

SYMPOSIUM ARTICLE

The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History

*Peter S. Menell***

ABSTRACT

The Defend Trade Secrets Act of 2016 (“DTSA”) was the product of a multi-year effort to federalize trade secret protection. In the final stages of drafting the DTSA, Senators Grassley and Leahy introduced an important new element: immunity “for whistleblowers who share confidential information in the course of reporting suspected illegal activity to law enforcement or when filing a lawsuit, provided they do so under seal.” The meaning and scope of this provision are of vital importance to enforcing health, safety, civil rights, financial market, consumer, and environmental protections and deterring fraud against the government, shareholders, and the public. This article explains how the whistleblower immunity provision was formulated and offers insights into its proper interpretation.

* Koret Professor of Law and Co-Director, Berkeley Center for Law & Technology, University of California at Berkeley School of Law. This article grows out of a presentation that I made at a symposium hosted by the Center for Intellectual Property & Entrepreneurship and the Business, Entrepreneurship & Tax Law Review at the University of Missouri School of Law on March 17, 2017. I am grateful to Professor Dennis Crouch for organizing the symposium and Brittany Bruns and Amit Elazari for research assistance. I am especially grateful to the Senate Judiciary Committee staff for reaching out to me in drafting the Defend Trade Secrets Act of 2016. This article is largely based on Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 Calif. L. Rev. 1 (2017).

No. 2]	<i>Menell: The DTSA Whistleblower Immunity Provision</i>	399
--------	--	-----

TABLE OF CONTENTS

I. INTRODUCTION.....	400
II. PROLOGUE.....	401
III. SUBVERSION OF TRADE SECRET PROTECTION.....	403
IV. FORMULATING THE WHISTLEBLOWER IMMUNITY PROPOSAL.....	407
<i>A. The Trade Secrecy/Law Enforcement Tension.....</i>	<i>407</i>
<i>B. The Interplay of Trade Secrecy and Whistleblowing.....</i>	<i>410</i>
<i>C. Tailoring a Trade Secret Public Policy Exception.....</i>	<i>416</i>
V. LEGISLATIVE HISTORY OF THE DTSA WHISTLEBLOWER IMMUNITY PROVISION	419
VI. INTERPRETING THE WHISTLEBLOWER IMMUNITY PROVISION.....	425

I. INTRODUCTION

On May 11, 2016, President Barack Obama signed the Defend Trade Secrets Act (“DTSA”)¹ into law.² This historic legislation was the product of a multi-year effort to federalize trade secret protection.³ In the final stages of drafting the law, Senators Chuck Grassley and Patrick Leahy introduced an important new element: immunity “for whistleblowers who share confidential information in the course of reporting suspected illegal activity to law enforcement or when filing a lawsuit, provided they do so under seal.”⁴

The meaning and scope of this provision are of vital importance to enforcing health, safety, civil rights, financial market, consumer, and environmental protections and deterring fraud against the government, shareholders, and the public. Unlike other aspects of the DTSA, the whistleblower immunity provision emerged toward the end of the legislative process and was not the subject of formal hearings.⁵ Senator Leahy’s remarks on the Senate floor on the day that the Senate unanimously approved the DTSA summarize the provision’s rationale and note a source for its formulation:

1. See Defend Trade Secrets Act of 2016, Pub. L. No. 114–153, 130 Stat. 376 (to be codified at 18 U.S.C. § 1836).

2. See The White House, Office of the Press Secretary, *Remarks by the President at Signing of S. 1890 – Defend Trade Secrets Act of 2016* (May 11, 2016, 3:43 PM), <https://obamawhitehouse.archives.gov/the-press-office/2016/05/11/remarks-president-signing-s-1890-defend-trade-secrets-act-2016>.

3. See Victoria Espinel, *Launch of the Administration’s Strategy to Mitigate the Theft of U.S. Trade Secrets*, OBAMA WHITE HOUSE ARCHIVES: BLOG (Feb. 20, 2013, 2:59 PM), <https://obamawhitehouse.archives.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets>; THE COMM’N ON THEFT OF AM. INTELLECTUAL PROPERTY, THE IP COMMISSION REPORT 1 (May 2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf (“The scale of international theft of American intellectual property (IP) is unprecedented—hundreds of billions of dollars per year. . . .”); OFF. OF THE NAT’L COUNTERINTELLIGENCE EXECUTIVE, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection of Industrial Espionage 2009–2011*, (Oct. 2011), <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-055.pdf> (“Estimates from academic literature on the losses from economic espionage range . . . from \$2 billion to \$400 billion or more a year. . . .”); U.S. INT’L TRADE COMMISSION, *China: Effects of Intellectual Property Infringement and Innovation Policies in the U.S. Economy* xiv (May 2011), <http://www.usitc.gov/publications/332/pub4226.pdf> (estimating that in 2009, U.S. firms lost between \$14.2 billion and \$90.5 billion due to intellectual property infringement in China). Legislation to establish a federal civil cause of action for trade secret misappropriation dates back to 2012. See S. 3389, 112th Cong. (2012). Bills were offered in 2014 and 2015. See H.R. 5233, 113th Cong. (2014); S. 2267, 113th Cong. (2014); H.R. 3326, 114th Cong. (2015).

4. *Statement of Senator Patrick Leahy (D-Vt.), Ranking Member, Senate Judiciary Committee, Executive Business Meeting*, U.S. SENATE (Jan. 28, 2016), <https://www.judiciary.senate.gov/imo/media/doc/012816%20Leahy%20Statement1.pdf> [hereinafter *Executive Business Meeting*]; Press Release, Senator Patrick Leahy (D-Vt.), Ranking Member, Senate Judiciary Comm., Leahy-Grassley Amendment to Protect Whistleblowers Earns Unanimous Support in Judiciary Committee (Jan. 28, 2016), https://www.leahy.senate.gov/press/leahy-grassley-amendment-to-protect-whistleblowers_earns-unanimous-support-in-judiciary-committee [hereinafter Press Release].

5. In the most thorough analysis of the general legislative history of the DTSA, Research and Instructional Services Librarian John Cannan merely summarized the whistleblower immunity provision. See John Cannan, *A (Mostly) Legislative History of the Defend Trade Secrets Act of 2016*, SSRN 26-27 (May 4, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2775390.

Today, the Senate voted on legislation that will provide a valuable tool to protect against trade secret theft. This legislation is supported by businesses from diverse sectors of our economy, including companies large and small. . . . The Defend Trade Secrets Act contains a bipartisan provision I offered with Senator Grassley to ensure that employers and other entities cannot bully whistleblowers or other litigants by threatening them with a lawsuit for trade secret theft. The provision protects disclosures made in confidence to law enforcement or an attorney for the purpose of reporting a suspected violation of law and disclosures made in the course of a lawsuit, provided that the disclosure is made under seal. It requires employers to provide clear notice of this protection in any nondisclosure agreements they ask individuals to sign. This commonsense public policy amendment is supported by the Project on Government Oversight and the Government Accountability Project and builds upon valuable scholarly work by Professor Peter Menell.⁶

This article explains how the whistleblower immunity provision was formulated and offers insights into its proper interpretation. Before turning to the crafting of the provision, I retrace the scholarly journey that motivated the DTSA whistleblower immunity provision.

II. PROLOGUE

I begin with the story of Dr. Jeffrey Wigand, part of the inspiration for the whistleblower immunity provision. Dr. Wigand was a public health research scientist who became one of the most famous whistleblowers in United States history.⁷ He was the subject of a “mishandled” 60 Minutes episode⁸ that provided the basis for “The Insider,” a riveting motion picture exposing the tobacco industry’s efforts to suppress disclosure of its insidious efforts to increase the addictiveness of cigarettes.⁹

In 1989, Brown & Williamson Tobacco Corporation (“B&W”) hired Dr. Wigand, a Ph.D. biochemist, as Vice President of Research and Development.¹⁰ Dr.

6. 162 CONG. REC. S1636-37 (daily ed. Apr. 4, 2016) (statement of Sen. Leahy). Senator Leahy was referring to a draft of the article referenced in note *. The final version of that article faithfully reflects the text and analysis of the draft version that attracted the Senate Judiciary Committee’s attention. The only substantial change in the article was the addition of Part V, which summarizes the DTSA whistleblower immunity provision. The reason for this addition was that passage of the DTSA leapfrogged the publication process (the article was accepted in February 2015, several months before passage of the DTSA). Parts I–IV of the article, which provided the basis for the DTSA whistleblower immunity provision, were published as initially submitted apart from modest formatting edits so as to preserve a record of the foundation for the DTSA whistleblower immunity provision.

7. See Cassi Feldman, *60 Minutes’ Most Famous Whistleblower*, CBS NEWS: 60 MINUTES OVERTIME (Feb. 4, 2016), <https://www.cbsnews.com/news/60-minutes-most-famous-whistleblower/> (quoting 60 Minutes Executive Producer Jeff Fager observing that “[t]he story itself was one of the most – probably the most important story that was ever reported by 60 Minutes.”); see also Marie Brenner, *The Man Who Knew Too Much*, VANITY FAIR (Apr. 1, 2004, 12:00 AM), <https://www.vanityfair.com/magazine/1996/05/wigand199605>.

