Journal of Legislation

Volume 44 | Issue 2 Article 6

4-20-2018

The Pragmatic Disappointment of State Preemption: The 2016 Defend Trade Secrets Act and Its Failure to Protect Employee Whistleblowers from Federal Computer Crime Law

Kristine Craig

THE PRAGMATIC DISAPPOINTMENT OF STATE PREEMPTION: THE 2016 DEFEND TRADE SECRETS ACT AND ITS FAILURE TO PROTECT EMPLOYEE WHISTLEBLOWERS FROM FEDERAL COMPUTER CRIME LAW

Kristine Craig†

INTRODUCTION

Since the first reported trade secret case, *Vickery v. Welch*, which was decided by the Supreme Court in 1837, trade secret law and enforcement has existed exclusively in state law statutes and common law doctrines.[1] Yet, on May 16, 2016, over 150 years since *Vickery*, President Barack Obama signed the Defend Trade Secrets Act ("DTSA") into law as an amendment to the Economic Espionage Act ("EEA").[2] In addition to providing a federal claim of relief for misappropriation, the text of the DTSA contains a provision that provides immunity for whistleblowers from trade secret misappropriation liability. However, the immunity provision is not sufficient on its face for the protection of whistleblowers as intended by the DTSA's authors. The provision does nothing to define how far whistleblowers can go in accessing incriminating information, which is integral to encouraging disclosure and assuring whistleblowers of immunity under the DTSA. Furthermore, the immunity provision does not extinguish liability for violation of computer access laws, which directly govern the scope of authorized access to employer data or information.

Because the definition of lawful computer access under the federal Computer Fraud and Abuse Act ("CFAA") is fairly limited in scope, the DTSA provides a false sense of security to whistleblowers who are reassured by a broad grant of immunity, but also subtly warned about an unspecified number of related laws with enormous potential for liability. By contrast, state computer access laws, such as the California Comprehensive Computer Data Access and Fraud Act ("CDAFA") and N.Y. Penal Law § 156.00, provide broader protections for whistleblowers. These statutes are in alignment with the purpose and history of DTSA because they allocate liability only

† Candidate for Juris Doctor, University of Notre Dame Law School, 2019; B.A. Political Science and Economics, University of California, Davis, 2016. I would like to extend my sincerest thanks to Professor Stephen Yelderman (University of Notre Dame Law School) for his guidance and direction throughout the writing process, and the editors of the Journal of Legislation, especially James Britton. I would also like to thank my mom, Ketty, sister Juliana, and my dearest friends.

1 Harry First, *Trade Secrets and Antitrust Law*, 910 (N.Y.U Law & Econ. Working Paper No. 255, 2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1765244.

2 Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

where whistleblowers access material in malicious and intentional ways, such as hacking.

This Note is divided into six parts. After assessing the emergence and features of the DTSA in Parts I and II, this paper will explore the Congressional intent of DTSA immunity in Part III. Next, Part IV discusses the practical problems with the immunity provision and is divided into two sections. Section 1 discusses whistleblower protection under state and federal computer access statutes, and Section 2 discusses emerging case law on the functionality of the immunity provision in litigation. Part V considers solutions to practical problems with the provision, and Part VI concludes the main proposals in this Note.

I. EMERGENCE OF THE DTSA

In the 1990s, rapidly advancing technology solidified confidence in the patent law system as an attractive and agreeable option for protecting commercially valuable products.[3] Monopolistic property rights granted by the patent law system were regarded as a worthy benefit in exchange for public disclosure of the claimed invention. Inventors' exclusive property rights under patent law allowed them to enter licensing agreements in return for royalties, or acquire the sole profits from the sale of their invention. Due to the fact that the subject matter of inventions during the 1990s was often useful and applicable to a wide range of industries (i.e. computers, software, DVD/CDs, text messaging), inventions proved to be enormously profitable for inventors, and also useful to the public and essential to improving quality of life.

The patent system's requirement of eventual public disclosure came with clear societal advantages, the most obvious example in the case of medicine and drug advances. However, nearly two decades after the technology boom of the 1990s, technological developments slowed and became more refined.[4] Made possible by development of the modern computer, expansive industries formed around "app" development and computer programming, highlighting the value of computer technology to customize digital devices for consumers.[5] As a fundamental building block, the computer was a centerpiece of innovation upon which further technology focused, and a main contributor to the refinement of innovation over time. Because a vast amount of technological innovation today no longer deals with fundamentals, I propose that it has become oriented towards consumers with disposable income. For this reason, benefits to society from public disclosure of new technology became marginally lower over time. The marginal benefit to the public from *disclosure* of "the useful arts" declined, and the *secrecy* of "the useful arts," supported by trade secret protection, became fundamentally valuable to companies in the form of comparative advantages and competition in the market via product advancement.

3 U.S. Patent Statistics Chart Calendar Years 1963–2015, U.S. PAT. & TRADEMARK OFF., https://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.htm (last visited Apr. 14, 2018).

4 *See* David Rotman, *Tech Slowdown Threatens the American Dream*, MIT TECH. REV. (Apr. 6, 2016), https://www.technologyreview.com/s/601199/tech-slowdown-threatens-the-american-dream/.

5 Catherine Clifford, *By 2017, the App Market Will Be a $77 Billion Industry (Infographic)*, ENTREPRENEUR (Aug. 26, 2014), https://www.entrepreneur.com/article/236832.

Furthermore, as confirmed by a boom in litigation, scholarly attention, and legislation, the benefit of trade secrets to companies is clear.[6] As David S. Almeling, Counsel at O'Melveny & Myers LLP, hypothesizes: a mobile workforce, the rising value of intellectual property, and trade secret's flexible definition fueled the ascent of trade secrets in recent years.[7] I propose that these reasons, combined with the greater marginal value companies gain from concealing their information, has lessened attraction to the patent law system and its disclosure requirement. Inventors have turned towards trade secret law instead.

Additionally, the availability of legal protection during the early research and development stages of a product—that trade secret law exclusively provides—makes it a comparatively better option than patent law to companies.[8] The popularity of trade secrets that flows from the availability of protection during the research and development phase is clear, especially when considering the fragility of inventive activity and critical early months of start-ups and venture capitalist incubation initiatives. During these periods, ideas and early inventive activity are hot commodities, with great potential for misappropriation in tight-knit communities such as Silicon Valley and the San Francisco Bay Area.[9] This change in the innovative landscape after the 1990s paved the way for federal recognition of trade secrets through the DTSA.

II. FEATURES OF THE DTSA

The story of the DTSA began with the passage of the Economic Espionage Act ("EEA") in 1996.[10] The EEA sought to increase protection and provide remedies for theft of trade secrets by foreign governments and agents. However, because the EEA did not contain a federal private cause of action, increasing enforcement and protection required action of the federal government to initiate a lawsuit. Given the enormous amount of prosecutorial discretion within the U.S. Attorney's Office, trade secret misappropriation cases could easily be subordinated to those of corporate abuse, fraud, or tax avoidance. Yet, President Obama's adoption of the DTSA in 2016 marked the advent of the first federal codification of trade secret law and created a federal cause of action for trade secret misappropriation.[11]

6 David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L. J. 1091 (2012), https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.bing.com/&httpsredir=1&art-icle =1958&context=btlj

7 *Id.* at 1091.

