *see also* HALLIGAN, *supra* note 1, at 146 (establishing the congressional purpose for the amendments to The Economic Espionage Act).

[69] *See* Defend Trade Secret Act, 18 U.S.C. § 1836 (indicating that a civil action is available for the misappropriation of trade secrets related to products used in interstate and foreign commerce).

[70] *See* H.R REP. NO. 114-529, at 2 (2016) (declaring that the DTSA's definition of misappropriation is modeled after the UTSA); *see also* HALLIGAN, *supra* note 1, at 150 (suggesting that the existing body of precedent regarding the UTSA will apply to DTSA cases as the DTSA uses the same definition of trade secret).

[71] *See* Michael J. Songer, *The Defend Trade Secrets Act: What's the Big Deal?*, CROWELL MORING: LITIGATION FORECAST 2017 18 (2017) (listing the remedies available under the new law).

[72] *See* HALLIGAN, *supra* note 1, at 151 (suggesting that trade secret owners will no longer have to rely on the CFAA to gain access to federal courts).

in technological matters.[73] Additionally, federal courts use consistent discovery procedures that will provide increased efficiency, particularly in cases that involve theft by companies in different states or foreign countries.[74] Lastly, the DTSA will result in a more uniform application of trade secret law because there will not be different variations and applications of the law from state to state.[75]
In addition to access to federal courts, the DTSA has significant advantages over the UTSA.[76] The DTSA provides for enforcement authority against interstate and foreign actors, allowing prevailing parties to collect judgments for monetary damages and enforce court orders across state and national borders.[77] Furthermore, the DTSA provides *ex parte* seizure orders, allowing trade secret owners to seize stolen property before it is transmitted or transported out of the United States.[78] As the DTSA offers a federal cause of action, it may be unnecessary to invoke CFAA claim in order to bring trade secret cases into federal court.[79]

III. Facts

A. The Threat of the Malicious Insider

Businesses identify company insiders, including employees, consultants, lawyers and contractors, as some of their most dangerous

[73] *See* Songer, *supra* note 71, at 18 (indicating that the greatest impact of the DTSA will be providing companies with trade secret protection in federal courts).
[74] *See* Songer, *supra* note 71, at 18 (identifying consistent and efficient discovery procedures as a key advantage for litigating trade secret cases in federal courts).
[75] *See* Songer, *supra* note 71, at 18 (projecting that the DTSA will result in greater uniformity in trade secret cases).
[76] *See* HALLIGAN, *supra* note 1, at 148-49 (conveying the deficiencies of the Uniform Trade Secret Act).
[77] *See* HALLIGAN, *supra* note 1, at 148-49 (stating that the UTSA lacks enforcement authority against interstate and foreign actors). A significant problem under the UTSA is collecting judgments and enforcing court orders in other jurisdictions. *Id.* at 149.
[78] *See* HALLIGAN, *supra* note 1, at 151 (describing new ex parte provisions of the Defend Trade Secret Act). Provisions of the DTSA allow ex parte seizure orders to "preserve the evidence of trade secret misappropriation and to prevent the propagation or dissemination of the trade secrets that are the subject of the action. *Id.* at 150.
[79] *See* HALLIGAN, *supra* note 1, at 151 (declaring that claims under the CFAA are no longer necessary to bring a trade secret case into federal court).

threats to trade secrets and data security.[80] This can be attributed to the distinct knowledge that these individuals have of how a company produces, uses and stores trade secrets.[81] The prevalence of insider data and trade secret theft is heightened by developments in technology.[82] The use of smartphones, laptops and cloud-based technologies to transfer and store company data makes misappropriation easier for employees and more difficult for employers to detect.[83] Another significant factor in the rise of employee trade secret misappropriation is a change in employment norms.[84] Today, workers change jobs more frequently, averaging twelve times throughout their career.[85] As a result it is common for employees to face conflicts of loyalty in times of job transition.[86] A diminished sense of loyalty to employers, cou-

[80] *See* HALLIGAN, *supra* note 1, at 77 (indicating that U.S. companies report that the greatest risk to their proprietary data are employees). The number of occurrences and total value of misappropriated data by company insiders greatly exceeds that of outsiders. *Id. See also* THE CENTER FOR RESPONSIBLE ENTERPRISE AND TRADE & PRICEWATERHOUSECOOPERS LLP, THE ECONOMIC IMPACT OF TRADE SECRET THEFT: A FRAMEWORK FOR COMPANIES TO SAFEGUARD TRADE SECRETS AND MITIGATE POTENTIAL THREATS 11 (Feb. 2014) [hereinafter ECONOMIC IMPACT OF TRADE SECRET THEFT] (indicating that malicious insiders often work with other actors who can provide "money, other resources or ideological motivation" for the misuse of trade secrets and data).

[81] *See* ECONOMIC IMPACT OF TRADE SECRET THEFT, *supra* note 80, at 11 (recognizing that corporate insiders have special knowledge of company systems that make them a greater threat to trade secrets and other valuable information).

[82] *See* YEH, *supra* note 2 (maintaining that the theft of trade secrets increasingly involves computer technology and mobile communication devices).

[83] *See* YEH, *supra* note 2 (indicating that the use of mobile communication devices can make the theft of trade secrets more difficult to detect); *see* Cash, *supra* note 2, at 282 (stating that the use of mobile devices reduces security because these devices increase the amount of operating systems and endpoints that trade secret thieves can use to acquire data). In addition to mobile devices, increases in trade secret theft are attributed to the use of cloud-based technology to transfer large amounts of data. *Id.*

[84] *See* ECONOMIC IMPACT OF TRADE SECRET THEFT, *supra* note 80, at 11 (suggesting that a higher rate of lifetime job changes negatively impact an employee's loyalty to their employer).

[85] *See* Alison Doyle, *How Often Do People Change Jobs?*, THE BALANCE (May 1, 2017), *archived at* https://perma.cc/4F6J-CPHU (stipulating that the average person changes jobs about twelve times throughout their career).