8. Feldman, *supra* note 7; Brenner, *supra* note 7.

9. See *The Insider*, IMDB, <http://www.imdb.com/title/tt0140352/> (last visited Dec. 3, 2017).

10. See Brown & Williamson, WIKIPEDIA, https://en.wikipedia.org/wiki/Brown_%26_Williamson (last updated Nov. 2, 2017).

Wigand was led to believe that he would be developing a safer cigarette.¹¹ In the course of his work, Dr. Wigand learned that the company was looking for ways to make cigarettes *more* addictive through nicotine-impact boosting—the use of ammonia and other chemicals to enhance nicotine absorption in the lungs.¹² Dr. Wigand’s unwillingness to support this effort ultimately led to his firing in March 1993.¹³ Dr. Wigand believed that he was barred from disclosing confidential information, including information pertaining to B&W’s efforts to make cigarettes more addictive, because he had signed a non-disclosure agreement (“NDA”).¹⁴

Dr. Wigand reassessed his adherence to the broad terms of the NDA after he became suspicious that B&W had sabotaged his efforts to find gainful employment.¹⁵ B&W’s filing of a breach of contract drove him to take action. Dr. Wigand cautiously reached out to Andrew McGuire, a trauma prevention activist with whom he was acquainted.¹⁶ McGuire passed Dr. Wigand’s contact information along to Lowell Bergman, then a 60 Minutes investigative reporter,¹⁷ as a source for a possible story on cigarette and fire safety. Dr. Wigand reluctantly agreed to talk with Bergman and eventually became a paid consultant for a 60 Minutes episode on a fire-safe cigarette project at Phillip Morris.¹⁸

In April 1994, tobacco company executives from B&W and other major cigarette manufacturers testified before Congress that they believed that “nicotine is not addictive.”¹⁹ The Food and Drug Administration (“FDA”) contacted Dr. Wigand about the truth of the industry’s position.²⁰ With Bergman’s encouragement, Dr. Wigand eventually agreed to disclose the industry’s dirty secrets about nicotine-impact boosting on camera.²¹

11. See *id.*; Brenner, *supra* note 7.

12. See Brenner, *supra* note 7; Brown & Williamson, *supra* note 10.

13. Brenner, *supra* note 7.

14. See *Anatomy of a Decision: Facts and Context in the “60 Minutes” Decision Not to Air a Tobacco Industry Exposé*, PBS: FRONTLINE, <http://www.pbs.org/wgbh/pages/frontline/smoke/cron.html> (last visited Dec. 4, 2017). He later signed a more restrictive “nondisclosure settlement agreement.” *Id.*

15. See Brenner, *supra* note 7.

16. *Id.*

17. *Id.* The corporate machinations surrounding the 60 Minutes reporting about the tobacco industry ultimately led to Bergman’s departure. See Alex Berenson, ‘60 Minutes’ Producer Aims Bitter Blast at Ex-Colleague, N.Y. TIMES (June 4, 2000), <http://www.nytimes.com/2000/06/04/us/60-minutes-producer-aims-bitter-blast-at-ex-colleague.html>. He now holds the Reva and David Logan Distinguished Chair in Investigative Journalism at the University of California at Berkeley. Lowell Bergman, UC BERKELEY: JOURNALISM, <https://journalism.berkeley.edu/person/bergman/> (last visited Dec. 3, 2017).

18. See Brenner, *supra* note 7. The fire-safe cigarette project episode was itself the result of whistleblowing in the tobacco industry. *Private Sector Whistleblowers: Are There Sufficient Legal Protections?*, Hearing Before Subcomm. on Workforce Prot. of the H. Comm. on Educ. & Labor, 110th Cong. 11 (2007) (statement of Jeffrey Wigand). Lowell Bergman had received a box with approximately 2,400 Philip Morris documents from an anonymous source. *Id.* Bergman employed Dr. Wigand to interpret these technical documents, which revealed that Philip Morris had developed a fire-safe cigarette, but had chosen not to market it. *Id.* at 11–12.

19. See Philip J. Hilts, *Tobacco Chiefs Say Cigarettes Aren’t Addictive*, N.Y. TIMES (Apr. 14, 1994), <http://www.nytimes.com/1994/04/15/us/tobacco-chiefs-say-cigarettes-aren-t-addictive.html>; *Regulation of Tobacco Products: Hearings Before the Subcomm. on Health & the Env’t of the H. Comm. on Commerce & Energy*, 103d Cong. 628 (1994) (testimony of Messrs. Campbell, J. Johnston, Taddeo, Tisch, Horrigan, Sandefur, and D. Johnston).

20. See Brenner, *supra* note 7.

21. *Id.*

That summer, Dr. Wigand also became involved with several tobacco-related litigations,²² which raised the specter that B&W would seek to block disclosure of its confidential information. CBS's General Counsel became concerned that B&W could sue CBS for tortious interference with contractual relations—namely B&W's NDA with Dr. Wigand—if it aired an interview in which Dr. Wigand disclosed B&W trade secrets.²³

As feared, B&W pursued litigation seeking to bar Dr. Wigand from disclosing confidential information.²⁴ Nonetheless, Dr. Wigand testified in a Mississippi suit in which the state sought reimbursement from the tobacco industry for the welfare and health care costs associated with illnesses arising from the use of tobacco products.²⁵ This and parallel litigation in other states alleging claims for restitution and unjust enrichment on the basis of tobacco companies' "wrongful conduct" and common law public nuisance²⁶ ultimately resulted in settlements totaling hundreds of billions of dollars and bringing about substantial changes in the industry.²⁷

III. SUBVERSION OF TRADE SECRET PROTECTION

This story brought to light a disturbing misuse of trade secret protection. A major tobacco company subverted legal protections designed to promote socially beneficial innovation so as to maximize corporate profits at the expense of public health. As even a cursory examination of the history of corruption and fraud litigation reveals, such abuse has not been limited to a few bad actors or questionable industries. Many of the most significant public health and environmental problems, corrupt practices, and fraudulent activities—including the asbestos toxicity cover-

22. See *id.*; Henry Weinstein, *Tobacco Whistle-Blower's Star is Rising*, L.A. TIMES (Apr. 25, 1996), http://articles.latimes.com/1996-04-25/news/mn-62701_1_tobacco-industry; Michael Janofsky, *Philip Morris Accuses ABC of Libel*, N.Y. TIMES (Mar. 25, 1994), <http://www.nytimes.com/1994/03/25/us/philip-morris-accuses-abc-of-libel.html>.

23. Brenner, *supra* note 7.

24. See *Brown & Williamson Tobacco Corp. v. Wigand*, 913 F. Supp. 530, 531 (W.D. Ky. 1996) (noting that B&W filed suit against Dr. Wigand on November 21, 1995 alleging theft, fraud, breach of contract, breach of fiduciary and common law duties, and violation of the Kentucky Uniform Trade Secrets Act).

25. See *Money & Investigating Update*, WALL STREET J., <https://online.wsj.com/public/resources/MoneyInvesting/reference/bw.htm> (last visited Dec. 4, 2017); see also Hunt Helm, *Blowing the Whistle on Big Tobacco: Wigand, Williams Lifted Secrecy's Veil – Their Revelations Changed the History of the Tobacco Industry*, COURIER-J. (May 25, 1997), <http://archive.tobacco.org/News/97052shelms.html>.

26. See Mitchell L. Lothrop, *Tobacco – Related Litigation: How It May Impact the World's Insurance Industry*, 3 CONN. INS. L. J. 305, 320–21 (1997).

27. John M. Broder, *Cigarette Makers in a \$368 Billion Accord to Curb Lawsuits and Curtail Marketing*, N.Y. TIMES (June 21, 1997), <http://www.nytimes.com/1997/06/21/us/cigarette-makers-in-a-368-billion-accord-to-curb-lawsuits-and-curtail-marketing.html>.

up,²⁸ the obesity crisis,²⁹ evasion of environmental protection laws,³⁰ fraud against the government,³¹ and Ponzi schemes³²—have been hidden behind the veil of corporate secrecy. These abuses have an institutional cause: NDAs functioning as a form of corporate omertà.³³ Furthermore, some members of the defense bar have openly advocated the use of trade secret claims against current and former employees to discourage whistleblowing.³⁴

This pattern of abuse exposes a dark underside of trade secret protection. I have long been teaching a course surveying the principal modes of intellectual property protection: trade secret, patent, copyright, and trademark. Over the years, I became

28. See PAUL BRODEUR, *OUTRAGEOUS MISCONDUCT: THE ASBESTOS INDUSTRY ON TRIAL* 74 (1985) (concluding that for half a century asbestos manufacturers withheld and suppressed information about the risks to insulation workers from breathing asbestos fibers).

29. See Anahad O'Connor, *How the Sugar Industry Shifted Blame to Fat*, N.Y. TIMES (Sept. 12, 2016), <https://www.nytimes.com/2016/09/13/well/eat/how-the-sugar-industry-shifted-blame-to-fat.html> (revealing documents showing that the sugar industry corrupted researchers in an effort to shift public opinion); see also Camila Donomske, *50 Years Ago, Sugar Industry Quietly Paid Scientists To Point Blame At Fat*, NPR (Sept. 13, 2016, 9:59 AM), <http://www.npr.org/sections/thetwo-way/2016/09/13/493739074/50-years-ago-sugar-industry-quietly-paid-scientists-to-point-blame-at-fat>; Cristin Kearns et al., *Sugar Industry and Coronary Heart Disease Research: A Historical Analysis of Internal Industry Documents*, 176 JAMA INTERN. MED. 1680, 1685 (2016).