8 Georgi Paskalev & Benoit Yelle, *Trade Secrets Made Practical - Pt. 2*, MONDAQ (Sept. 15, 2017), http://www.mondaq.com/canada/x/630854/Trade+Secrets/Trade+Secrets+Made+Practical+Part+2 (explaining the benefits that trade secret law provided, in comparison to patent, particularly regarding the maturity of the invention or idea).

9 Peter Holley, *Tech Titans, Trade Secrets and Alleged Conspiracy: Inside the Waymo-Uber Battle Captivating Silicon Valley*, WASH. POST (Feb. 4, 2018), https://www.washingtonpost.com/news/innovations/wp/2018/02/04/tech-titans-trade-secrets-and-alleged-conspiracy-inside-the-waymo-uber-battle-captivating-silicon-valley/?utm_term=.a5c6e52a74b0 (referring to Silicon Valley as "the wildly aspirational, incestuous, high-tech valley").

10 Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified as 18 U.S.C. § 1831 (2012)).

11 Defend Trade Secrets Act of 2016, 18 U.S.C.S § 1832 et seq. (LEXIS through Pub. L. No. 115-137).

Trade secrets, under U.S. law, are established by a three-part test: (1) the information must be non–public; (2) reasonable measures are taken to protect that information; and (3) the underlying information derives independent economic value from not being publicly known.[12] Under the meaning of Defend Trade Secrets Act:

> the 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, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.[13]

Further, trade secret misappropriation is defined as an:

> (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 . . . used 1) improper means to acquire it, 2) knew or should've know that it was derived from a person who used improper means or 3) knew that the trade secret was a trade secret and it had been acquired by mistake before the person's position changed.[14]

With the creation of a federal private cause of action in the DTSA, Congress authorized those who were harmed by a misappropriation to take legal action in federal court and protect themselves. Language in the statute explains that courts may order injunctions against violators to prevent "actual or threatened misappropriation," so long as the order does not "otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[15] Moreover,

> [e]xcept as provided in section 1833(b), this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee

12 *See* Mark L. Krotoski, *Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases*, 57 U.S. ATT'YS BULL. 2 (2009); 18 U.S.C.S § 1839(3); *Id.* § 1839(3)(A); *Id.* § 1839(3)(B).

13 18 U.S.C.S § 1839(3) (LexisNexis through Pub. L. No. 115-137).

14 *Id.* § 1839(5).

15 *Id.* § 1836(b)(3)(A)(i).

> under section 552 of title 5 (commonly known as the Freedom of Information Act).[16]

This language makes clear that the statute suggests no preemption of state law through the Supremacy Clause for trade secret misappropriation claims. Rather, state and federal law coexist.

In addition to a federal cause of action, Congress carved out an exception to trade secret protection and enforcement against whistleblowers under the DTSA, requiring that

> [a]n individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that (A) is made (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; (ii) solely for the purpose of reporting or investigating a suspected violation of law.[17]

Additionally, immunity would apply for disclosures made in a complaint or other filing, but only if "made under seal."[18] Importantly, a rule of construction was established, stating: "Except as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means."[19]

The issue of whistleblower immunity arises often when the government enlists employee assistance in revealing confidential information to attorneys or government investigators in good faith. During lawsuits initiated by the federal government against employers, which are made possible by the help of employees, the disclosure of an employer's trade secret in the process is certainly possible. In exchange for efforts to disclose information to the government (containing either an employer's misappropriation of another company's trade secret or an employer's own trade secrets), the DTSA grants mandatory immunity to employees from retaliatory trade secret misappropriation claims by employers. The most aggressive form of lawsuits are called "*qui tam*" actions, which are filed by an individual on behalf of the government, and are empowered by Section 3730(b) of the False Claims Act ("FCA").[20] Recognizing the importance of a whistleblower's function in society, "Section 3730(b)(2) provides that a *qui tam* complaint must be filed with the court under seal. The complaint and a written disclosure of all the relevant information

16 *Id.* § 1838.

17 *Id.* § 1833(b)(1).

18 *Id.*

19 *Id.* § 1833(b)(5).

20 U.S. DEP'T OF JUSTICE, THE FALSE CLAIMS ACT: A PRIMER 2–3 (2011), *available at* https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf.

known to the relator must be served on the U.S. Attorney for the judicial district where the *qui tam* was filed and on the Attorney General of the United States."[21]

This is consistent with the scheme Congress imagined when enacting the DTSA immunity provision. As reflected in the DTSA text, for the disclosure to qualify for immunity, it must be made "(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law."[22] Congress has acknowledged the important function that employees can play in revealing illegal conduct for over a century, most notably in passing the FCA during the Civil War.[23] However, throughout history, limits placed on the scope of employee activity have been important to the functionality of whistleblowing regimes. Some scholars and legal professionals, such as Robert B. Milligan, suggest upon analyzing Sarbanes-Oxley whistleblowing cases that "special attention should be given to the employee's specific potential whistleblower claims as certain claims . . . may provide *protection* to take [c]ompany documents (or at a minimum divulge [c]ompany information), particularly if such information is shared with the SEC."[24]

Historically, Congressional focus in *qui tam* actions has been on protecting the trade secret itself, and much less on protecting those who assist the government by disclosing it. Congress made clear, prior to the DTSA, that protective orders on trade secrets must be in place during criminal cases in each stage of the prosecution. Yet these protective orders failed to address employee concerns directly, despite the enormous value that promoting useful disclosures may contribute. Instead of aiming to strike a balance in light of the need for whistleblower assistance in disclosing fraudulent practices, legislative efforts were concentrated more on protecting trade secret confidentiality. Because of the risk that turning over trade secret information to the federal government would result in retaliation by their employer, employee whistleblowers were uneasy about assisting the government in *qui tam* lawsuits at all. Until the DTSA, employee whistleblowers continued to face strong concerns about personal legal consequences.

Overall, the DTSA strikes a balance between protecting the legitimate ownership of company trade secrets by providing a federal cause of action for relief, while at the same time enhancing law enforcement activities by protecting whistleblowers. Especially because the inherent value of a trade secret stems from the fact that they are, by definition, kept secret, potentially significant losses are at risk in the furtherance of any lawsuit. Yet despite the risk that trade secrets may be exposed without revealing illegal conduct, Congress decided that the public and private benefits from exposing potential fraud in *qui tam* actions were *greater* than potential losses. Furthermore, because enlisting the assistance of employees as quasi-public actors is sometimes the only way to gather information regarding potential abuse or

21 *Id.*

22 18 U.S.C.S § 1833 (b)(1) (LexisNexis through Pub. L. No. 115-137).