[86] *See* HALLIGAN, *supra* note 1, at 78 (suggesting that when employees leave a firm to pursue another opportunity their "bonds of loyalty" to that firm are compromised).

pled with numerous tools that simplify the transfer of data, have increased the risk that employees pose to their company's information assets.[87]

B. Cases of Employee Trade Secret Theft under the CFAA

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.[88] demonstrates how some courts have developed an employer-friendly "agency theory" when applying the civil provisions of the CFAA to insider data misappropriation cases.[89] Shurgard became an international industry leader in storage facilities through use of sophisticated marketing plans and procedures.[90] Safeguard Storage, a direct competitor of Shurgard, approached one of Shurgard's Regional Development Managers, who possessed full access to Shurgard's business and expansion plans, and solicited him for employment.[91] While still employed with Shurgard, the employee emailed various Shurgard marketing documents to Safeguard without Shurgard's knowledge.[92]

Shurgard's claim under the CFAA alleged that (1) the former employee, as an agent of Safeguard, intentionally accessed a protected computer without authorization or by exceeding authorized access to obtain information, (2) that the employee knowingly accessed a protected computer without authorization or exceeded authorized access to further fraud, and (3) that he intentionally accessed a pro-

---

[87] *See* ECONOMIC IMPACT OF TRADE SECRET THEFT, *supra* note 80, at 11 (predicting that "cultural and technological factors" may increase the risk of insider trade secret misuse and theft in in the future).

[88] 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[89] *See id.* at 1125 (applying an agency theory to disestablish "authorization"); *see also* Liccardi, *supra* note 38, at 163 (establishing *Shurgard* as the critical case originating a broad interpretation of "without authorization" under the CFAA).

[90] *See Shurgard*, 119 F. Supp. 2d at 1122-23 (crediting Shurgard's growth to the expansion of their storage centers and explaining how strategic marketing systems furthered the company's expansion).

[91] *See id.* (implying that the defendant approached Shurgard's Regional Development Manager and offered him employment for the purpose of gaining Shurgard's trade secrets). "Because of his position with the plaintiff, Mr. Leeland had full access to the plaintiff's confidential business plans, expansion plans, and other trade secrets." *Id.*

[92] *See id.* (describing how the employee transferred trade secrets and proprietary information to Safeguard through e-mail).

tected computer without authorization and as a result caused damage.[93] The district court denied the defendant's motion to dismiss on all three provisions, reasoning that the employee's access to Shurgard's information had been unilaterally terminated by the employee's conduct.[94]

The court pointed to the Second Restatement of Agency, which states, "the authority of an agent, terminates if without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[95] The court reasoned that here, the former employee's authority to access Shurgard's computers and proprietary data ended when he became an agent of the other competing firm and emailed private documents to the competitor.[96] The court determined that because the employee had unilaterally terminated his agency relationship with Shurgard, his access to the company's proprietary information was "without authorization" under the CFAA.[97]

The Seventh Circuit adopted this "agency theory" in *International Airport Centers, L.L.C. v. Citrin*.[98] International Airport Centers (IAC), a real estate business, employed Citrin for the purpose of identifying acquisition targets for IAC and assisting with those acquisitions.[99] He was provided with a company laptop for the purpose of conducting his work.[100] Citrin eventually quit IAC to start his own real estate business, but before leaving deleted all of the information

[93] *See id.* at 1124-25 (indicating the provisions of the CFAA under which the plaintiff brought a claim); *see also* Liccardi, *supra* note 38, at 164 (stating the three provisions of the CFAA under which the plaintiff alleged violation).
[94] *See Shurgard*, 119 F. Supp. 2d at 1125-29 (concluding that the defendant's motion to dismiss was denied as the plaintiff properly stated a claim under the CFAA).
[95] *See id.* at 1125 (quoting Restatement (Second) of Agency § 112 (1958)).
[96] *See id.* at 1124 (explaining how the employee lost authorization when he acted against his employer's interests); *see also* Liccardi, *supra* note 38, at 164 (interpreting the court's reasoning to mean the employee's authorization terminated "the moment he acted against his employer for the defendant's benefit").
[97] *See Shurgard*, 119 F. Supp. 2d at 1124 (holding that accessing an employer's computer to transfer proprietary information to a competitor is acting without authorization).
[98] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (stating that the defendant's breach of his duty of loyalty terminated his agency relationship with International Airport Center).
[99] *See id.* at 419 (explaining Citrin's employment relationship with International Airport Centers).
[100] *See id.* (explaining that the purpose of IAC providing Citrin with a laptop was for so that he could record data for IAC's use).

he compiled for IAC from the laptop and deleted information that would reveal additional misconduct on his part.[101] Additionally, he loaded a secure-eraser onto the laptop to prevent the recovery of the data.[102] The *Citrin* court decided that Citrin's conduct was in violation of the CFAA as his authorization to access the computer was terminated when he engaged in conduct inconsistent with his employment and violated the terms of his employment contract.[103] Using the "agency theory", the court reasoned that when an employee violates their duty of loyalty, they terminate the authorization to use an employer's computer and access company data.[104] Although the *Citrin* court did not address the legislative intent of the CFAA, it confirmed that the CFAA is an appropriate cause of action for an employee-employer data misappropriation cases.[105]

The Ninth Circuit rejected the "agency theory" approach in *LVRC Holdings, LLC v. Brekka* and formed a narrow, "employee-friendly".[106] Brekka was hired as a marketing consultant for one of the residential treatment centers that LVRC operated.[107] While em-

[101] *See id.* (explaining how Citrin deleted the contents of the company laptop before returning it, depriving IAC of the information he acquired for business purposes as an employee).
[102] *See Citrin*, 440 F.3d at 419 (describing Citrin's use of a secure-eraser for the purpose of preventing recovery of the data on the laptop). Usually, deleting files on a computer does not destroy data, but merely removes the index entry and pointers, making the file appear that it is no longer available. *Id.* The secure-eraser program that Citrin used writes over the deleted file so that they are no longer recoverable to the owner. *Id.*
[103] *See id.* at 420 (explaining that Citrin's access rights to the laptop stemmed from his agency relationship with IAC, thus the access rights were terminated when he breached his duty of loyalty).
[104] *See id.* at 421 (inferring that acquiring adverse interests to IAC terminated the agency relationship between Citrin and IAC).
[105] *See* Pollaro, *supra* note 14, at *16 (explaining that the Seventh Circuit has made a policy judgment that the CFAA can encompass employer-employee claims).
[106] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (stating that the court is unpersuaded by the reasoning in *Citrin,* primarily because the court did not want to impose criminal liability for violating employer-placed limits); *see also* Pollaro, *supra* note 14, at *18 (stating that the Ninth Circuit and Supreme Court rejected the *Citrin* interpretation of authorization as it would "impose unexpected criminal burdens on defendants").
[107] *See Brekka*, 581 F.3d at 1129 (explaining Brekka's responsibilities as an employee of LVRC).