30. See Nathaniel Rich, *The Lawyer Who Became DuPont's Worst Nightmare*, N.Y. TIMES (Jan. 6, 2016), <https://www.nytimes.com/2016/01/10/magazine/the-lawyer-who-became-duponts-worst-nightmare.html> (describing DuPont Corporation's cover-up of a massive toxic pollution attributable to manufacturing of Perfluorooctanoic (PFOA) acid, a chemical used producing its Teflon nonstick cookware products); see also Sharon Kelly, *DuPont's Deadly Deceit: The Decades-Long Cover-up Behind the "World's Most Slippery Material"*, SALON (Jan. 4, 2016, 4:00 AM), https://www.salon.com/2016/01/04/teflons_toxic_legacy_partner/; see also Jack Ewing, *Volkswagen Engine-Rigging Scheme Said to Have Begun in 2008*, N.Y. TIMES (Oct. 4, 2015), <https://www.nytimes.com/2015/10/05/business/engine-shortfall-pushed-volkswagen-to-evade-emissions-testing.html>.

31. See generally CLAIRE M. SYLVIA, *THE FALSE CLAIMS ACT: FRAUD AGAINST THE GOVERNMENT* § 2:9 (3d ed. 2016).

32. See HARRY M. MARKOPOLOS, *NO ONE WOULD LISTEN: A TRUE FINANCIAL THRILLER* (2010).

33. The omertà refers to a code of silence, associated most commonly with the Mafia, used to hide criminal activity. NAT'L CRIME SYNDICATE, *What Was The Code of Omertà?*, <http://www.nationalcrimesyndicate.com/code-of-omerta/> (last visited Dec. 4, 2017).

34. See Carlton Fields, *Employers Fight Back Against Whistleblowers*, LEXOLOGY (July 2, 2014), <http://www.lexology.com/library/detail.aspx?g=b2e89afd-6e2a-4310-9139-b94176e38e13> (noting that "[e]mployers may even have options against employees who have been successful in [False Claims Act (FCA) cases], but who have breached their employment agreements or who have stolen documents. Courts have recently been more willing to permit counterclaims against employee relators. Additionally, there is at least one case in which an employer filed suit against a whistleblower after losing a FCA case."); see also Amanda Haverstick, *Health Care Employers Take Note: New Weapons Are Available When Defending False Claims Act Suits*, FORBES (June 20, 2014, 3:51 PM), <http://www.forbes.com/sites/theemploymentbeat/2014/06/20/health-care-employers-take-note-new-weapons-are-available-when-defending-false-claims-act-suits> (reporting on cases allowing counterclaims against whistleblowers for taking documents and observing that the "takeaway" for employers was that they have "more defense options in qui tam suits brought by employees who impermissibly disclose protected health information (PHI) or other confidential employer information"); see also Samantha P. Kingsbury & Karen S. Lovitch, *Can a Relator be Held Liable for Using Confidential Company Documents to Support a Qui Tam Case?*, HEALTH L. & POL'Y MATTERS (June 24, 2014), www.health-lawpolicymatters.com/2014/06/24/; see also Lisa M. Noller & Brandi F. Walkowiak, *Holding Rogue Employees Accountable Under the FCA*, FOLEY (Nov. 3, 2011, 1:29 PM), <https://www.foley.com/files/Publication/6e6b9e4f-38f1-457a-a7ad-c331a0757194/Presentation/PublicationAttachment/e45a77e2-8d6e-487b-80d3-c58826bdf89/WCL36011-3-11.pdf>; see also *Corporate Crime: The Age of the Whistleblower*, ECONOMIST (Dec. 3, 2015), <https://www.economist.com/news/business/21679455-life-getting-better-those-who-expose-wrongdoing-companies-continue-fight> (reporting that companies continue to fight back against those who expose wrongdoing, often against their own interests).

aware of an unusual gap in the trade secrets component of the course. Whereas the patent, copyright, and trademark regimes featured exceptions and limitations designed to counterbalance social harm from overprotection—such as patent law’s misuse doctrine³⁵ and various other limitations,³⁶ copyright’s fair use doctrine³⁷ and statutory licenses,³⁸ and trademark law’s First Amendment limitations³⁹—there were no analogous balancing limitations in trade secrets coverage. The Uniform Trade Secrets Act (“UTSA”),⁴⁰ on which the trade secrets laws in most states are based,⁴¹ lacks any public policy provision. My own casebook at the time,⁴² like others,⁴³ overlooked this defect of trade secret protection.

To explore this lacuna, I added some material from the Restatement (Third) of Unfair Competition relating to a public policy limitation on trade secret protection to my spring 2015 intellectual property course.⁴⁴ For the final examination, I formulated the following question to test students’ policy analysis skills:

PART III (60 minutes)

To: Attorney, Congressional Research Service
From: Senator Boxstein
Re: Proposed Trade Secret “Public Policy” Safe Harbor

35. See *Motion Picture Patents Co. v. Universal Film Mfg. Co.*, 243 U.S. 502 (1917).

36. 35 U.S.C. § 271(e)(1) (2012) (patent experimental use doctrine applicable to drug testing); *id.* § 273(b) (patent prior user right); *id.* § 287(c) (bar against remedies for infringement of medical procedure patents by doctors and hospitals); *Adams v. Burke*, 84 U.S. (17 Wall.) 453 (1873) (exhaustion doctrine); *Bloomer v. Millinger*, 68 U.S. (1 Wall.) 340 (1863) (repair doctrine); *Whittemore v. Cutter*, 29 F. Cas. 1120 (C.C.D. Mass. 1813) (common law experimental use).

37. See 17 U.S.C. § 107 (2012).

38. See *id.* § 108 (limitations on exclusive right to copy for archival copies for public libraries); *id.* § 110 (public interest exceptions for exclusive right to publicly perform copyrighted works).

39. See 15 U.S.C. § 1115(b)(4) (2012) (classic [descriptive] fair use); *id.* § 1125(c)(3) (trademark dilution exclusions for fair use [including nominative and descriptive fair use], news reporting, and non-commercial use from trademark dilution); *New Kids on the Block v. News Am. Publ’g, Inc.*, 971 F.2d 302 (9th Cir. 1992) (nominative fair use).

40. UNIF. TRADE SECRETS ACT, 14 U.L.A. 437 (1985).

41. All states except New York, North Carolina, and Massachusetts have adopted the UTSA. See *Trade Secrets Act*, UNIFORM L. COMMISSION, <http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act> (last visited Dec. 3, 2017). North Carolina’s trade secret statute borrows heavily from the UTSA. See N.C. GEN. STAT. ANN. §§ 66–152 (West 2015).

42. See ROBERT P. MERGES, PETER S. MENELL, & MARK A. LEMLEY, *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE* (6th ed. 2012) (lacking any discussion of the subversion of trade secret protection to discourage whistleblowing). This oversight has since been corrected. See PETER S. MENELL, MARK A. LEMLEY, & ROBERT P. MERGES, *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE – VOLUME I: PERSPECTIVES, TRADE SECRETS AND PATENTS* 98–102 (2017).

43. See, e.g., DAVID L. LANGE, MARY LAFRANCE, GARY MYERS, & LEE ANN W. LOCKRIDGE, *INTELLECTUAL PROPERTY: CASES AND MATERIALS* 372–413 (4th ed. 2012) (overlooking the public policy limitation); MARGRETH BARRETT, *INTELLECTUAL PROPERTY: CASES AND MATERIALS* 32–119 (4th ed. 2011) (same); SHUBHA GHOSH, RICHARD GRUNER, JAY P. KESAN & ROBERT I. REIS, *INTELLECTUAL PROPERTY RIGHTS, THE PUBLIC INTEREST, AND THE REGULATION OF CREATIVE ACTIVITY* 7–71 (2007) (same).

44. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (AM. LAW INST. 1995) (noting that trade secret protection can “implicate the interest in freedom of expression or advance another significant public interest” and a “privilege is likely to be recognized . . . in connection with the disclosure of information that is relevant to public health or safety, or to the commission of a crime or tort, or to other matters of substantial public concern”).

Although many states have adopted a version of the Uniform Trade Secrets Act, there is growing interest in passing a broad federal trade secrets statute for several reasons: (1) to strengthen U.S. protection for intellectual property by bringing trade secrets on par with patents, copyrights, and trademarks as a national, federal regime; (2) to address the growing tide of international trade secret theft by adding a robust “seizure” provision that would give federal courts power to enter *ex parte* seizure orders before trade secrets can leave the country; and (3) to promote a nationally uniform trade secrets regime—businesses wish to reduce the uncertainty of doing business in many states with different rules.