23 Joel D Hesch. *Breaking the Siege: Restoring Equity and Statutory Intent to the Process of Determining Qui Tam Relator Awards Under the False Claims Act*, 29 T. M. COOLEY L. REV. 217, 283 (2012).

24 Robert B. Milligan, *An Employee Is Stealing Company Documents…That Can't Be Protected Activity, Right?*, TRADING SECRETS (July 3, 2013), https://www.tradesecretslaw.com/2013/07/articles/ trade-secrets/an-employee-is-stealing-company-documentsthat-cant-be-protected-activity-right/ (emphasis added).

fraud by employers, the functionality of this immunity clause is key to carrying out the DTSA authors' intent.

III. CONGRESSIONAL INTENT

Whistleblowers as quasi-public actors are essential playing pieces in the broader scheme of law enforcement and serve as important checks on corporations with concentrated power. As Senate Judiciary Committee Chairman Charles Grassley, a co-sponsor of the whistleblower immunity provision, explained:

> Too often, individuals who come forward to report wrongdoing in the workplace are punished for simply telling the truth. The amendment I championed with Senator Leahy ensures that these whistleblowers won't be slapped with allegations of trade secret theft when responsibly exposing misconduct. It's another way we can prevent retaliation and even encourage people to speak out when they witness violations of the law.[25]

Fellow co-sponsor, Senator Leahy, added, "Whistleblowers serve an essential role in ensuring accountability. It is important that whistleblowers have strong and effective avenues to come forward without fear of intimidation or retaliation. The amendment I authored with Senator Grassley takes another important step in our bipartisan efforts to protect whistleblowers and promote accountability."[26]

The immunity provision was created through a bipartisan amendment to the DTSA and co-authored by Senate Judiciary Committee Chairman Senator Charles Grassley, R-Iowa, and Senator Patrick Leahy, D-Vt. In the abstract, the purpose of immunity under 18 U.S.C. § 1833 is to prevent companies from using the threat of a trade secret suit or a breach of a non-disclosure agreement to stifle legitimate whistleblowing.[27] It also serves to mitigate concerns of whistleblowers and provide a clear message that motivates employees to come forward with essential information to assist the federal government in the furtherance of a *qui tam* law suit.

Notably, the bipartisan support for the whistleblowing amendment speaks to the agreement among the parties on the value of immunity for legitimate whistleblowing activity. At an executive business meeting of the full Senate Judiciary Committee, on January 28, 2016, the bill's Democratic Co-Sponsor, Patrick Leahy, thanked Chairman Grassley for "working with [him] on an amendment to provide needed protections for whistleblowers who share confidential information in the course of reporting suspected illegal activity to law enforcement or when filing a lawsuit,

25 Press Release, U.S. Senator Patrick Leahy, Leahy-Grassley Amendment to Protect Whistleblowers Earns Unanimous Support in Judiciary Committee (Jan. 28, 2016), *available at* https://www.leahy.senate.gov/press/leahy-grassley-amendment-to-protect-whistleblowers_earns-unanimous-support-in-judiciary-committee.

26 *Id*. (emphasis added).

27 Randall E. Kahnke et al., *Key Trade Secret Developments Of 2017: Part 1*, LAW 360 (Dec. 21, 2017), https://www.law360.com/articles/996861/key-trade-secret-developments-of-2017-part-1.

provided they do so under seal."[28] Leahy added that "[o]ur amendment is supported by the Government Accountability Project and the Project on Government Oversight ("POGO"), and I look forward to its adoption."[29]

IV. PRACTICAL PROBLEMS WITH THE DTSA'S FUNCTIONALITY

In addition to a federal cause of action and immunity provision, the DTSA mandates notice for employees in their employment contract of immunity from retaliation in the form of threats of lawsuits for state or federal trade secret misappropriation. In 18 U.S.C. § 1833(b)(1) and § 1833(b)(5), the DTSA states required text to be included in all contracts:

> An individual shall not be held criminally or civilly liable under *any Federal or State trade secret law* for the disclosure of a trade secret that (A) is made (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.[30]

Section (b)(3) requires notice of this immunity to be given in an employee's contract and "applies only to contracts and agreements entered into after May 11, 2016, the effective date of DTSA."[31]

Many politicians, including Senator Dianne Feinstein, have emphasized this as the highlight of the legislation.[32] However, the text of the statute is much more complex than it first appears. Section (b)(5) reflects that "[e]xcept as expressly provided for under this subsection, *nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means*."[33] A clear interpretation of Section (b)(5) reflects that the immunity provided in the notice requirement grants protection solely from claims under federal and state *trade secret* law. It does not provide protection to actions taken by the whistleblower employee, such as a violation of computer access or computer crime laws, which directly govern the scope of authorized access to employer data or information. Specifically, the DTSA does not provide further guidance on the domain of authorized access or scope of this whistleblower immunity, and federal law is less than clear.

28 Statement of Senator Patrick Leahy, U.S. COMM. JUDICIARY (Jan. 28, 2016), https://www.judiciary.senate.gov/download/1-28-16-leahy-statement.

29 *Id.*

30 18 U.S.C.S. § 1833(b)(1) (LexisNexis through Pub. L. No. 115-137).

31 26 MILGRIM ON TRADE SECRETS § 6.02 (LexisNexis through Dec. 2017).

32 James Pooley, *What You Need to Know About the Amended Defend Trade Secrets Act*, PATENTLYO (Jan. 31, 2016), https://patentlyo.com/patent/2016/01/amended-defend-secrets.html.

33 18 U.S.C.S § 1833(b)(5) (LexisNexis through Pub. L. No. 115-137).

Persistent circuit splits on federal computer crime statutes such as the Computer Fraud and Abuse Act ("CFAA"), which governs information an employee can access or actions an employee can take to uncover fraud, still exist. The circuit splits, considered in combination with the low thresholds for liability under the CFAA, complicate the picture and compromise the functionality of DTSA immunity. Furthermore, the mandatory notice requirement in an employee's employment contract also fails to disclose what activities qualify for this immunity and what activities do not. Derivative reliance on the absence of defined criminal activity by statutes with unclear authority puts this supposed "notice" of immunity on shaky footing. Without defining the scope of lawful activities for a potential employee whistleblower, the immunity provision of the DTSA is an attempt at best to encourage employee whistleblowers to come forward. The failure of the DTSA to fully protect whistleblowers from aggressive and restrictive forms of computer access laws is an essential impediment to safe exercise of whistleblowing under the DTSA's immunity. Because of this, *qui tam* lawsuits that rely on the assistance of employees to reveal fraudulent activity to the public and keep companies accountable are likely to be fatally undermined.