ployed by LVRC, Brekka owned two consulting businesses that referred clients to rehabilitation services.[108] During his time at LVRC Brekka was assigned log in credentials for an LVRC computer and the company website, which provided him with access to usage statistics, financial statements, and patient admission reports.[109] Brekka emailed a number of LVRC documents to his personal email as well as to his wife while he was employed.[110]

In analyzing the alleged CFAA violations, the court acknowledged that liability hinges on the meaning of "without authorization" and "exceeds authorized access".[111] The court was reluctant to apply the "agency theory" from *Citrin,* reasoning that the CFAA is primarily a criminal statute and that liability under the *Citrin* application would be determined by the speculated mental state of the employee.[112] The court used a textual approach to establish that in an employment context, "without authorization" refers to when an employee has not been granted permission to use a computer or when the employer rescinds authorization.[113] The court indicated that an employee "exceeds authorized access" when that employee has permission to access a computer, but uses the computer to access information that the employee is not entitled to use.[114] Since Brekka had permission to use the laptop and was required to use company data in furtherance of his work duties, the court found that he did not access data "without authorization" nor did he "exceed authorized access"

[108] *See id.* (stating that Brekka owned two consulting business in additional to the consulting work he conducted for LVRC).
[109] *See id.* (describing the extent of Brekka's access to LVRC's website data).
[110] *See id.* at 1129-30 (indicating that Brekka had emailed documents and reports to his and his wife's personal email accounts prior to leaving LVRC).
[111] *See id.* at 1132 (indicating that in order to prove a violation of 1030 (a)(2) and 1030 (a)(4), it must be shown that Brekka either acted without authorization or exceeding authorized access).
[112] *See Brekka*, 581 F.3d at 1134 (stating that the court is unpersuaded by the argument in *Citrin* that a breach of duty of loyalty terminates the employee relationship, and therefore terminates any access rights). "Applying this reasoning, Brekka would have acted 'without authorization' for the purposes of §§ 1030 (a)(2) and (4) once his mental state changed from loyal employee to disloyal competitor." *Id.*
[113] *See id.* at 1132, 1135 (indicating that court considered the plain language of the statute and the legislative intent in determining the meaning of authorization).
[114] *See id.* at 1133 (stating that under the plain language of the statute the term "exceeds authorized access" refers to using authorized access "to obtain and alter information in the computer that the person accessing it is not entitled so to obtain or alter").

under the CFAA when accessing and emailing company documents to himself and his wife.[115]

The Ninth Circuit expanded on its analysis of the CFAA in *United States v. Nosal*[116] (*Nosal I*).[117] The Ninth Circuit considered whether an employee exceeds their authorized access when transferring proprietary data from an employer's computer in violation of company policy.[118] Nosal was a director at a Korn/Ferry International.[119] Korn/Ferry was an executive search firm that utilized an internal database called "Searcher" to identify corporate candidates for their clients.[120] Korn/Ferry policy prohibited any disclosure of any information on the company's database.[121] Nosal resigned from his position at Korn/Ferry in 2004, and subsequently his access to the database was revoked.[122] After his resignation, Nosal, along with two other Korn/Ferry employees launched a competing executive search firm.[123] Nosal solicited former colleagues, which were still employed at Korn/Ferry, to use their login credentials to gather confidential data from "Searcher" and transfer that data to him.[124] Nosal was indicted on twenty criminal charges, including violations of the CFAA

[115] *See id.* at 1135 (holding that permission provided by LVRC for Brekka to access company data provided him with authorization under the meaning of the CFAA).
[116] 676 F.3d 854 (9th Cir. 2012) [hereinafter *Nosal I*].
[117] *See Nosal I*, 676 F.3d at 856-57 (analyzing the CFAA under the circumstance of employees disclosing data to a former employee in violation of their company's non-disclosure policy).
[118] *See id.* at 856 (indicating that Nosal was charged with a CFAA violation for aiding and abetting other Korn/Ferry employees in "exceeding their authorized access" after they provided him with company trade secrets or the purpose of starting a competing business).
[119] *See Nosal II*, 844 F.3d 1024, 1030 (9th Cir. 2016) (establishing the defendant's position at Korn/Ferry).
[120] *See id.* (describing the "Searcher" database as Korn/Ferry's "core asset"). The internal database used by Korn/Ferry included coded information on over one million corporate executives. *Id.* Employees used the database to compile "source lists" of potential candidates for their clients. *Id.*
[121] *See Nosal I*, 676 F.3d at 856 (stating that "Searcher" content was confidential), *see also Nosal II*, 844 F.3d at 1031 (stating that "Searcher" displayed a message indicating that the database was only to be used for Korn/Ferry business).
[122] *See Nosal II*, 844 F.3d at 1029 (indicating that Nosal's access to Korn/Ferry's computers was revoked following his resignation).
[123] *See Nosal I*, 676 F.3d at 856 (establishing that Nosal received proprietary data belonging to Korn/Ferry from employees who had valid login credentials).
[124] *See id.* (indicating that Nosal convinced former colleagues to provide him with proprietary information).

for aiding and abetting Korn/Ferry employees in exceeding authorized access in furtherance of fraud."[125]

The *Nosal I* court rejected the position that Korn/Ferry's employees exceeded authorized access when violating the company's policies.[126] The court established that the language of the CFAA is ambiguous and reasoned that if Congress wanted to impose liability for violations of company computer policies, the language would be explicit.[127] The court further reasoned that interpreting the phrase "exceeds authorized access" to apply to an authorized employee using a computer for unauthorized purposes would stray too far from the purpose of the computer hacking statute.[128]

The Ninth Circuit analyzed a different element of Nosal's conduct in *Nosal II*.[129] The second decision involving the data theft at Korn/Ferry considered whether Nosal acted "without authorization" when he accessed the company's database through his former assistant's login credentials.[130] The court reiterated that the Ninth Circuit's interpretation of "without authorization" was simply non-permissive use, and indicated that the analysis strictly focused on the concept of accessing a computer through a third party.[131] The court decided that Nosal's conduct fell within the scope of the CFAA as

[125] *See id.* (identifying that Nosal was indicted with twenty counts of criminal charges, including aiding and abetting in violations of the CFAA). Nosal's other charges included trade secret theft, mail fraud, and conspiracy. *Id.*

[126] *See id.* at 862-64 (declining to follow the broad interpretation of the First, Fifth, Seventh and Eleventh Circuits and adopting the narrow interpretation set out in *Brekka*).