While I generally support such legislation as a way to promote technological innovation, I worry that the focus on strengthening trade secret protections could exacerbate an existing problem of trade secret protection—the widespread use of non-disclosure agreements to deter employees and contractors from disclosing illegal and fraudulent activities to government officials. For example, corporations routinely require employees to sign broad confidentiality agreements with sometimes excessive liquidated damages provisions and arbitration clauses that restrict reporting wrongdoing to the government. If an individual faces a potential lawsuit for crushing liability (not to mention the costs of defending such a lawsuit and the adverse effects on future employment prospects) for disclosing information that could be considered a trade secret, he or she may not be willing to risk reporting information. I worry that a federal trade secret law will become a bigger cudgel to prevent whistleblowers from providing information about violations of law to the appropriate authorities. I would also like to see state trade secret laws blunted so as to avoid these undesirable effects on ferreting out illegal and fraudulent activities.

I am considering proposing a “public policy” safe harbor to address these concerns. I anticipate that there will be substantial opposition to any “public policy” limitation on trade secret protection from the Chamber of Commerce and other pro-business groups. It is critical that we anticipate their concerns and address them in a balanced manner.

Here is a sketch of what I have in mind:

- **Immunity from Liability for Confidential Disclosure of Trade Secret Information to the Government:** An individual who discloses information, either directly or through his or her lawyer, in confidence to a federal, state, or local government official, or files a lawsuit or initiates a proceeding filed under seal in connection with a whistleblower program, solely for the purpose of investigating a violation of law is not subject to suit under federal (or state) trade secret law for that disclosure.
- **Attorney-Client Privilege:** This immunity extends to the whistleblower’s attorney so long as the attorney does not disclose or use the information outside of representing the whistleblower in reporting the alleged illegal conduct.
- **Exception:** If the person disclosed or used the information for non-law enforcement purposes, such as starting a competing business or discussing the information in the press, he or she cannot benefit from the safe harbor.

- **Use of Trade Secret Information in Anti-Retaliation Lawsuits:** A person bringing a lawsuit for retaliation by an employer for the reporting of a violation of law may share the trade secret information with their attorney and use the trade secret information in the court proceeding without violating federal (or state) trade secret law so long as they file the information under seal and do not disclose the information except pursuant to court order.
- **Notice:** All non-disclosure agreements must include notice of the public policy safe harbor. Failure to include this notice shall make the agreement null and void.

Please prepare a short memo (four to six paragraphs) addressing the pros and cons of the “public policy” safe harbor proposal. Feel free to suggest any improvements, changes, or issues that should be considered.

IV. FORMULATING THE WHISTLEBLOWER IMMUNITY PROPOSAL

This foray into the social justice and public policy ramifications of trade secret law piqued my curiosity. I added exploration of a public policy exception to trade secret protection to my summer research agenda. In addition to tracing the history of trade secret protection, I embarked on a deep dive into the social science literature on whistleblowers and the personnel management literature on onboarding of employees.⁴⁵

A. The Trade Secrecy/Law Enforcement Tension

The emergence and evolution of trade secret protection explained why state trade secrets statutes had not included a public policy limitation. The trade secrets regime emerged in response to the economic upheaval of the Industrial Revolution. Before the nineteenth century, an informal system of social norms afforded craftsmen effective protection for most technological advances.⁴⁶ Craftsmen passed along their trade knowledge to their apprentices with the understanding that the know-how would be kept secret during the apprenticeship period. After this training, the apprentice was free to practice the trade. Custom, trade-guilds, and close-knit communities reinforced these trust-based protections.

The rise of factories and increased employee mobility during the Industrial Revolution eroded the small-scale, localized social norm system that had adequately safeguarded trade knowledge in the preindustrial age. Recognizing the need for commercial morality and technological progress in the rapidly industrializing economy,⁴⁷ courts gradually developed a common law tort-based regime for protecting

45. The discussion in this section summarizes the analysis in Menell, *supra* note *. That article provides more detailed analysis and references for the summary that follows.

46. These protections were augmented by the patent system, which afforded protection for larger, discrete advances.

47. See *Eastman Co. v. Reichenbach*, 20 N.Y.S. 110, 116 (Sup. Ct. 1892), *aff'd sub nom.* *Eastman Kodak Co. v. Reichenbach*, 29 N.Y.S. 1143 (Sup. Ct. 1894) (enjoining defendants' competing venture on the ground that “[t]his is not legitimate competition, which it is always the policy of the law to foster and encourage, but it is *contra bonos mores* [against good morals], and constitutes a breach of trust which a court of law, and much less a court of equity, should not tolerate”).

trade secrets.⁴⁸ Trade secret protection could encompass information that was not generally known to the public so long as the employer undertook reasonable precautions to preserve secrecy.⁴⁹ This latter requirement brought NDAs into common practice. Failure to guard against disclosure of trade secrets by employees and contractors would jeopardize trade secret protection.

Thus, trade secret protection emerged and largely crystallized before the vast expansion of the government's role in regulating economic activity.⁵⁰ Over the course of the past century and a half—encompassing the Progressive, New Deal, Civil Rights, Environmental Protection, and Information Eras—the federal and state governments have assumed a much larger role in regulating product and service markets, worker safety, civil rights, public health, the environment, securities markets, and information technologies.⁵¹ Moreover, the federal and state governments have taken on a much larger role as economic actors in the general economy,⁵² contracting with private enterprises for provision of goods and services,⁵³ providing health insurance,⁵⁴ and funding research and development.⁵⁵ Government spending across all levels of government has risen over the course of the twentieth century from about 7% of the gross domestic product to about 45%.

This transformation expanded private enterprises' responsibilities to comply with public health and safety, civil rights, environmental, consumer, and financial market regulations, meet contractual obligations with the government, and shoulder tax burdens. The federal and state governments enacted laws and established poli-

48. See Catherine L. Fisk, *Working Knowledge: Trade Secrets, Restrictive Covenants in Employment, and the Rise of Corporate Intellectual Property, 1800–1920*, 52 HASTINGS L. J. 441, 450–88 (2001); see also *Vickery v. Welch*, 36 Mass. (19 Pick.) 523, 525–27 (1837) (granting specific performance of a contractual agreement regarding the “exclusive use” of a secret method for making chocolate); see also MELVIN F. JAGER, *TRADE SECRETS LAW* § 2:3 (2013). The emerging law of trade secrets was collected in the Restatement of Torts. See RESTATEMENT (FIRST) OF TORTS §§ 757–58 (AM. LAW INST. 1939). When the Restatement (Second) of Torts was published in 1979, the authors omitted sections 757 and 758 on the grounds that the law of trade secrets had developed into an independent body of law that no longer relied on general principles of tort law. See RESTATEMENT (SECOND) OF TORTS div. 9, intro. n. (AM. LAW INST. 1979). As noted earlier, trade secrets were incorporated into the RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (AM. LAW INST. 1995).

49. See *Eastman Co. v. Reichenbach*, 20 N.Y.S. at 116.

50. See Robert L. Rabin, *Federal Regulation in Historical Perspective*, 38 STAN. L. REV. 1189, 1196 (1986) (prior to the mid-1880s, “[f]ederal agencies did not generally inspect, investigate, or monitor any significant business activity to protect against unreasonable risks . . . From a national perspective, commercial affairs took place in a world without regulation.”).

51. See 3 BRUCE ACKERMAN, *WE THE PEOPLE: THE CIVIL RIGHTS REVOLUTION* (2014); see also PHILLIP J. HILTS, *PROTECTING AMERICA’S HEALTH: THE FDA, BUSINESS, AND ONE HUNDRED YEARS OF REGULATION* (2003); see also RICHARD J. LAZARUS, *THE MAKING OF ENVIRONMENTAL LAW* (2006).

52. See Paul Stephen Dempsey, *Transportation: A Legal History*, 30 TRANSP. L. J. 235, 267 (2003); see also Kevin Werbach, *Higher Standards Regulation in the Network Age*, 23 HARV. J. L. & TECH. 179, 201 (2009).

53. See *GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY* (Jody Freeman & Martha Minow eds., 2009).

54. *How is Medicare Funded?*, MEDICARE.GOV, <https://www.medicare.gov/about-us/how-medicare-is-funded/medicare-funding.html> (last visited Dec. 3, 2017); *Financing & Reimbursement*, MEDICAID.GOV, <https://www.medicaid.gov/medicaid/financing-and-reimbursement/> (last visited Dec. 3, 2017).

55. *Historical Trends in Federal R&D*, AM. ASS’N FOR THE ADVANCEMENT OF SCI., <https://www.aaas.org/page/historical-trends-federal-rd> (last updated Oct. 11, 2017).

cies encouraging reporting of regulatory violations, fraud, and tax evasion. In addition, they enacted and strengthened laws encouraging citizens to come forward with information revealing fraud against the government.⁵⁶

As government regulations and compliance with government contracts increasingly hit corporate bottom lines, many companies came to see trade secret protections as a tool not only to discourage commercial threats but also to manage exposure to enforcement risks. Violations of regulatory requirements, environmental standards, civil rights laws, and military specifications of government contracts—like corporate know-how and technological process advances—are not directly observable to the public or government regulators. By using NDAs to silence employees and contractors, companies could evade responsibility and control their exposure to liability. Consequently, many companies came to see trade secrets as encompassing all confidential information within the enterprise, not just technological information that could provide commercial advantage. In this way, trade secret protection was subverted from its historical and intended purposes of promoting commercial morality and technological progress.