Despite the ambiguity latent in the statute, room for salvation certainly exists. Although the trade secret misappropriation provision does not preempt state law, the whistleblower immunity provision does result in a narrow preemption of state law. This is evinced by the text of Section (b)(1), which requires notice to employees and grants immunity "under any Federal *or State* trade secret law," thus sweeping in and including immunity under state trade secret law and state law governing non-disclosure agreements. Practically, this means that even when asserting a cause of action against an employee whistleblower under state law, an immunity provision for whistleblowers exists. It remains necessary to show evidence of prerequisites to immunity: namely that the disclosure is 1) made in confidence to a federal, state, or local government official, or to an attorney, and is solely for the purpose of reporting or investigating a suspected violation of law, or (2) under seal in a complaint for a lawsuit.[34] Once established, immunity from state trade secret misappropriation claims is in place, and therefore a retaliating employer may look to assert violations of computer access laws instead.

Every state has their own version of the federal CFAA, or some form of criminal computer act,[35] with clearer guidance than federal law on the domain of access and enhanced protection for whistleblowers. Given that the whistleblower immunity provision of DTSA preempts state law and adds an immunity requirement, this combination of legal claims (immunity by the DTSA and state computer access law) is an ideal relationship compared with federal computer access law. Together, these statutes operate practically to carry out the intent of Congress and ensure full functionality of the incentive system put in place: which is ultimately aimed at getting employees to come forward. When the practical details of what action an employee may take to exercise this immunity are unpacked, employees encounter two related

34 *Id.* § 1833 (b)(1).

35 JONATHAN MAYER, THE COMPUTER FRAUD AND ABUSE ACT AND STATE COMPUTER CRIME LAWS (2014), *available at* https://stanford.edu/~jmayer/law696/summaries/CFAA.pdf.

doctrines of law and potential liability outside of trade secret law—namely, the federal CFAA and state computer crime laws.

A. Computer Access Law Under State Statutes Provides More Protection for Employee Whistleblowers

State computer crime and access law, such as the California Comprehensive Computer Data Access and Fraud Act ("CDAFA") and N.Y. Penal Law § 156.00, provide the necessary protection for legitimate whistleblowing activity that is authorized under the Defend Trade Secrets Act ("DTSA"). In contrast, federal computer crime and access law under the Computer Fraud and Abuse Act ("CFAA") is much less promising. Due to the fact that the CDAFA, N.Y. Penal Law § 156.00, and the CFAA each provide a private cause of action for employers, examining the impact of whistleblower liability from these statutes is fundamental to understanding the larger picture of whistleblowing the DTSA imagines.

1. State Computer Crime Statutes

In *Kewanee Oil v. Bicron*, nearly forty years ago, the Supreme Court reasoned that "Congress, by its silence over these many years, has seen the wisdom of allowing the States to enforce trade secret protection."[36] Along this rationale, state-led trade secret litigation has remained a historic cornerstone in intellectual property disputes. Yet, given preemptive effect of the whistleblower provision of the federal Defend Trade Secrets Act on state trade secret law, it is essential to examine the text of state statutes such as computer crime, trade secret, and state non-disclosure agreement law.

The underlying conduct involved in a whistleblowing situation often overlaps and implicates both trade secret law and computer crime law. Imagine an employee who discovers fraudulent information on a company computer and turns over files that may contain protected trade secret information. Yet, because the immunity provision applies to causes of action under *trade secret* law, employers often seek alternative channels of liability exclusively under computer crime law, to which no immunity applies.[37] Therefore, the very same conduct that benefits from immunity under trade secret liability, does not benefit from immunity under computer access law, creating a fundamental disconnect in achieving a working incentive system for whistleblowers. For these reasons, sensible thresholds for liability under computer access law must also be in place, to ensure that the whistleblowing function in society is preserved. As we will explore below, these thresholds for liability vary greatly between federal and state computer crime law.

36 Bruce A. Wessel & Harry Mittleman, *Here's What You Need to Know About the Defend Trade Secrets Act*, RECORDER (Apr. 27, 2016, 5:54 PM), https://www.law.com/therecorder/almID/1202756170494/heres-what-you-need-to-know-about-the-defend-trade-secrets-act/ (citing Kewanee Oil v. Bicron, 416 U.S. 470 (1974)).

37 The text of the DTSA makes clear that "nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means." 18 U.S.C.S § 1833(b)(5) (LexisNexis through Pub. L. No. 115-137).

Even before the federal CFAA's enactment in 1986, many states had their own computer crime laws, although some waited for guidance from the CFAA before enacting their own.[38] Because of the high volume of intellectual property litigation in California, this paper will focus on the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), as codified in California Penal Code Section 502, and compare it with other state computer crime laws. Upon examining these state laws, the consequences of federal preemption of state law become apparent.

a. California Comprehensive Computer Data Access and Fraud Act

The quintessential "whistleblowing situation" the Defend Trade Secrets Act contemplates, where an employee suspects a wrongdoing that prompts an internal investigation, begs the questions of *what*, *where*, and *how* that employee can gain information to bring forth as evidence without triggering personal liability. Yet the DTSA fails to distinguish these crucial details. Instead, it contains a catch-all clause, instructing employees to abide by other applicable laws or face liability.[39] Therefore, seeking guidance from state computer crime law is made necessary. While the boundaries of *what*, *where*, and *how* are unclear under the federal CFAA (as we will see in subsequent sections), the CDAFA's guiding case law from California state courts and the U.S. Northern District of California create whistleblower-friendly thresholds and clear guidelines.

The CDAFA, which is codified in California Penal Code § 502, contains many similar, but a few relevant and distinct provisions as compared to the CFAA.[40] For instance, the CDAFA imposes liability on a person who "[k]nowingly accesses and *without permission* takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network."[41] In *NovelPoster v. Javitch Canfield GroupParties*, the Court reasoned that parties act "without permission" within the meaning of California law and the CDAFA when they "circumvent technical or code-based barriers in place to restrict or bar a user's access."[42] Such circumvention of technical barriers may commonly be referred to as "hacking." In *Sunbelt Rentals Inc. v. Victor*, the absence of facts showing an alleged violator circumvented technical or code-based barriers led the Northern District of California to dismiss the claim under the CDAFA (California Penal Code § 502). The hacking requirement is compelling from a policy perspective, because it requires a showing of clear disregard for privacy and morally culpable behavior. Additionally, requiring hacking activity narrows the scope of liability to specific acts that an employee would be unlikely to

38 MAYER, *supra* note 30.

39 18 U.S.C.S § 1833(b)(5) (LexisNexis through Pub. L. No. 115-137).

40 CAL. PENAL CODE § 502 (Deering 2017).

41 *Id.* § 502(c)(2).

42 NovelPoster v. Javitch Canfield Grp., 140 F.Supp.3d 938, 950 (N.D. Cal 2014) (quoting *Facebook v. Power Ventures, Inc.*, 844 F.Supp.2d 1025, 1036 (N.D.Cal. 2012)); *see also* Sunbelt Rentals v. Victor, 43 F.Supp.3d 1026, 1032 (N.D. Cal. 2014) (dismissing claim under Section 502 where party failed to allege facts showing alleged violator circumvented technical or code-based barriers).

unintentionally take. In this Note, we will see that the California state CDAFA and federal CFAA diverge on this important outer-bound of liability.