[127] *See Nosal I*, 676 F.3d at 857 (suggesting that the broad interpretation would transform the CFAA from an anti-hacking statute into a misappropriation statute).

[128] *See id.* at 858 (rejecting the government's broad interpretation of the statute as an internet policing mandate and approving the defendant's argument that the CFAA imposes liability on outside hackers).

[129] *See Nosal II*, 844 F.3d at 1028 (reaffirming that the second decision addressed statutory provisions that were not at issue in the first Nosal case).

[130] *See id.* (stating that the court analyzed "without authorization" in regards to a former employee who accesses a computer through alternative means after their authorization has been revoked).

[131] *See id.* at 1033-34 (indicating that the meaning of "without authorization" under the CFAA was established in *Brekka*). "[A] person uses a computer 'without authorization' under [the CFAA] . . . . when the employer has rescinded permission to use the computer and the defendant uses the computer anyway." *Id.* at 1034.

Nosal acted with intent to defraud and did not have permission to access the database.[132] This was demonstrated by Nosal circumventing the revocation of his access to Korn/Ferry's "searcher" database by using his former assistant's credentials to access the company's data.[133] The *Nosal II* court utilized the technical interpretation to establish that once an employer revokes access to a computer, a former employee may not "sidestep the statute" by accessing the computer through a third party.[134] The court stressed that this decision was not based on password sharing or violating the company's internal policies but on former employees accessing trade secrets through a backdoor once their access to the company's computer had been revoked.[135]

IV. Analysis

A. Interpreting the CFAA in the Insider Misappropriation Context

The CFAA has long been used as tool to litigate the theft of proprietary information in federal court; however, it remains unclear whether the statute was intended to be used in that manner.[136] Since the CFAA's expansion to provide a civil action to protect private computers, the circuit courts have delivered conflicting opinions on whether Sections 1030(a)(2) and (a)(4) impose liability on the malicious insider who misuses company information.[137] The First, Fifth,

[132] *See id*. at 1031 (observing that Nosal and his co-conspirators continued to use "Searcher" after Korn/Ferry revoked their access to the computer system).
[133] *See id*. at 1028 (reasoning that Nosal and his co-conspirators access of the database after the revocation of their login credentials was] "without authorization," regardless of being effectuated by a user with permissive access).
[134] *See Nosal II*, 844 F.3d at 1028 (holding that accessing a computer through a third party with intent to defraud once access to that computer has been revoked violates the CFAA).
[135] *See id.* (emphasizing that the court's decision did not focus on the conduct as a violation of the company's computer use policy, but as a circumvention of the company's system of securing confidential data).
[136] *See* HALLIGAN, *supra* note 1, at 149 (declaring that the conflicting Circuit Court decisions that restrict the employment of the CFAA to cases of insider trade secret theft involving a computer).
[137] *See e.g.*, Ef Cultural Travel BV v. Explorica, Inc., 274 F.3d 578, 581 (1st Cir. 2001) (holding "that because of the broad confidentiality agreement appellants ac-

Seventh and Eleventh Circuits have held that an employee's authority to access a company's data is based his duty of loyalty as an agent of the company.[138] Under this broad interpretation, any disloyal use of a company computer would terminate the employee's agency relationship with the employer, and therefore, end the employee's authorization to use that computer.[139] This section will demonstrate that the broad application of the CFAA in cases of employee theft is incorrect.[140]

The broad interpretation of the CFAA imposes liability for conduct that is analogous to misappropriation of trade secrets, e.g., an employee downloading a client list from a company database and emailing that information to a competitor.[141] Additionally, the mis-

tions' 'exceeded authorized access,' and so [the court does] not reach the more general arguments made about statutory meaning, including whether use of a scraper alone renders access unauthorized."); *see also* Int'l Airport Centers L.L.C. v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006) (indicating the skewed interpretations of 1030(a)(1), (2), (4)); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1131 (9th Cir. 2009) (noting the differences of what a plaintiff must show to prove a defendant accessed an employer's computer "without authorization"); United States v. Rodriguez, 628 F.3d 1258, 1261 (11th Cir. 2010) (addressing the Computer Fraud and Abuse Act interpretation of what "exceeds authorized access"); United States v. John, 597 F.3d 263, 269 (5th Cir.2010) (recognizing the criminal liability that the statute places on defendants who "exceed authorized access" without permission).

[138] *See Citrin*, 440 F.3d at 420-21 (reaffirming that Citrin's breach of duty of loyalty terminated his authority to access his company laptop); *see EF Cultural*, 274 F.3d at 583 (holding that the access and use of an employer's proprietary information to form a competing company qualified as exceeding authorized access under the CFAA).

[139] *See* Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (stating that under agency principals, "Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal").

[140] *See* Liccardi, *supra* note 38, at 172 (asserting that "the CFAA applies to: (1) outsiders who never have authorization to access a business's computers, network, or trade secrets, (2) employee insiders who never possessed authorization to access the proprietary information, and (3) employee insiders who go beyond the parameters of their authorized access").

[141] *See* Liccardi, *supra* note 38, at 172 (suggesting that the CFAA is a powerful tool against the theft of proprietary information).

appropriated data in many CFAA cases is information that may qualify as trade secrets.[142] However, the CFAA lacks the evidentiary requirements of establishing the existence of a trade secret before imposing liability.[143] Under the DTSA, as well as state trade secret law, plaintiffs have the burden of showing that the information derived economic value from not being known, not readily ascertainable, and that the owner of the information took reasonable measures to maintain its secrecy.[144] The CFAA has no standard for qualifying misappropriated information, and merely requires the plaintiff to show that the information was taken from a "protected" computer without authorization or in a way that exceeded authorized access.[145] Consequently, applying the CFAA to cases of trade secret theft allows employers to litigate misappropriation in federal courts without the necessary safeguards of trade secret law.[146]

This is not to say that insider trade secret theft involving a computer never qualifies as a violation of the CFAA.[147] A textual analysis of Section 1030 supports the narrow interpretation, that an

[142] *See* Liccardi, *supra* note 38, at 172 (indicating that the CFAA protects data stored on a computer and used in business).
[143] *See* 18 U.S.C.. § 1030(a)(2) (2017) (asserting "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer").
[144] *See* 18 U.S.C. § 1839 (2016).