As my initial foray into the interplay of trade secret protection and whistleblowing revealed,⁵⁷ courts recognize that disclosure of a trade secret protection for non-commercial purposes can “implicate the interest in freedom of expression or advance another significant public interest,”⁵⁸ and developed a limited privilege to disclose trade secrets.⁵⁹ This privilege, however, is murky. The Restatement (Third) of Unfair Competition notes that the exception:

depends upon the circumstances of the particular case, including the nature of the information, the purpose of the disclosure, and the means by which the actor acquired the information. A privilege is likely to be recognized, for example, in connection with the disclosure of information that is relevant to public health or safety, or to the commission of a crime or tort, or to other matters of substantial public concern.⁶⁰

This framing offers relatively little clarity or assurance to prospective whistleblowers. At a minimum, its characterization as a defense that turns on a case-by-case balancing of potentially subjective factors means that an employee or contractor who divulges proprietary information to the government could be sued for breach of an NDA. The prospective whistleblower would likely have to consult an

56. SYLVIA, *supra* note 31, § 2:9.

57. See *supra* parenthetical explanation accompanying note 44.

58. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (AM. LAW INST. 1995).

59. *Re v. Horstmann*, 1987 WL 16710, at *3 (Del. Super. Ct. Aug. 11, 1987) (recognizing a privilege to disclose to law enforcement officials trade secrets relevant to criminal fraud that had been disclosed to the defendants in confidence, citing the former Restatement); JERRY COHEN & ALAN S. GUTTERMAN, *TRADE SECRETS PROTECTION AND EXPLOITATION* (1998); JAGER, *supra* note 48, § 3:14; DAVID W. QUINTO & STUART H. SINGER, *TRADE SECRETS: LAW AND PRACTICE* § 3.02 (2d ed. 2012). The Restatement (Third) of Unfair Competition notes that, “policies underlying the privilege are similar to those supporting the numerous state and federal ‘whistleblower’ statutes that prohibit retaliatory personnel actions by employers against employees who disclose violations to public officials.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (AM. LAW INST. 1995).

60. *Id.*

attorney, with the attendant costs, and face some exposure. Moreover, most prospective whistleblowers will not even be aware of this exception to their NDA without such a consultation.

This inquiry begged the question: was this limited, murky privilege sufficient to overcome the strong forces suppressing whistleblowing by the relatively few key employees and contractors best positioned to uncover illegal activity?

B. The Interplay of Trade Secrecy and Whistleblowing

To analyze the effects of NDAs and trade secret law on whistleblowing, I turned to management and social science research on corporate onboarding practices, socialization within corporate environments, and whistleblowing. This research revealed that potential whistleblowers face a gauntlet of legal impediments, indoctrination policies, financial risks, and workplace and social pressures discouraging reporting of illegal conduct.⁶¹ As the authors of an empirical study examining 230 corporate fraud scenarios at large U.S. companies concluded, “[g]iven the costs [of whistleblowing], the surprising part is not that most employees do not talk, but that some talk at all.”⁶² These costs include not only litigation costs, but also damage to the whistleblowers’ future employment prospects. As the attorney for Jim Bingham, a former accountant who successfully blew the whistle on Xerox,⁶³ observed, “Jim had a great career, but he’ll never get a job in Corporate America again.”⁶⁴

From their first day on the job, employees and contractors are introduced to an array of legal and institutional measures intended to dissuade them from disclosing information that could adversely affect their employer. Thereafter, many companies condition employees through carrots and sticks to place the company’s profitability above all else. Employees quickly come to realize the benefits of loyalty and the professional, social, psychological, and other consequences that befall those who dare to expose corporate misdeeds. Those employees who come forward typically experience a mix of specific, tangible economic harms as well as social ostracization.

The widespread use of broad NDAs plays a central role in creating an environment in which employees and contractors feel duty-bound to stay silent about illegal activity. To ensure compliance with trade secret law, companies routinely require that corporate employees and contractors sign an NDA before they can begin work. This process is typically handled by a human resources employee who explains the terms of the agreement. Many larger enterprises use formal orientation programs. Such meetings emphasize the importance of trade secrets to the company and the breadth of the NDA. Most employees and contractors do not seek or obtain independent counsel. For the unsophisticated and the legally savvy alike, NDAs can be

61. See Jamie Darin Prekert et al., *Retaliatory Disclosure: When Identifying the Complainant Is an Adverse Action*, 91 N.C. L. REV. 889, 928 (2013).

62. Alexander Dyck et al., *Who Blows the Whistle on Corporate Fraud?*, 65 J. FIN. 2213, 2245 (2010).

63. James Bandler & Barbara Martinez, *Ex-Xerox Whistleblower Bingham Could Get Boost From Settlement*, WALL STREET J. (Apr. 2, 2002, 12:01 AM), <https://www.wsj.com/articles/SB101770190756960240>; James Bandler & Mark Maremont, *How Ex-Accountant Added Up to Trouble for Humbled Xerox*, WALL STREET J. (June 28, 2001, 12:01 AM), <https://www.wsj.com/articles/SB993674133642973302>.

64. Dyck et al., *supra* note 62, at 2245.

confusing, intimidating documents, and employees who sign them often lack any leverage to negotiate terms.

The express terms of NDAs appear to bar whistleblowing. Aside from being formal and often fairly technical, most NDAs are broadly worded.⁶⁵ They typically reference and bar the disclosure of every conceivable form of information that might be deemed confidential. Before the passage of the DTSA, NDAs did not mention any public policy exception or justification for reporting confidential information to law enforcement officials.

Such blanket framing communicates that any disclosure of confidential information to persons outside of the company would breach the agreement and thereby expose the employee or contractor to termination and liability for damages. Even though whistleblowers are unlikely to cause compensable damage by reporting illegal activity to the government or a lawyer, many will be discouraged by the strong terms of the NDA from even seeking outside counsel. They might reasonably infer from the NDA's strict and broad terms that even explaining their concerns to an attorney could potentially breach the NDA. And based on the murkiness of the former public policy exception, cautious attorneys could not provide full assurance that the whistleblower will be shielded from liability. The safest course of action for NDA signatories was to never disclose information about the company's business practices. The end result, likely intended by the company, is that NDAs foster a culture of corporate loyalty and secrecy.

Many companies reinforce the legal restrictions of NDAs with formal and informal processes aimed at integrating employees into a corporate culture that discourages both trade secret leaks and whistleblowing. For many companies, the

65. Norman D. Bishara et al., *An Empirical Analysis of Noncompetition Clauses and Other Restrictive Postemployment Covenants*, 68 VAND. L. REV. 1, 43 (2015) ("[T]he majority of firms will seek the broadest possible restrictions."). A commonly referenced NDA defines confidential information to include "all information or material that has or could have commercial value or other utility in the business." Rich Stim, *Sample Confidentiality Agreement (NDA)*, NOLO, <http://www.nolo.com/legal-encyclopedia/sample-confidentiality-agreement-nda-33343.html> (last visited Dec. 4, 2017); UCB Mfg., Inc. v. Tris Pharma, Inc., No. A-5095-10T2, 2013 WL 4516012, at *8 (N.J. Super. Ct. App. Div. Aug. 27, 2013) (stating that the confidentiality provision at issue "is not limited in terms of time, space, or scope. Rather, it sets forth an exhaustive and non-exclusive list of information that [defendant] must refrain from disclosing. Many of the descriptions in that list ... are so vague as to encompass every phase of [defendant]'s work experience."). The provision at issue in that case states:

I shall not disclose to any person, either inside the Company to employees without a need to know, or outside the Company, or use at any time, either during or after termination of employment, except as required in my duties to the Company, any secret or confidential information, whether or not developed by me, unless I shall first obtain written consent of the President of the Company or unless such information shall have become general public knowledge by any means other than disclosure by me. Secret or confidential information shall include, but not be limited to, acquisition or merger negotiations or information, know-how, designs, formulas, processes, devices, machines, inventions, research or development projects, plans for future development, materials of a business nature, financial data, legal documents and records, trade secrets, processes, formula data, techniques, know-how, improvements, inventions, marketing plans, strategies, forecasts, pricing information, customer information, work procedures, personnel and labor relations information, product specifications, financial information, models, blueprints, drawings, vendor information, proprietary information of other persons that has been disclosed to the Company and any other information of a similar nature in a form or to the extent not available to the public.

Id. at *3. The New Jersey appellate court affirmed summary judgment in favor of a pharmaceutical employee on the ground that the NDA was unenforceable due to its over breadth. *Id.* at *1. Such challenges, however, are exceedingly rare.

NDA signing occurs during a comprehensive and meticulously planned “onboarding” process aimed at inculcating loyalty and corporate pride among new employees.⁶⁶ This process can extend for months or even years.⁶⁷ The goal—or, at the least, one of the foremost goals—is to begin to mold everyday workers into fiercely loyal employees who will align their own interest with that of the company.