Furthermore, the scope of the authorized access that employees can engage in when collecting incriminating evidence is defined by the exception from liability of the CDAFA. In Sections (h)(1) and (h)(2), liability is exempted for "any acts which are committed by a person within the scope of his or her lawful employment."[43] Further, "[f]or purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment."[44] In *Chrisman v. City of Los Angeles*, the Court held that "an employer's disapproval of an employee's conduct does not cast the conduct outside the scope of employment."[45] It went on further to describe that "[i]f the employer's disapproval were the measure, then virtually any misstep, mistake, or misconduct by an employee involving an employer's computer would, by respondents' reasoning, be criminal."[46] This is in sharp contrast to the CFAA, which focuses on the employer's disapproval.

To illustrate, the court in *Chrisman* poses a hypothetical under the CFAA's approach: if an employer prohibited employees from logging onto the Internet to check their personal email, respondents' definition of scope of employment would make reading one's email on company time a crime even where the employee read the email on a computer regularly assigned to that employee. In *Chrisman,* the Court relied on general interpretations of what "within the scope of employment" means to support their interpretation of the CDAFA.[47] The Court in *Chrisman* cites a general example in *Perez v. Van Groningen & Sons, Inc.*, where the California Supreme Court agreed that the employer disapproval is not the measure of the scope of employment.[48] In *Perez,* the court reasoned that, even though a child was hurt while riding a tractor with his uncle, in violation of company rules, the uncle was still within the scope of employment "because he was working for his employer while operating the tractor."[49] Although *Perez* dealt with a personal injury action, the Court in *Chrisman* relied on it to expound the California Supreme Court's general interpretation of scope of employment, and apply it for purposes of the CDAFA's liability exemption. The Court in *Chrisman* ultimately held that under the CDAFA, the "scope of employment" exception of the statute prohibiting unauthorized computer access is not limited to "legitimate job-related conduct."[50] In other words, exemption from liability could be found even for conduct in contravention of an employment policy, because the scope of employment is not defined by employer's disapproval of an activity. The CDAFA expands coverage to any act within the scope of employment, regardless of the act's legitimacy from the employer's perspective. By refusing to hedge liability on the employer's terms, the employer's control over

43 CAL. PENAL CODE § 502(h) (Deering 2017)

44 *Id*. § 502(h)(1).

45 Chrisman v. City of Los Angeles, 155 Cal. App. 4th 29, 37 (Cal. Ct. App. 2007).

46 *Id.* at 37.

47 *Id.* at 36.

48 Perez v. Van Groningen & Sons, Inc., 41 Cal.3d 962, 969 (Cal. 1986).

49 *Id.* at 967–70; *see also Chrisman*, 155 Cal. App. 4th at 36.

50 Chrisman v. City of Los Angeles, 155 Cal. App. 4th 29, 36 (Cal. Ct. App. 2007).

the ability of their employees to discover wrongdoings is dramatically reduced, and the security of the employee whistleblower is elevated.

Everything considered, the standards of the CDAFA are good policy. At the same time that they protect the legitimate conduct of whistleblowers from liability under computer crime law, they do not protect those who engage in fishing expeditions. This aligns with the DTSA's goal of balancing trade secret protection with whistleblower protection, because the CDAFA only exempts whistleblowers who accessed the information within the scope of what was reasonable to their work activities, and does not hedge liability on employer policy. In addition, it does not provide incentives to employees to look outside their daily activities for information and waste time monitoring their employer, because these activities are not covered by the CDAFA's liability exemption.

b. New York Penal Law § 156

Although California boasts the largest state population by far, New York comes close to matching the number of Fortune 500 companies headquartered within the state.[51] Not surprisingly, California, New York, and Texas house nearly one third of America's top companies and sixty-four percent of all Fortune 500 company headquarters.[52] With this in mind, examining relevant New York state statutes available to employers for claims against employee whistleblowers is fundamental to understanding the full scope of considerations that may impact an employee's willingness to speak up regarding employer wrongdoings.

Like California, state computer access and crime laws in New York provide sufficient protection for whistleblowers, in alignment with the balance the DTSA intends to strike between protecting company trade secrets and punishing fraud. Under N.Y. Penal Law § 156.00, criminal access to a computer "without authorization" is defined as "access[ing] a computer, computer service or computer network without the permission of the owner."[53] This requires that the offender had actual, not merely constructive, notice of a revocation of permission, yet proceeded regardless.[54] Paragraph 8 of the statute emphasizes that "[p]roof that such person used or accessed a computer . . . through the knowing use of a set of instructions, code or computer program that bypasses, defrauds or otherwise circumvents a security measure. . . . Such action would be presumptive evidence that such person used or accessed such computer, computer service or computer network without authorization."[55] The presumption of liability from an act of "hacking" is distinctly the line where the CDAFA also seeks to draw liability for potential whistleblowers. Emphasizing hacking to gain unlawful access, over exceeding already authorized access, is the best way to protect legitimate whistleblowing. In practice commentary for N.Y. Penal Law § 156.00, William C. Donnino celebrated the addition of the

51 Robert Hackett, *States with the Most Fortune 500 Companies*, CEO.COM, (June 15, 2015), http://fortune.com/2015/06/15/states-most-fortune-500-companies/.

52 *Id.*

53 N.Y. PENAL LAW § 156.00 (LexisNexis 2018).

54 *Id.*

55 *Id.*

"actual notice" requirement to the offender, which repealed the presumption of notice. He emphasizes the protections that the law provides, namely that "'[i]t remains a defense to both 'unauthorized use of a computer' [N.Y. Penal Law § 156.05] and 'computer trespass' [N.Y. Penal Law § 156.10] that 'the defendant had reasonable grounds to believe that he had authorization to use the computer' [N.Y. Penal Law § 156.50(1)]."[56] Therefore, the statute focuses on assigning liability to instances of explicit contravention of password privacy mechanisms.