> The term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information . . . if . . .
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

Id.
[145] *See* 18 U.S.C. § 1030(a)(2) (2017) (defining "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer").
[146] *See Nosal I*, 676 F.3d 854, 863 (9th Cir. 2012) (concluding the CFAA's general purpose is to protect against hacking and not the misappropriation of trade secrets).
[147] *See Nosal II*, 844 F.3d 1024, 1028 (9th Cir. 2016) (holding that the act of an insider accessing trade secrets through the use of another employee's login credentials is a violation of § 1030 (a)(4)).

employee's authorization to access a computer is determined by the actual or technological permission granted by the employer.[148] The controversial phrase "exceeds authorized access" is defined under the CFAA as "access a computer without authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[149] Interpreted literally, this phrase refers a circumstance where an individual has general permission to use a computer but accesses files or data that the individual does not have permission to use.[150] The definition of "exceeds authorized access" indicates that Congress sought to punish acts of inside hacking rather than misappropriation, as the statute does not prohibit the unauthorized use or disclosure of data.[151] Based on common employment practices, an employer gives an employee authorization to use a computer when they give an employee permission to use it through physical and technological access.[152] Therefore, if an employee that has physical or technological access to certain data or proprietary information, they should not be liable under the CFAA for using that information for unauthorized purposes.[153] However, the narrow application of "exceeds authorized access" would impose liability on the inside hacker who obtains data to which they were not granted permission access.[154]

The broad application of the statute also poses significant policy concerns.[155] Although the CFAA has been amended to provide a

[148] *See id.* (explaining the narrow interpretation of the Computer Fraud and Abuse Act).
[149] *See* 18 U.S.C. § 1030(e)(6) (2017) (defining the phrase "exceeds authorization").
[150] *See Authorize*, MERRIAM-WEBSTER.COM (Feb. 2017), *archived at* https://perma.cc/L67Y-YKEL (defining "authorize" as "to endorse, empower, justify, or permit by or as if by some recognized or proper authority").
[151] *See* Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, et al., 390 F.Supp.2d 479, 499 (D. Md. 2005) (recognizing that the CFAA does not prohibit unauthorized use or disclosure of information).
[152] *See* Brenton, *supra* note 9, at 438 (indicating that a user name and password are considered technological access to a computer).
[153] *See* LVRC Holdings, L.L.C v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (asserting that exceeding authorized access refers to going beyond authorized limits).
[154] *See Nosal I*, 676 F.3d 854, 858 (9th Cir. 2012) (suggesting that "exceeds authorized access" should apply to individuals whose initial access to use a computer is authorized but who accesses unauthorized data).
[155] *See id.* at 857 (indicating that expanding the CFAA to encompass the misuse of company information would criminalize the conduct of many people unsuspecting people).

civil action against those who violate computers, the CFAA is primarily a criminal statute.[156] The broad interpretation, used by the First, Fifth, Seventh, and Eleventh circuits subjects employees to federal criminal liability based on an employer's claim that the employee breached their duty of loyalty to the company.[157] Under this approach, the mere violation of a company's computer policy, such as emailing company documents to a personal computer, would put the employee at risk of prosecution.[158] Relying on agency principles to determine authority would also allow an employee's perceived mental state to determine whether or not their actions were criminal.[159]

The *Nosal I* court correctly recognized that applying this computer crime statute to cases on employee data misappropriation would place unexpected burdens on employees and would overreach of the statute's authority.[160] Additionally, applying the CFAA to cases of employee data theft and misuse is inconsistent with the legislative purpose of expanding the statute.[161] The legislative history of the CFAA indicates that the central purpose of the "protected computer"

---

[156] *See* Kelsey T. Patterson, *Narrowing it Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 492-93 (describing the CFAA as a criminal statute enacted to address hacking).

[157] *See Brekka*, 581 F.3d at 1134 (emphasizing that even though the CFAA is being interpreted in a civil context, the interpretation would be applicable to criminal cases); *see also* Patterson, *supra* note 156, at 513 (stating the concern that an adoption of a broad CFAA interpretation would result in the criminalization of a wide range of computer activities).

[158] *See Nosal I*, 676 F.3d at 856 (indicating that a broad reading of the CFAA allows businesses to turn their computer-use and personnel policies into criminal law). The *Nosal I* court suggests that interpreting the term "exceeds authorized access" to mean any action of an employee that is adverse to their employer would allow employers threaten prosecution for any violation of company computer policy. *Id.* at 860.

[159] *See Brekka*, 581 F.3d at 1134 (reasoning that under the agency theory, a violation of §§1030(a)(2) and (4) would occur when an employee's mental state changed from loyal to disloyal).

[160] *See Nosal I*, 676 F.3d at 859 (recognizing that a broad interpretation of the CFAA would criminalize any unauthorized use of information stored on a computer); *see also Brekka*, 581 F.3d at 1134 (pointing to the Supreme Court's warning about using novel and surprising applications of statutes that are both civil and criminal). The Supreme Court has indicated that interpreting criminal statutes in novel ways places an "unexpected burden on defendants." *Id.*

[161] *See Nosal I*, 676 F.3d at 857 (recognizing that the broad interpretation of "exceeds authorized access" would transform the CFAA from anti-hacking statute into a misappropriation statute).

and civil action amendments were to protect privately owned computers from malicious outsiders, such as hackers and those seeking to trespass into computer systems and networks.[162] In *Shurgard*, the court found that an employee emailing a company's marketing strategies to a competitor amounted to unauthorized access to information in violation of the CFAA.[163] Similarly, in *Citrin*, the court held that an employee deleting compiled information from his business laptop also qualified as unauthorized access as this action was adverse to his employer's interests.[164] While these types of computer use may breach a duty of loyalty to an employer and cause significant damage, they do not amount to actions of trespass, such as hacking, that the statute was intended to prevent.[165] The expansive interpretation of the CFAA would broaden liability for the misuse of information held on a computer and likely expand the scope of the statute far beyond the intent of Congress.[166]