Once employees are onboarded, many firms reinforce loyalty through internal branding.⁶⁸ These efforts can be in the form of training sessions, expanded compensation opportunities based on employee engagement, and specifically focused evaluation criteria. The overarching goal is to create lasting bonds between the company and its workers such that employees align their thinking with that of the owners of the firm.⁶⁹ Some of these programs have been compared to religious conversions or indoctrinations into cults.⁷⁰

Those employees and contractors that report what they believe to be illegal activity face an uncertain, time-consuming, and costly legal challenge. Although various whistleblower laws ostensibly protect employees from retaliation for reporting alleged violations of law to the government,⁷¹ none prior to the DTSA expressly immunized whistleblowers who breach NDAs by reporting illegal activity to the government from trade secret liability.

While several cases have recognized a public policy protecting such whistleblowers,⁷² the contours of the defense are unclear. Courts use balancing tests to

66. TALYA N. BAUER, SHRM FOUND., ONBOARDING NEW EMPLOYEES: MAXIMIZING SUCCESS 9 (2011), <https://www.shrm.org/foundation/ourwork/initiatives/resources-from-past-initiatives/Documents/Onboarding%20New%20Employees.pdf> (last visited Dec. 4, 2017) (reporting that 93% of organizations use a new employee orientation program).

67. *Id.* at 2 (highlighting Zappos’s “intensive” onboarding course that lasts for five weeks and L’Oreal’s two-year process).

68. Marion Crain, *Managing Identity: Buying into the Brand at Work*, 95 IOWA L. REV. 1179, 1184 (2010) (“[M]anagement theorists and business consultants recommend that firms invest at least as much in internal marketing to employees – that is, selling the corporate brand inside the firm – as they do in external advertising campaigns directed at consumers. By managing employees’ identities and aligning them with the firm’s brand, employers can nurture an emotional attachment to the firm that yields a significant payoff in employee loyalty and productivity, and, ultimately, in customer satisfaction and loyalty.”).

69. *Id.* at 1200 (“Employees are persuaded to internalize brand values through a systemic recruiting, training, development, and compensation program that fosters a psychological commitment to the firm and a ‘consciousness of kind’ that translates into deeper attachment to the firm. The goal is to produce a workforce that reacts and behaves instinctively ‘on-brand,’ effectively managing itself.”).

70. *Id.* at 1212–15 (discussing internal branding efforts at Southwest Airlines and Disney) (“Disney carefully strips away other sources of identity that have negligible job relevance . . . inculcat[ing] its own special language designed to shape workers’ attitudes toward service in a way that furthers the Disney brand . . .”). *Id.* at 1214; see also Peter Waldman, *Motivate or Alienate? Firms Hire Gurus to Change Their ‘Culture’*, WALL ST. J. (July 24, 1987), <http://www.ex-cult.org/Groups/Landmark/landmark-cherries.dir/apostate/lecarchive/corptng2.htm> (“Although the efforts to transform corporate ‘cultures’ vary widely among companies, many of the programs draw heavily from motivational themes popularized by entrepreneurs like L. Ron Hubbard and Werner Erhard. Indeed, most of the programs share a common, simple goal: to increase productivity by converting worker apathy into corporate allegiance.”).

71. See, e.g., False Claims Act, 31 U.S.C. § 3730(h) (2012); Scott L. Silver & Janine D. Garlitz, *SEC Whistleblower Incentives Under the Dodd-Frank Wall Street Reform Act*, 18 PIABA B. J. 169, 171–72 (2011).

72. See U.S. ex rel. *Ruhe v. Masimo Corp.*, 929 F. Supp. 2d 1033, 1039 (Cal. Cir. 2012); U.S. ex rel. *Head v. Kane Co.*, 668 F. Supp. 2d 146, 153 (D.C. Cir. 2009); U.S. ex rel. *Grandeau v. Cancer Treatment Ctrs. of Am.*, 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004).

assess whether an exception should apply in a particular case.⁷³ The factors to be balanced vary and can be subjective.

Not only do differing tests lead to uncertain consequences for the whistleblowers who risk their livelihoods,⁷⁴ but the application of any balancing test, as opposed to a clear safe harbor, is itself problematic. Most whistleblowers considering reporting information about misconduct to the government are not represented by counsel when they need to decide what information to provide the government and are not in a position to anticipate how a court in an undetermined jurisdiction will evaluate those choices. Even if the whistleblower is represented by counsel, the lawyer will often be hard-pressed to provide definitive advice.

The decisions in *Cafasso v. General Dynamics C4 Systems*,⁷⁵ serve as a cautionary tale of the risks that whistleblowers face. While working as a Chief Scientist at General Dynamics C4 Systems (“GDC4S”), a government aerospace contractor, Mary Cafasso became aware of corporate decisions that she believed to be in violation of the company’s obligations under its government contracts.⁷⁶ She reported these concerns internally, but her warnings went unheeded.⁷⁷ Upon learning that her position was being eliminated, she hurriedly downloaded a large number of confidential files that could support her suspicions.⁷⁸ GDC4S learned of Cafasso’s removal of proprietary documents and filed suit against her in state court for breach of contract, misappropriation of trade secrets, and conversion.⁷⁹ Shortly thereafter, Cafasso filed a *qui tam* action under the False Claims Act (“FCA”).⁸⁰ GDC4S then asserted counterclaims in the federal action based on breach of the NDA, misappropriation of trade secrets, conversion, and other claims based on her removal of computer files as part of her *qui tam* action.⁸¹

After granting summary judgment in favor of GDC4S on Cafasso’s FCA action, the district court turned to GDC4S’s counterclaims.⁸² The court readily determined that Cafasso’s disclosure of the documents in question to her attorney constituted a breach of her NDA.⁸³ The court rejected a public policy privilege, noting that:

73. See *Cafasso v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1062 (9th Cir. 2011); *JDS Uniphase Corp. v. Jennings*, 473 F. Supp. 2d 697, 702 (E.D. Va. 2007); *Jefferies v. Harris Cty. Cmty. Action Ass’n*, 615 F.2d 1025, 1036 (5th Cir. 1980) (“[C]ourts have required that the employee conduct be reasonable in light of the circumstances, and have held that ‘the employer’s right to run his business must be balanced against the rights of the employee to express his grievances and promote his own welfare.’”) (internal citation omitted); see also *X Corp. v. Doe*, 805 F. Supp. 1298 (E.D. Va. 1992), *aff’d sub nom. Under Seal v. Under Seal*, 17 F.3d 1435 (4th Cir. 1994) (using a balance-of-hardship test when deciding whether to grant a preliminary injunction against the disclosure of documents by former in-house counsel filing *qui tam* claim).

74. See Joel D. Hesch, *The False Claims Act Creates a “Zone of Protection” that Bars Suits Against Employees Who Report Fraud Against the Government*, 62 *DRAKE L. REV.* 361, 367 (2014).

75. See *Cafasso v. Gen. Dynamics Sys., Inc.*, No. CV06-1381-PHX-NVW, 2009 WL 1457036 (D. Ariz. May 21, 2009).

76. *Id.* at *2–3.

77. *Id.* at *3–4.

78. *Id.* at *5–6.

79. *Id.* at *8.

80. “‘*Qui tam*’ is short for the Latin phrase *qui tam pro domino rege quam pro se ipso in hac parte sequitur*, which means ‘who pursues this action on our Lord the King’s behalf as well as his own.’” *Vt. Agency of Nat. Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 768 n.1 (2000) (citing 3 WILLIAM BLACKSTONE, COMMENTARIES *160).

81. *Cafasso*, 2009 WL 1457036, at *8.

82. *Id.* at *13.

83. *Id.* at *13–15.

[p]ublic policy does not immunize Cafasso. Cafasso confuses protecting whistleblowers from retaliation for lawfully reporting fraud with immunizing whistleblowers for wrongful acts made in the course of looking for evidence of fraud. The limitation of statutory protection for retaliation to “lawful acts done by the employee” weighs against any inference of a broad privilege for Cafasso to breach her contract with GDC4S. Statutory incentives encouraging investigation of possible fraud under the FCA do not establish a public policy in favor of violating an employer’s contractual confidentiality and nondisclosure rights by wholesale copying of files admittedly containing confidential, proprietary, and trade secret information.⁸⁴

The court granted GDC4S summary judgment on its breach of contract claim.⁸⁵ It also held that Cafasso’s actions caused irreparable harm and were not immunized by the FCA.⁸⁶ The court ordered Cafasso to pay \$300,000 in attorneys’ fees for the breach of contract action.⁸⁷

The court rejected Cafasso’s argument that such an award could deter future qui tam plaintiffs from pursuing claims on the ground that:

Cafasso’s claims under the False Claims Act and GDC4S’s breach of contract claims and counterclaims do not have a reciprocal relationship. The award poses no threat to False Claims Act plaintiffs who perform a reasonable inquiry into the facts and law underlying their claim and avail themselves of the discovery under the law.⁸⁸

Yet the breach of contract action was based in substantial part on Cafasso’s disclosure to her attorney of the proprietary documents on which she based her qui tam action.⁸⁹

The Ninth Circuit affirmed the district court rulings.⁹⁰ The court declined to adopt a public policy exception in a case involving “vast and indiscriminate appropriation” of confidential files, even for the purpose of reporting allegedly illegal activity to her attorney and to the government.⁹¹ The court emphasized the overbreadth of the document retrieval, notwithstanding that Cafasso was under tremendous time pressure in gathering the documents.⁹² The court expressed concern about the sensitivity of the information, yet it was all information that Cafasso was authorized to view.⁹³ Cafasso limited disclosure to her attorney (who was also duty-

84. *Id.* at *14.