2. Federal Computer Crime Statutes

18 U.S.C. § 1833(b)(5) of the DTSA states that "[e]xcept as expressly provided for under this subsection, nothing in this subsection shall be construed to authorize, or limit liability for, an act that is otherwise prohibited by law, such as the unlawful access of material by unauthorized means."[57] The primary federal statute implicated by the absence of guidance from the above provision is the Computer Fraud and Abuse Act ("CFAA"). Under this Act, anyone who "intentionally accesses a computer *without authorization or exceeds authorized access*, and thereby obtains . . . information from any protected computer" is liable.[58] The term "protected computer" is defined as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[59] To prove a violation of the CFAA, the plaintiff must show that the defendant: "(1) intentionally accessed a computer; (2) without authorization or exceeded authorized access; and (3) thereby obtained information from any protected computer if the conduct involved an interstate or foreign communication."[60] "Without authorization" under the CFAA includes *exceeding the purposes* for which access is authorized, and defines liability around limits placed on the *use* of information, even if the information or data may be obtained by permitted *access* to a computer system.[61] Importantly, under the CFAA, it is not necessary that a defendant circumvents a technological access barrier to prove that they accessed a computer without authorization and violated the Computer Fraud and Abuse Act ("CFAA").[62] The court in *Cloudpath Networks v. SecureW2 B.V.* affirmed this idea, reasoning (in alignment with the "Second, Fourth, and Ninth Circuits' shared conclusion") that the term "exceeds authorized access" under the CFAA applies to "individuals who are allowed to access a company computer but use that access to obtain data they are not allowed to see for any purpose."[63]

56 N.Y. PENAL LAW § 156.00 practice cmt. (McKinney 2006).

57 18 U.S.C.S § 1833(b)(5) (LexisNexis through Pub. L. No. 115-137).

58 18 U.S.C. § 1030 (a)(2)(C) (2012).

59 *Id.* § 1030 (e)(2)(B).

60 15B AM. JUR. 2D *Computers and the Internet* § 248 (Westlaw 2018) (discussing accessing computer without authorization or exceeding authorized access).

61 U.S. v. John, 597 F.3d 263, 272 (5th Cir. 2010).

62 United States v. Nosal, 844 F.3d 1024, 1038–39 (9th Cir. 2015).

63 Cloudpath Networks v. Securew2 B.V., 157 F. Supp. 3d 961, 983 (D. Colo. 2016).

Furthermore, in interpreting the CFAA, courts have focused on permission from the employer to limit liability. Yet, the determination of whether an employer has given permission and an employee is without authorization or exceeds authorized access often turns on differences of opinion.[64] In *International Airport Centers v. Citrin*, the Seventh Circuit reasoned that "an employee loses authorization to use a computer when the employee violates a state['s] . . . duty of loyalty [to his employer] because, based on common law agency principles, the employee's actions terminated the employer–employee relationship 'and with it his authority to access the [computer].'"[65] However, in rejecting this view, the Ninth Circuit in *U.S. v. Nosal* reasoned that

> it is the action of the employer that determines whether an employee is authorized to access the computer, and that the only logical interpretation of the statutory phrase "exceeds authorized access" is that the employer has placed limitations on the employee's "permission to use" the computer and the employee has violated—or "exceeded"—those limitations.[66]

Yet in both interpretations, deference is given to the employer's interests. What results? Employer insulation from whistleblowing activity, at the cost of society's benefit from the reporting and disclosure of employer fraud.

Overall, these interpretations result in the potential imposition of liability on employees who, although authorized to use a computer, discover information or data that their employers do not want them to, or do not give explicit permission to view. This undermines the purpose of whistleblowing immunity under the DTSA and strips the value of the whistleblowing function in society. By simply designating specific data or documents that are accessible from an employee's computer as private and unauthorized, employers can use the threat of liability under the CFAA to discourage employees who unintentionally uncover documents revealing fraud from reporting. Under the CFAA, broad liability results for whistleblowers because the scope of *authorized* access is defined *by their employer*. Regardless of the DTSA immunity provision, this threat provides an enormous shield for employers and prevents necessary whistleblowing activity from happening in the first place.

Additionally problematic for whistleblowers is the Circuit split involving broad and narrow interpretations of the CFAA's phrases "without authorization" and "exceeds authorized access." In *EF Cultural Travel B.V. v. Explorica*, the First Circuit held that because an employee of a competing company violated his former employer's confidentiality agreement, he "exceed[ed] authorized access" under the CFAA.[67] In a troubling conclusion, the defendants in *EF Cultural Travel* were found

64 15B AM. JUR. 2D *Computers and the Internet* § 248 (Westlaw 2018) (discussing accessing computer without authorization or exceeding authorized access).

65 United States v. Nosal, 642 F.3d 781, 787 (9th Cir. 2011) (citing Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006)).

66 *Nosal*, 642 F.3d at 787.

67 EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579–84 (1st Cir. 2001).

liable under the CFAA for exceeding authorized access even though they did not in fact access anything unavailable to the general public.[68]

Furthermore, the Seventh Circuit found in *International Airport Centers., LLC v. Citrin*, that by principles of agency law, "an employee acted 'without authorization' [under the CFAA] as soon as the employee severed the agency relationship through disloyal activity."[69] Along with the standard in *Citrin*, a "violati[on] [of] the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship."[70] The Fifth and Eleventh Circuits also apply a broad interpretation of access.[71]

As a whole, these four circuits have interpreted the CFAA in slightly different factual scenarios, yet all have held that "the statutory terms 'without authorization' and/or 'exceeds authorized access' are broad enough to reach the situation in which an employee misuses employer information that he or she is otherwise permitted to access."[72] By relying on loyalty, confidentiality agreements, and agency principles, such a broad interpretation cripples whistleblowing and doles out liability for acting disloyal to an employer, even when acting disloyal may be in the best interest of society and will aid compliance with the law. Alarmingly, the broad view of "exceeds authorized access" has recently become fixated on a violation of employer's policy regarding access and use of computers, putting control over an employee's whistleblowing activity in the hands of the potential violator.[73]

In contrast, the Ninth Circuit was the first to repudiate the "broad" approach of the above mentioned circuits.[74] The Ninth Circuit's narrow approach explicitly refuses to use abstract agency theory to hold an employee liable.[75] In *LVRC Holdings LLC v. Brekka*, the court held that whether the employee "exceeds authorized access"

68 *Id.* at 579 (explaining that using a computer program called a scraper to glean necessary information off of EF's public website exceeded authorized access).

69 Am. Furukawa, Inc. v. Hossain, 103 F. Supp. 3d 864, 871 (E.D. Mich. 2015) (citing Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)).

70 *Citrin*, 440 F.3d at 421 (citing State v. DiGiulio, 835 P.2d 488, 492 (Ariz. 1992)).

71 *Id.*

72 JBCHoldings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 521 (S.D.N.Y. 2013). *See, e.g.*, United States v. John, 597 F.3d 263, 271–72 (5th Cir. 2010) (employee "exceed[ed] authorized access" when he used employer information, to which he had access for other purposes, to perpetrate a fraud); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010) (employee "exceed[ed] his authorized access" when he accessed information for a non-business reason in violation of employer policy); *Citrin*, 440 F.3d at 420 (7th Cir. 2006) (based on principles of agency, employee's authorization to use employer's laptop ended once he violated duty of loyalty to employer, and thus employee accessed computer "without authorization"); *EF Cultural Travel*, 274 F.3d at 581–82 (disloyal employee "exceed[ed] authorized access" when he breached employer confidentiality agreement by helping competitor obtain proprietary information).