As computers have become the primary instrument for use and storage of data and trade secrets, it is logical that certain com-

[162] *See* 18 U.S.C. § 1030(e)(2) (1986) (defining "protected computer"); *see also* S. REP. NO. 101-544, at 1 (1990) (stating that the purpose of the amendments were to strengthen the laws against the intentional transfer of damaging computer programs and provide a civil remedy for certain computer crimes). The amendments of the CFAA followed senate hearings on advancements in malicious techniques that damage computer systems. *Id.* The hearings held by the Subcommittee on Technology and the Law that preceded the amendments focused on the serious threats to computer security posed by hacking, "viruses," and "worms." *Id.* at 2.

[163] *See* Shurgard Storage Ctrs, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1129 (W.D. Wash. 2000) (explaining Court's reasoning for applying the CFAA to defendant's actions). The Court reasoned the employee's conduct of emailing the employer's business plans to a competitor without the employer's knowledge constituted a violation of the CFAA. *Id.* at 1122-23.

[164] Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (discussing Court's reasoning for their finding that Citrin breached the CFAA). The Court described how Citrin deleted data from him business laptop before returning it to his employer after he was no longer an employee. *Id.* at 419.

[165] *See* S. REP. NO. 99-432, at 2487 (1986) (inferring that the statute seeks to prevent acts of intentional trespass into a computer); *see also* S. REP. NO. 101-544, at 5 (stating that the proposed amendment aims to deter malicious computer hacking).

[166] *See Nosal I*, 676 F.3d at 857 (suggesting that "exceeding authorized access" applies to individuals who have general access to a computer but use the computer to access unauthorized files or data). Limiting the definition of "exceeds authorized access" to an inside hacker maintains the legislative purpose of the CFAA as a hacking statute. *Id*.

puter abuse laws would be used to litigate the misuse of trade secrets.[167] Nevertheless, interpreting the CFAA to encompass employee misuse of an employer's data would be a significant overreach from the statute's purpose and also present considerable policy concerns.[168] Therefore, the narrow, application of the CFAA taken by the Second, Fourth, and Ninth Circuits is the appropriate interpretation of the statute.

A. Insider Misappropriation Under the DTSA

With the enactment of the Defend Trade Secrets Act, providing trade secret owners with direct access to federal courts, businesses should no longer use the CFAA to litigate cases of insider trade secret theft.[169] Whether or not the DTSA will be applicable to cases of employee misappropriation will hinge upon whether the type of data involved in these cases meet the requirements of establishing a trade secret and whether the conduct of the employee qualifies as misappropriation.[170] The DTSA adopts the trade secret qualifications of the UTSA, requiring that the information in question (1) derives economic value, (2) is not known to others that could benefit from the information, (3) is not readily ascertainable by proper means, (4) is subject to reasonable precautions to maintain its secrecy.[171] Under

[167] *See* Brenton, *supra* note 9, at 430 (indicating that storing trade secrets on computers potentially provides users with protection under computer misuse statutes).
[168] *See Nosal I*, 676 F.3d at 860 (stating that broad interpretation of the CFAA would turn common behavior into federal crimes simply because a computer is involved); *see also* LVRC Holdings, L.L.C v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (holding that it would be improper to interpret a criminal statute which would punish a defendant despite his lack of knowledge of the offense).
[169] *See* Brenton, *supra* note 9, at 442-43 (suggesting that the lack of proof requirements in the CFAA make the action inadequate cause of action for misappropriation of proprietary information).
[170] *See* Beckerman-Rodau, *supra* note 54, at 251 (indicating that a trade secret misappropriation action consists of two elements: establishing a trade secret and establishing misappropriation).
[171] *See* 18 U.S.C.A. § 1839 (setting forth a similar definition of trade secret as the UTSA).

> (3) [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques,

the DTSA a trade secret is misappropriated if it is acquired by improper means or disclosed by some who had reason to know that the trade secret was obtained through improper means.[172] By applying

> processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

Id.

[172] *See* 18 U.S.C.A. § 1839 (interpreting the definition for misappropriation).

> 5)[T]he term "misappropriation" means--
> (A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
> (B) disclosure or use of a trade secret of another without express or implied consent by a person who--
> (i) used improper means to acquire knowledge of the trade secret;
> (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was--
> (I) derived from or through a person who had used improper means to acquire the trade secret;
> (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or
> (iii) before a material change of the position of the person, knew or had reason to know that--
> (I) the trade secret was a trade secret; and
> (II) knowledge of the trade secret had been acquired by accident or mistake.

Id. See also 18 U.S.C.A. § 1839 (discussing the use of the term "improper means").

> 6) [T]he term 'improper means'-- (A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;

the DTSA to cases brought under Section 1030 (a)(2) and (a)(4) of the CFAA, the section will demonstrate how the prototypical civil CFAA claim can be successfully brought under the DTSA.

The source lists of corporate candidates involved in *Nosal I* and *Nosal II* would likely satisfy the trade secret requirements in order to bring a claim under the DTSA.[173] The DTSA requires that the information derives economic value, is not generally known, is not readily ascertainable by proper means, and that reasonable precautions were undertaken in order to maintain the secrecy of the information.[174] First, the source lists of corporate candidates derive economic value because a database of biographical and contact information for over one million candidates provides immense value to an executive search firm that profits from providing clients with qualified corporate candidates.[175] Secondly, the information contained in the database was not generally known by others who could benefit from it because the source lists were developed by Korn/Ferry employees by combining publicly available and private information.[176] Thirdly, the source lists were not readily ascertainable because Korn/Ferry's database was developed over fifteen years and

> and (B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition . . . .

Id.

[173] *See Nosal I*, 676 F.3d at 856 (identifying the misappropriated business information as source lists, names, and contact information derived from Korn/Ferry's confidential databases); *see also Nosal II*, 844 F.3d 1024, 1030 (9th Cir. 2016) (describing Searcher, Korn/Ferry's internal database, that consisted of personal data covering over one million corporate executives).