85. *Id.* at *15.

86. *Id.*

87. *Cafasso v. General Dynamics C4 Sys.*, No. CV06-1381-PHX-NVW, 2009 WL 3723087, at *4-9. (D. Ariz. Nov. 4, 2009), *aff’d*, 637 F.3d 1047 (9th Cir. 2011). The court reduced the award of \$575,415 to \$300,000 as a result of the “possibility of extreme hardship” and Cafasso having devoted over 5,000 hours during the prior three years to the litigation and the depletion of her savings. *Id.*

88. *Id.* at *7.

89. *Cafasso*, 2009 WL 1457036, at *13.

90. *Cafasso v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047 (9th Cir. 2011).

91. *Id.* at 1062.

92. *Id.*

93. *Id.*

bound to protect the information) and the government through a sealed qui tam filing.⁹⁴ Nevertheless, the court concluded that:

[a]n exception broad enough to protect the scope of Cafasso’s massive document gather in this case would make all confidentiality agreements unenforceable as long as the employee later files a qui tam action. *See JDS Uniphase Corp. v. Jennings*, 473 F. Supp. 2d 697, 702 (E.D. Va. 2007) (“[E]mployees would feel free to haul away proprietary documents, computers, or hard drives, in contravention of their confidentiality agreements, knowing they could later argue they needed the documents to pursue suits against employers. . . .”). Were we to adopt a public policy exception to confidentiality agreements to protect relators—a matter we reserve for another day—those asserting its protection would need to justify why removal of the documents was reasonably necessary to pursue an FCA claim. Cafasso has made no such particularized showing.⁹⁵

Such a “particularized showing” puts whistleblowers in the difficult position of having to carefully screen documents, often under extreme time pressure and otherwise stressful circumstances. A whistleblower will not necessarily know what documents they will need to support a claim, and documents can be evanescent—disappearing if they are not preserved.

In another case that recognized a public policy exception for whistleblowers, the district court nonetheless allowed a counterclaim to go forward. In *Siebert v. Gene Security Network, Inc.*, the court cited *Cafasso* and concluded that enforcing a confidentiality agreement to suppress evidence of fraud would frustrate Congress’s intent in enacting the FCA—to encourage whistleblowing.⁹⁶ However, the court allowed the parties to determine through discovery if the relator took documents unrelated to the FCA claim.⁹⁷ But the prospect of potentially prevailing against a counterclaim—requiring a nonlawyer relator to establish that documents are “relevant” to a false claim—is little solace to a person contemplating reporting alleged wrongdoing to the government. Having to respond to discovery, retain counsel, and face possible liability would discourage many whistleblowers from reporting at all.

The net effect of corporate onboarding policies, broad NDAs, and murky legal standards for determining whether an employee or contractor who seeks to report allegedly illegal activities to the government is to place potential whistleblowers in a Catch-22.⁹⁸ While there are potential defenses to breach of contract and trade secret claims against whistleblowers who use proprietary information for reporting allegedly illegal activity, the prospect of having to hire a lawyer to defend against such claims has a significant deterrent effect on whistleblowers. As the *Cafasso* case illustrates, the act of sharing the allegedly incriminating information with an

94. *Id.* at 1052.

95. *Id.* at 1062.

96. *See Siebert v. Gene Sec. Network*, No. 11-cv-01987, 2013 WL 5645309, at *8 (N.D. Cal. Oct. 16, 2013).

97. *Id.*

98. Drawing on the clever plot device employed repeatedly in Joseph Heller’s 1961 blockbuster novel of the same name, a “Catch-22” is “a problematic situation for which the only solution is denied by a circumstance inherent in the problem or by a rule.” *Catch-22*, MERRIAM-WEBSTER, <http://www.merriam-webster.com/dictionary/catch%2022> (last visited Dec. 5, 2017).

attorney who is duty-bound to maintain the proprietary status of trade secret information can expose the whistleblower to liability,⁹⁹ even though the very test for assessing availability of a public policy defense requires the careful assessment that lawyers are uniquely qualified to provide.

It became clear that routine NDAs that are essential to safeguarding trade secrets can be subverted to chill those in the best position to reveal illegal activity. I next turned my attention to finding a solution to this problem that did not undermine the protection of trade secrets that promote commercial morality and technological progress.

C. Tailoring a Trade Secret Public Policy Exception

I came to realize that there were two keys to solving the trade secrecy/whistleblower puzzle. First, the empirical studies show that most whistleblowers are not interested in undermining an employer's lawful commercial advantage. They are not seeking to divulge a company's innovative process technology to competitors. Nor are they seeking to compete with the employer. Rather, they are driven by moral and social desires to prevent, halt, or rectify illegal activity. They seek to promote the social good, not something that is inconsistent with the guiding principles of trade secret protection: commercial morality and technological advance. It is ironic that a legal regime grounded in promoting commercial morality has stood in the way of ferreting out illegal activity. Such misconduct undermines commercial and social morality.

Second, existing confidentiality rules within the legal profession¹⁰⁰ and government institutions provide safeguards against disclosure of trade secrets by attorney and government officials. Government agencies routinely deal with trade secrets and follow strict rules for ensuring that this information remains confidential.¹⁰¹ The Freedom of Information Act exempts trade secrets from public disclosure.¹⁰² More generally, the federal government holds federal officers and employees strictly accountable for disclosing trade secrets to the public without authorization. The Trade Secrets Act provides that:

Whoever, being an officer or employee of the United States or of any department or agency thereof . . . publishes, divulges, discloses, or makes

99. See *supra* text accompanying notes 84–85.

100. See Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CALIF. L. REV. 1061, 1061 (1978) (observing that “[t]he attorney-client privilege may well be the pivotal element of the modern American lawyer’s professional functions.”). Attorneys representing whistleblowers are especially cognizant of the importance of maintaining the confidentiality of trade secrets. The FCA requires that complaints be filed “under seal for at least [sixty] days, and shall not be served on the defendant until the court so orders.” 31 U.S.C. § 3730(b)(2) (2012). The seal enables the government to investigate the allegations without tipping off the defendant. S. REP. NO. 99-345, at 24 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 5266, 5289.

101. See, e.g., 35 U.S.C.A. § 122 (West 2013) (requiring the U.S. Patent & Trademark Office to maintain trade secrecy of patent applications); Federal Food, Drug, and Cosmetic Act, 21 U.S.C.A. § 331(j) (West 2016) (requiring the Food and Drug Administration to maintain trade secrecy during its review of drugs); 7 C.F.R. § 200.83(c)(1) (2008) (requiring the SEC to respect confidential business information); see generally Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791, 798–818 (2011) (surveying government policies safeguarding trade secrets).

102. See 5 U.S.C.A. § 552(b)(3)–(4) (West 2016).

known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets . . . shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.¹⁰³

Furthermore, trade secret owners whose trade secrets have been violated by improper government disclosure can pursue compensatory damages through an action filed with the U.S. Court of Claims.¹⁰⁴

Thus, reporting of allegedly illegal activity by employees and contractors subject to NDAs can be reconciled with the protection of trade secret law by immunizing whistleblowers from trade secret liability so long as they maintain the secrecy of confidential information. This can be accomplished by authorizing individuals subject to NDAs to share confidential information with what I refer to as “trusted intermediaries”: government officials and attorneys legally bound to safeguard proprietary information. Thus, disclosure of even substantial amounts of proprietary information to a trusted intermediary—an attorney, court, or government official—does not jeopardize trade secrecy.

Such a regime enables potential whistleblowers to obtain legal advice without risk of liability for trade secret misappropriation. It also provides government enforcers with access to critical information about compliance with the law, government contracts, and other vital areas of public concern.

My research demonstrated the critical importance of affording potential whistleblowers with a clear safe harbor that would not expose them to the costs and risks of trade secret litigation. As the *Cafasso* case illustrated,¹⁰⁵ having to defend a trade secret misappropriation case threatens crushing liability. Apart from disclosing trade secrets to her attorney and the government under seal, the defendant in that case maintained the secrecy of the confidential information at issue.¹⁰⁶ Yet, the case resulted in costly litigation.¹⁰⁷

Therefore, I proposed that Congress *immunize* potential whistleblowers from liability, not merely codify a defense to liability. As prior case law establishes, an immunity from suit affords a defendant the ability to resolve litigation as early in the litigation as possible. The Supreme Court and all circuit courts that have addressed the procedural requirements of qualified immunity issues have held that the

103. 18 U.S.C. § 1905 (2012).

104. See *Demodulation, Inc. v. United States*, 103 Fed. Cl. 794, 813 (2012); *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984) (holding that trade secrets constitute property interests pursuant to the Takings Clause of the Fifth Amendment and finding that the EPA effected a taking of private property requiring just compensation where the agency used, pursuant to statute, confidential studies submitted by one pesticide manufacturer in evaluating similar pesticides submitted for approval by another manufacturer).

105. See *supra* text accompanying notes 75–79, 81–95.

106. *Cafasso v. Gen. Dynamics Sys., Inc.*, No. CV06-1381-PHX-NVW, 2009 WL 1457036, at *13 (D. Ariz. May 21, 2009).