73 *See, e.g.*, *John*, 597 F.3d at 271–73 ("While we do not necessarily agree that violating a confidentiality agree-ment . . . would give rise to criminal culpability, we do agree with the First Circuit that the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'"); *Rodriguez*, 628 F.3d at 1263; EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003), 318 F.3d at 62 ("A lack of authorization could be established by an explicit statement . . . ."); *see also* United States v. Salum, 257 F. App'x 225, 230 (11th Cir. 2007); United States v. Teague, 646 F.3d 1119, 1121–22 (8th Cir. 2011).

74 *Am. Furukawa*, 103 F. Supp. 3d at 864 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009)).

75 *Id.*

"depends on the actions taken by the employer."[76] As outlined above,[77] this philosophy approaches (but does not match) the outlook of the California Comprehensive Computer Data Access and Fraud Act, because it suggests that an employer's action to rescind the defendant's right to use the computer is required to satisfy "without authorization." By placing emphasis on an employee acting in the face of his employer taking action to rescind his right to access, the Ninth Circuit indicates that actions synonymous with "hacking" would be a violation. However, though this interpretation is more favorable than the First, Fifth, Seventh and Eleventh Circuit's, it still does not clearly require hacking as under the CDAFA to breach "authorized access."

B. What Immunity Means for Whistleblowers in the Face of Litigation

In the 2016 case *Unum Group v. Loftus*, the U.S. District Court for the District of Massachusetts interpreted Loftus's assertion of immunity under the DTSA as an affirmative defense and emphasized that, "[a]s a general rule, a properly raised affirmative defense can be adjudicated on a motion to dismiss so long as (i) the facts establishing the defense are definitively ascertainable from the complaint and the other allowable sources of information."[78] Employee Loftus filed a motion to dismiss employer Unum's claims for federal and state trade secret misappropriation.[79] Loftus alleged that because he had turned over documents that he removed from his employer to his attorney in order to "report and investigate a violation of law," he validly invoked the whistleblower immunity provision of the DTSA.[80] The court denied Loftus's motion, and reasoned that a defendant must present evidence to justify his immunity, specifically that "the record lack[ed] facts to support or reject his affirmative defense at this stage of litigation. There has been no discovery to determine the significance of the documents taken or their contents . . . ."[81]

Here, the court interpreted the immunity provision to be an affirmative defense, or "immunity from liability," conditioned on the satisfaction of the requirements of the immunity provision, namely Sections 1833 (b)(1)(A) and (b)(1)(B).[82] This is a convincing and well-founded analysis, as the text of the statute reads: "An individual shall not be held criminally or civilly liable under *any Federal or State trade secret law"* and continues to establish strict prerequisites.[83] However, because of the suggestion of broad exemption from liability, it is tempting to interpret the text of Section (b)(1) to indicate an immunity from suit altogether. One may argue that because the word "shall" is included to eliminate liability, Congress indicated

76 *Brekka*, 581 F.3d at 1135.

77 *See* p. 16, *supra.*

78 220 F.Supp.3d 143, 147 (D.Mass. 2016) (quoting Rodi v. S. New England Sch. of Law, 389 F.3d 5, 12 (1st Cir. 2004)).

79 *Unum*, 220 F.Supp.3d at 146.

80 *Id.* at 147.

81 *Id.*

82 *Id*.

83 18 U.S.C.S § 1833(b)(1) et seq. (LexisNexis through Pub. L. No. 115-137).

mandatory exemption from liability, barring a lawsuit entirely. Yet in truth, immunity is predicated upon the satisfaction of Sections (b)(1)(A) and (b)(1)(B).

For example, in a public research paper titled *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act,* Peter S. Menell suggests that the immunity provision of the DTSA "extinguishes liability before litigation gets underway, just as a vaccine immunizes the patient against disease, and thus differs from a 'defense' to liability."[84] From a broad perspective, Menell's argument aligns with the purpose of the DTSA to protect whistleblowers. He emphasizes that the intent of Congress was to create a practical and tangible way to incentivize employees to proceed without fear of incurring legal expenses or other repercussions from serving as a "relator" under the False Claims Act.[85] Yet, he fails to recognize that the authors of the immunity amendment to the DTSA did not seek boundless immunity, but a balance with the purpose of the rest of the statute and the protection it affords to employers' trade secrets. Menell argues that the DTSA's "[i]mmunity is not a 'mere defense' to liability but an 'immunity from suit,'" relying on the 2001 Supreme Court case, *Saucier v. Katz.*[86] However, Menell mistakes the immunity granted by the DTSA for the particularized legal concept of "qualified immunity," which was the relevant law in *Saucier v. Katz*. Justice Kennedy's reasoning in *Saucier*, that the "[t]he privilege is 'an immunity from suit rather than a mere defense to liability'" is in the context of qualified immunity, which is limited to government officials.[87] Qualified immunity "protects a *government official* from lawsuits alleging that the official violated a plaintiff's rights."[88]

To determine the point at which a motion asserting immunity can defeat a pending claim in litigation, sufficient support must be made for any preconditions required by the statute for immunity to apply. Therefore, it follows that the depth of factual inquiry into the prerequisites to immunity, as required by the statute, matter. In *Saucier v. Katz*, the Supreme Court established a two-part test for whether a government official is entitled to qualified immunity: first, "a court must look at whether the facts indicate that a constitutional right has been violated," and if so, then second, "a court must then look at whether that right was clearly established at the time of the alleged conduct."[89] Unique to qualified immunity (as opposed to immunity provisions generally) is that satisfaction of preconditions can be more easily determined from facts set out in the complaint; therefore, a judge may have sufficient evidence at that point in litigation to grant or deny the motion to dismiss. This is so because preconditions for *qualified immunity*, described by the two-part *Saucier* test are often simpler inquiries. Furthermore, facts indicating that a constitutional right was clearly established at the time of the alleged conduct in most

84 Peter S. Menell., *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act,* 1 NEV. L. J. F. 92, 93 (2017).

85 *Id.*

86 *Id.* (citing Saucier v. Katz, 533 U.S. 194 (2001)).

87 *Saucier*, 533 U.S. at 200–01; *see also* Am. Jur. 3d, *Proof of Qualified Immunity Defense in 42 U.S.C.A. § 1983 or Bivens Actions Against Law Enforcement Officers* § 1 (Westlaw 2018).

88 *Qualified Immunity*, CORNELL L. SCH.: LEGAL INFO. INST., https://www.law.cornell.edu/wex/qualified_immunity (last visited Apr. 14, 2018).

89 *Id.*; *see also Saucier*, 533 U.S. at 194.

cases is also easily ascertainable from a complaint, given that it satisfies Rule 12(b)(6) of the Federal Rules of Civil Procedure. In other words, Rule 12(b)(6) has likely done concurrent work to ensure that the complaint states a claim on which relief can be granted. In turn, this would make it likely that the complaint is sufficient to answer whether the plaintiff alleges a violation of rights, whether the defendant is a government official, and whether this right was clearly established at the time of alleged violation of rights.[90] Therefore, a motion to dismiss based on qualified immunity likely does not require additional evidence and can be a defense to suit entirely at the motion to dismiss stage of litigation (consistent with Justice Kennedy's reasoning of qualified immunity as a defense to stand trial, not just an affirmative defense that happens later after evidence is set forth).