[174] *See* 18 U.S.C.A. § 1839 (defining "trade secret").

[175] *See Nosal II*, 844 F.3d at 1030 (characterizing Searcher as Korn/Ferry's "core asset" and central to the firm's work for clients, because the database allowed employees to run queries based on candidate's background and generate source lists of potential candidates); *see also* HALLIGAN, *supra* note 1, at 25-26 (affirming that plaintiffs in trade secret actions must show that the information in question must be in actual use within the plaintiff's business operations or that the information may be of value to the plaintiff, defendant, or third parties in the future).

[176] *See Nosal II*, 844 F.3d at 1042-43 (explaining rationale behind ruling against Nosal's argument due to the combination of public and private information as it pertained to the data).

not all of the data was available in public sources.[177] Finally, reasonable efforts were made to maintain the secrecy of this information because employees were required to use login credentials to access the database.[178] Employees were also informed that the database's contents were confidential.[179] Thus, it is likely that the stolen source lists in *Nosal I* and *Nosal II* meets the qualifications of a trade secret under the DTSA.[180]

Additionally, Nosal's conduct would likely qualify as misappropriation under the DTSA.[181] Under the DTSA misappropriation can occur through the breach of an obligation to maintain a trade secret in confidentiality or through acquiring a trade secret through "improper means".[182] The DTSA lists "breach or inducement of a breach of a duty to maintain secrecy" as an example of improper means.[183] Nosal obtained confidential information from his previous employer's database through former colleagues still employed with

[177] *See id.* at 1030-31 (discussing the development of the Searcher database). The data on Searcher was gathered from non-public sources such as personal connections and resumes, as well as public and quasi-public sources, such as LinkedIn. *Id*. The information on the database was compiled since the firm was established in 1995. *Id*. *See* HALLIGAN, *supra* note 1, at 26 (asserting that the plaintiff in a trade secret action must show that the information in question cannot be easily, independently developed by a third party in order to qualify as a trade secret).

[178] *See Nosal II*, 844 F.3d at 1030 (stating that employees were issued unique usernames and passwords in order to access "Searcher").

[179] *See id.* (explaining that new employees were required to sign confidentiality agreements which explicitly stated that the information generated from the database was confidential and intended for use only by Korn/Ferry employees); *see also* HALLIGAN, *supra* note 1, at 26-27 (outlining the requirement of plaintiffs to show that "reasonable measures under the circumstances" to secure the information's confidentiality and that the information was not disclosed outside the parameters of a confidential relationship).

[180] *See* HALLIGAN, *supra* note 1, at 26 (listing proprietary customer lists and proprietary information concerning customers as examples of trade secrets).

[181] *See Nosal I*, 676 F.3d 854, 856 (9th Cir. 2012) (describing Nosal's conduct of obtaining Korn/Ferry's source list through current employees after convincing them to join his competing business).

[182] *See* 18 U.S.C.A. § 1839 (defining "misappropriation" and listing methods of obtaining trade secrets through "improper means"); *see also* Beckerman-Rodau, *supra* note 54, at 251 (describing the two ways in which the misappropriation of a trade secret can occur).

[183] *See* 18 U.S.C.A. § 1839 (discussing the term "improper means" includes conduct involving a breach).

Korn/Ferry.[184] These actions would qualify as acquiring through improper means because Nosal induced former colleagues to breach their duty to maintain the source lists in confidentiality when he asked them to provide him with the source lists after his employment with Korn/Ferry had ended.[185] Furthermore, Nosal was once employed with Korn/Ferry and was aware that employees were required to keep the source lists confidential.[186] For these reasons it is likely that Nosal's acquisition of candidate lists from his former colleagues could be established as trade secret misappropriation.[187]

The marketing and expansion strategies that were acquired in *Shurgard* would likely meet the requirements of a trade secret under the DTSA as well.[188] First, these procedures derived independent economic value because Shurgard attributed their company's success on their system of identifying and entering into high-barrier-to-entry markets.[189] If other storage facility companies became aware of Shurgard's strategies, these competing firms would be able to enter potential new markets before Shurgard causing Shurgard to lose its competitive advantage.[190] Secondly, the plans were not generally known by others who could benefit from them because they were derived internally and kept confidential.[191] Thirdly, the marketing procedures were not readily ascertainable because they were sophisticated systems developed over twenty-five years through the investment of significant resources and the combined skills of

---

[184] *See Nosal I*, 676 F.3d at 856 (stating that Korn/Ferry employees had authorization to access the "Searcher" database, but the company had a policy of keeping the data confidential).
[185] *See id.* (stating that the employees provided Nosal with the information because he offered them employment with his competing business).
[186] *See id.* (inferring that Nosal was aware of the confidentiality policy because he used to work as an executive at Korn/Ferry).
[187] *See* Beckerman-Rodau, *supra* note 54, at 252-53 (asserting that trade secret law protects against otherwise legal conduct that defies "commercial reasonableness").
[188] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000) (describing the employer's confidential business and expansion plans as trade secrets).
[189] *See id.* at 1122-23 (indicating that Shurgard's success was attributed to entering "high barrier to entry markets" through the sophisticated system of identifying development sites, marketing plans and evaluating return on investment).
[190] *See id.* at 1123 (suggesting that Shurgard's expansion plans and systems of marketing are what gave the company a competitive advantage in the storage industry).
[191] *See id.* (describing how Shurgard created marketing teams to carry out its strategies in new markets).

Shurgard's marketing professionals.[192] Finally, Shurgard took reasonable measures to maintain their business plans and strategies in secrecy because they were only known and available to members of the marketing team at Shurgard and designated the information as confidential.[193] Based on these factors it is likely that Shurgard's marketing systems would satisfy the trade secret requirements under the DTSA.[194]

The conduct of both the Shurgard insider and as well as the competing storage company would likely qualify as misappropriation.[195] The DTSA imposes liability on individuals who breach an agreement or an obligation to maintain the confidentiality of a trade secret.[196] While employed with Shurgard, a Regional Development Manager disclosed Shurgard's marketing procedures to a competing company.[197] This conduct would qualify as misappropriation because the manager was violating his duty to keep this information secret when he emailed the procedures to a competing firm.[198]

---

[192] *See id.* (establishing that Shurgard dedicated a significant amount of resources to the evaluation of new markets and put together teams to implement their strategies).