In contrast, in *Unum v. Loftus*, the U.S. District Court denied an employee's motion to dismiss his employer's DTSA claim, holding that a defendant under the DTSA must present evidence to justify the immunity.[91] The court reasoned that entitlement to the immunity provision as an affirmative defense must be established by the defendant.[92] Under the DTSA, a defendant must show that the trade secret disclosure: "(A) is made (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the *purpose* of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal."[93] In *Unum*, the preconditions to immunity laid out in the text of Section 1833(b) were not simply a matter of checking boxes, but rather an intensive and fact-based inquiry.

Inquiring as to the purpose of a defendant's actions is no small task. Proving a defendant's purpose in taking an action *ex post* is clearly an all-encompassing factual question. Because of the need for evidence to support the necessary conditions for immunity under the DTSA, it is incorrect to criticize *Unum v. Loftus* as Menell does. To show that Section (A)(ii) is satisfied would require a particularly detailed inquiry into the purpose of the defendant in turning over documents. As the court explains,

> it is not ascertainable from the complaint whether Loftus turned over all of Unum's documents to his attorney, which documents he took and what information they contained, or whether he used, is using, or plans to use, those documents for any purpose other than investigating a potential violation of law.[94]

Therefore, the court's decision to deny the motion to dismiss because of the need to attain more evidence to justify his immunity was proper and necessary given the statutory text.

90 *Id.*

91 Unum Grp. v. Loftus, 220 F.Supp.3d 143, 147 (D.Mass. 2016)

92 *Id.*

93 18 U.S.C.S § 1833(b)(1) (LexisNexis through Pub. L. No. 115-137).

94 *Unum*, 220 F.Supp.3d at 147.

Although not "immunity from suit" as Justice Kennedy suggests in *Saucier*, the "immunity from liability" upon proof of justification laid out in *Unum* aligns with the purpose of the DTSA. As explained above, the purpose of the DTSA was not to entirely *insulate* whistleblowers, but to strike a *balance* between protecting legitimate ownership of trade secrets and protecting important law enforcement activities by safeguarding whistleblowers. Immunity from suit, as Menell suggests, would mistakenly allow those hunting for their employer's unlawful activities to slip through the cracks and escape liability.

V. PROPOSED SOLUTION

All things considered, immunity from trade secret misappropriation as it currently exists in the DTSA is not enough to motivate legitimate whistleblowing activity. Immunity should not be predicated on the absence of conduct that violates the CFAA, when the broad scope of liability under the CFAA flies in the face of the purpose of the DTSA immunity provision. This would greatly confuse employees who are urged by Congress to act while simultaneously walk a thin rope that may lead to their own criminal or civil penalties.

To provide a necessary supplement, two amendments to the DTSA, consisting of 1) a third necessary condition to receiving immunity and 2) an extension of immunity to cover the CFAA, should be adopted. In addition to the existing pre-conditions to immunity,[95] a third element must define the scope of lawful access directly and describe the outer bounds of employee liability to which the immunity would apply. Following the lead of *state* computer crime law, this amendment should require that the employee did not engage in fishing expeditions or "hack" an information system. Most critically, the immunity must also be extended to federal computer access laws, upon satisfaction of the scope requirements. By implementing these requirements directly in the statute, the DTSA would finally have the effect the authors intended: to balance the need for trade secret protection with whistleblower protection.

Without these amendments, the fear of the CFAA's broad liability will put a potential whistleblower back in the very position he or she was before the DTSA: paralyzed by the likelihood of a claim under the employer-friendly CFAA. If a third necessary condition to immunity is added to the statute requiring that employees did not search past a certain scope of access, the federal government will be in the best position to protect legitimate whistleblowing only, as immunity will not extend to acts like hacking.

Because of the changing landscape of intellectual property and the popularity of trade secrets as a choice means of protection, reshaping the law to bar employers from using the threat of trade secret litigation to hide fraudulent activity is critical. A definition by the legislature of the scope of access within the text of the DTSA itself,

95 18 U.S.C.S § 1833(b)(1) (LexisNexis through Pub. L. No. 115-137) (Requiring that "the disclosure of a trade secret [be] made 1.) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and 2) solely for the purpose of reporting or investigating a suspected violation of law" or under seal in a complaint).

coupled with an extension of immunity to federal computer crime law, is essential. Not only would both of these amendments carry out the intent of Congress, but they would also assure whistleblowers when coming forward and prevent unbounded employee "fishing expeditions."

Moreover, if the Defend Trade Secrets Act does not adopt an amendment that defines the scope of access under immunity, a judicial solution to narrow how courts define "exceeds authorized access" is necessary. Specifically, circuit courts should interpret the CFAA to impose liability only on acts falling under the narrower view, requiring something analogous to hacking as laid out by the Ninth Circuit in *Brekka*.

CONCLUSION

The whistleblower immunity provision of the Defend Trade Secrets Act was included to "tackle a broader social justice program" involving the use of trade secret law and nondisclosure agreements ("NDAs") by employers to prevent employees from reporting fraud or illegal activity.[96] When President Obama signed the Defend Trade Secrets Act of 2016 and its whistleblower immunity amendment into law, a departure from past practices was on the horizon. The shift to trade secrets as a commonplace form of intellectual property protection and their wide use across companies heightened the potential for disclosure in a variety of whistleblowing circumstances. To combat fear and hesitation on the part of employees who discover information indicating employer fraud, the immunity provision granted a sweeping immunity from state *and* federal trade secret misappropriation claims. Without such immunity, the threat of impending litigation for trade secret misappropriation acted as a distinct roadblock in employee disclosure.

However, the DTSA has failed to make a legitimate dent in the larger roadblock of liability that employees face vis à vis computer access laws. Although state statutes in California and New York protect legitimate whistleblowing by requiring more malicious activity such as "hacking" to find liability, unfavorable federal statutes are just as easily accessible to employers. The requirement of hacking in many state statutes will punish those embarking on fishing expeditions to uncover potential fraud, while simultaneously protecting those who access incriminating data through the course of employment.

The intent of the legislature in drafting the immunity provision was to reassure and encourage employees who happen upon an employer's misconduct to do the right thing by disclosing it to the government. Without clarification of the scope of computer access that immunity covers and extension of immunity to federal computer law, through an amendment to the DTSA, the provision is a false sense of security. To solve this problem, a third necessary condition to immunity under the DTSA, requiring that employees do not search past a certain scope of access, will put employees and employers in the best position to motivate good behavior of corporate officers and protect legitimate whistleblowing only. The purpose of the whistleblower immunity regime is clear: trade secret law and state non-disclosure

96 Menell, *supra* note 84, at 92.

agreements may not be used to hide allegedly illegal conduct or discourage investigation of such matters.