[193] *See id.* (indicating that the information that Leland provided to Shurgard's competitor was confidential and that the information was provided to the competitor without Shurgard's approval).

[194] *See* HALLIGAN, *supra* note 1, at 262 (listing competitive analyses, market analyses, and marketing plans as examples of trade secrets).

[195] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000) (describing interaction between Leland and Safeguard Self Storage). Safeguard storage approached Leland, a Regional Development Manager at Shurgard, and offered him employment with Safeguard. *Id.*

[196] S*ee* 18 U.S.C.A. § 1839 (elaborating on the term "misappropriation").

> [M]isappropriation means . . . . [a] disclosure or use of a trade secret of another without express or implied consent by a person who . . . . at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was. . . . acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret . . . .

Id.

[197] *See Shurgard*, 119 F. Supp. 2d at 1123 (stating that Leland provided Safeguard with Shurgard's confidential marketing plans shortly after being solicited for employment).

[198] *See* Beckerman-Rodau, *supra* note 54, at 251 (stating that the breach of an agreement to keep a trade secret confidential qualifies as misappropriation).

Moreover, misappropriation occurs when a third party acquires a trade secret through improper means.[199] Safeguard Self Storage offered Shurgard's Regional Development Manager employment with their company and subsequently obtained emails from that manager containing confidential information regarding Shurgard's marketing plans.[200] Because Safeguard induced the manager to breach of his duty to maintain the information in secrecy, this conduct would qualify as misappropriation under the DTSA.[201] These cases demonstrate that conduct formerly litigated under the CFAA is likely to be actionable under the DTSA.

The DTSA provides a solution to the over-extension of the CFAA in cases of insider misappropriation.[202] Litigating insider trade secret misappropriation under the DTSA avoids the policy issues posed by the CFAA.[203] The DTSA provides employers with access to federal courts, but maintains the procedural safeguards that the CFAA is missing.[204] By placing evidentiary requirements on the accessed information, the DTSA preserves the balance between the rights of employers and employees.[205] Furthermore, the safeguards of trade secret law, such as the economic value and secrecy require-

[199] *See* 18 U.S.C. § 1839(5) (2016) (defining misappropriation as the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means . . . .").
[200] *See Shurgard*, 119 F. Supp. 2d at 1123 (describing the defendant's conduct in the late 1990s).
[201] S*ee* 18 U.S.C. § 1839(6) (2016) (stating that "improper means" includes a third party inducing another to breach a duty to maintain a trade secret in secrecy); *see also* Beckerman-Rodau, *supra* note 54, at 251 (suggesting that otherwise legal conduct could be deemed improper conduct under trade secret law).
[202] *See* Songer, *supra* note 71, at 18 (highlighting that the DTSA will provide trade secret owners with direct access to federal courts); *see also* HALLIGAN, *supra* note 1, at 151 (indicating that trade secret owners will not need the CFAA in order to bring claims in federal court for the misappropriation of trade secrets).
[203] *See* Brenton, *supra* note 9, at 441 (suggesting that the litigating of trade secret misappropriation under the CFAA undermines the policies trade secret law, such as the focus on the character of the information in question before the conduct of the accused).
[204] *See* HALLIGAN, *supra* note 1, at 150 (indicating that the DTSA will provide victims of trade secret theft with access to federal courts while maintaining the definition of trade secret set out in the UTSA).
[205] *See* Brenton, *supra* note 9, at 441 (asserting that the requirement of establishing a trade secret helps maintain a balance between the property rights of an employer and the commercial right of the employee).

ment, reduce the concern of imposing liability on common or everyday conduct in the workplace.[206] The CFAA does not provide complete protection against employee trade secret theft because of the inconsistent holdings on the extent to which it imposes liability on company insiders.[207] However, the DTSA affords employers access to federal courts without reliance on an ambiguous and indefinite computer law.[208] Unlike the CFAA, the DTSA's clear purpose is to impose liability on any individual who misuses proprietary information, regardless of whether that individual has been given access to the information.[209] Therefore, the enactment of the DTSA eliminates the need to litigate trade secret misappropriation under the CFAA.

V. Conclusion

As the future of the Computer Fraud and Abuse Act is uncertain, it does not provide companies with an adequate action against employees that steal or misuse their employer's valuable information assets. The broad interpretation of the CFAA, used by First, Fifth, Seventh and Eleventh Circuits, has the potential to impose criminal and civil liability for innocuous behavior, such a violation of a company computer policy. The broad interpretation disproportionately favors employer rights by not placing any qualification of confidentiality or value of the accessed business information. For these reasons, it is likely that the narrow interpretation, use by Second, Fourth,

---

[206] *See Nosal I*, 676 F.3d 854, 856-57 (9th Cir. 2012) (indicating that a broad reading of the CFAA allows businesses to turn their computer-use and personnel policies into criminal law); *see also* Brenton, *supra* note 9, at 449 (indicating that trade secret law only protects information that meets the strict requirements of a trade secret and therefore, allows employees to utilize knowledge and skills in new jobs without fear of liability); *see also* Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1032 (N.D. Ill. 2008) (stating that a broad application of the CFAA runs the risk of criminalizing of a wide range of computer activities common in the workplace).

[207] *See* HALLIGAN, *supra* note 1, at 149 (asserting that the conflicting decisions surrounding the CFAA indicates that the law is not a satisfactory tool to litigate in federal court).

[208] *See* HALLIGAN, *supra* note 1, at 151 (suggesting that the DTSA will allow companies to access federal courts without reliance on CFAA claims or diversity jurisdiction).

[209] *See* HALLIGAN, *supra* note 1, at 150 (explaining that the DTSA uses the same definitions of trade secret and misappropriation as the UTSA, and inferring that the same focus on the character of the information will apply in DTSA cases).

and Ninth Circuits, will ultimately be taken by the Supreme Court or implemented through amendments to the law. As the CFAA does not provide employers with an adequate action for cases of trade secret misappropriation, the Defend Trade Secret Act provides an effective alternative. The law allows companies to access federal courts, while maintaining the evidentiary safeguards of trade secret law. Accordingly, insider misappropriation actions should be brought exclusively under the DTSA.