107. *Cafasso v. General Dynamics C4 Sys.*, No. CV06-1381-PHX-NVW, 2009 WL 3723087, at *4–9. (D. Ariz. Nov. 4, 2009), *aff’d*, 637 F.3d 1047 (9th Cir. 2011).

immunity issue should be determined “at the earliest possible stage of the litigation.”¹⁰⁸ Furthermore, interlocutory appeals are generally available for immunities, but not defenses.¹⁰⁹

In addition, it is essential that potential whistleblowers have notice of this immunity, so they do not mistakenly interpret the broad NDA language as barring their discussing what they believe to be illegal activity with counsel and reporting of confidential information to the government through a confidential communication.

My ultimate proposed whistleblower immunity provision closely paralleled the spring 2015 exam question that inspired this project:

i. Immunity from Liability for Confidential Disclosure of Trade Secret Information to the Government: An individual who discloses information, either directly or through an attorney, in confidence to a federal, state, or local government official, or files a lawsuit or initiates a proceeding filed under seal in connection with a whistleblower program, solely for the purpose of investigating a violation of law is not subject to suit under federal or state trade secret law for that disclosure.

1. Attorney Immunity: This immunity extends to the whistleblower’s attorney so long as the attorney does not disclose or use the information outside of representing the whistleblower in reporting the alleged illegal conduct.

2. Exception: This immunity does not apply to persons who disclose or use the information for non-law enforcement purposes, such as starting a competing business or communicating the trade secret information to the press.

ii. Use of Trade Secret Information in Anti-Retaliation Lawsuit: A person bringing a lawsuit for retaliation by an employer for reporting any violation of law including fraud against the government may disclose the

108. *Anderson v. Creighton*, 483 U.S. 635, 646 (1987) (“[Q]ualified immunity questions should be resolved at the earliest possible stage of a litigation.”); *Hegarty v. Somerset Cty.*, 25 F.3d 17, 18 (1st Cir. 1994); *Meredith v. Fed. Mine Safety & Health Review Comm’n*, 177 F.3d 1042, 1051 (D.C. Cir. 1999); *X-Men Sec., Inc. v. Pataki*, 196 F.3d 56, 65–67 (2d Cir. 1999); *Thomas v. Indep. Twp.*, 463 F.3d 285, 300 (3d Cir. 2006); *Backe v. LeBlanc*, 691 F.3d 645, 648–49 (5th Cir. 2012); *Skousen v. Brighton High Sch.*, 305 F.3d 520, 526–27 (6th Cir. 2002); *Landstrom v. Ill. Dep’t of Children & Family Servs.*, 892 F.2d 670, 674 (7th Cir. 1990); *Solomon v. Petray*, 795 F.3d 777, 791 (8th Cir. 2015); *Little v. City of Seattle*, 863 F.2d 681, 685 (9th Cir. 1988); *Harbert Int’l, Inc. v. James*, 157 F.3d 1271, 1280–81 (11th Cir. 1998). Similarly, circuit courts addressing the procedures appropriate for adjudicating sovereign immunity under the Foreign Sovereign Immunities Act, 28 U.S.C. § 1609, have consistently dictated procedures that ensure that the immunity issue is decided early in the litigation. *See In re Papandreou*, 139 F.3d 247, 252 (D.C. Cir. 1998); *Filus v. Lot Polish Airlines*, 907 F.2d 1328, 1332 (2d Cir. 1990); *Kelly v. Syria Shell Petroleum Dev. B.V.*, 213 F.3d 841, 849 (5th Cir. 2000); *Rubin v. The Islamic Republic of Iran*, 637 F.3d 783, 795 (7th Cir. 2011); *Alpha Therapeutic Corp. v. Nippon Hoso Kyokai*, 199 F.3d 1078, 1087–88 (9th Cir. 1999), *withdrawn sub nom. Alpha Therapeutic Corp. v. Kyokai*, 237 F.3d 1007 (9th Cir. 2001); *Hansen v. PT Bank Negara Indonesia (Persero)*, TBK, 601 F.3d 1059, 1063–64 (10th Cir. 2010); *Butler v. Sukhoi Co.*, 579 F.3d 1307, 1314 (11th Cir. 2009).

109. *Plumhoff v. Rickard*, 134 S. Ct. 2012, 2019 (2014) (“[P]retrial orders denying qualified immunity generally fall within the collateral order doctrine.”).

trade secret information to their attorney and use the trade secret information in the court proceeding so long as they file the information under seal and do not disclose the information except pursuant to court order.

iii. Notice: All non-disclosure agreements (NDAs) must include reasonable notice of the public policy safe exception set forth in clauses (i) and (ii). Notice of clauses (i) and (ii) in NDAs is a prerequisite for enforcing these agreements in federal courts. Failure to provide notice of the public policy exception shall bar recovery of exemplary damages and attorneys' fees in any trade secret misappropriation action.

V. LEGISLATIVE HISTORY OF THE DTSA WHISTLEBLOWER IMMUNITY PROVISION

I completed a draft of "Tailoring a Public Policy Exception to Trade Secret Protection" in early November 2015, just as I was heading to Washington, D.C. for an annual patent law conference that I co-organize with Georgetown University Law Center ("GULC").¹¹⁰ I uploaded the trade secret article on the Social Science Research Network website¹¹¹ just before heading to the airport.

As I stepped down from the stage after moderating the opening panel of the GULC-BCLT (Berkeley Center for Law & Technology) Seventh Annual Patent Law and Policy Conference, I was greeted by a member of the Senate Judiciary Committee staff. She asked if I had a few minutes to discuss some pending legislation. I asked her what aspects of *patent reform* she had in mind. To my surprise, she said that she was interested in discussing the DTSA. I learned that the DTSA was moving through the legislative process, Senators Leahy and Grassley were interested in addressing the whistleblower problem, and the Senate Judiciary Committee staff was intrigued by the approach set forth in my draft article. We exchanged email addresses and agreed to communicate the following week.

Within a few days of the GULC-BCLT Patent Law Conference, the Senate Judiciary Committee staff vetted a whistleblower immunity provision modeled on the proposal in my article among DTSA stakeholders. In early January 2016, I forwarded a commentary that I had posted on Columbia Law School's Blue Sky Blog.¹¹² The Judiciary Committee provided me with a draft of the whistleblower immunity amendment that Senators Leahy and Grassley planned to introduce later that month. The language implemented nearly verbatim, the core elements of my proposal. I was especially pleased to see that staff had framed the provision as "immunity" from liability and not merely a defense to liability. We discussed ensuring that the provision applied to anyone, whether an employee or a contractor, who signs an NDA.

110. See *The Seventh Annual Patent Law and Policy Conference*, GEO. L. (Nov. 6, 2015), <https://www.law.georgetown.edu/continuing-legal-education/programs/academic-conferences/patent-law.cfm>.

111. See Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, SSRN (Nov. 5, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2686565.

112. See Peter S. Menell, *Detering Corporate Fraud from the Inside: Encouraging Whistleblowing Without Jeopardizing Trade Secrecy*, COLUM. L. SCH.: BLUE SKY BLOG (Jan. 5, 2016), <http://clsbluesky.law.columbia.edu/2016/01/12/detering-corporate-fraud-from-the-inside-encouraging-whistleblowing-without-jeopardizing-trade-secrecy/>.

On January 28, 2016, the Senate Judiciary Committee convened to consider the DTSA.¹¹³ After Senator Orrin Hatch introduced a substitute version of the DTSA, Senator Leahy introduced a whistleblower immunity amendment co-authored by Senator Grassley:

SEC. __. IMMUNITY FROM LIABILITY FOR CONFIDENTIAL DISCLOSURE OF A TRADE SECRET TO THE GOVERNMENT OR IN A COURT FILING.

(a) AMENDMENT.—Section 1833 of title 18, United States Code, is amended—

(1) by striking “This chapter” and inserting

(a) IN GENERAL.—This chapter”;

(2) in subsection (a)(2), as designated by paragraph (1), by striking “the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation” and inserting “the disclosure of a trade secret in accordance with subsection (b)”;

(3) by adding at the end the following:

(b) IMMUNITY FROM LIABILITY FOR CONFIDENTIAL DISCLOSURE OF A TRADE SECRET TO THE GOVERNMENT OR IN A COURT FILING.—

(1) IMMUNITY.—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.

(2) USE OF TRADE SECRET INFORMATION IN ANTI-RETALIATION LAWSUIT.—An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual—

(A) files any document containing the trade secret under seal; and

(B) does not disclose the trade secret, except pursuant to court order.

(3) NOTICE.—

(A) IN GENERAL.—An employer shall provide notice of the immunity set forth in this subsection in any contract or agreement with an employee that governs the use of a trade secret or other confidential information.

(B) POLICY DOCUMENT.—An employer shall be considered to be in compliance with the notice requirement in subparagraph (A) if the employer provides a cross-reference to a policy document provided to

113. See Comm. on the Judiciary, *Executive Business Meeting*, U.S. SENATE (Jan. 28, 2016), <https://www.judiciary.senate.gov/meetings/executive-business-meeting-01-28-16>.

the employee that sets forth the employer's reporting policy for a suspected violation of law.

(C) NON-COMPLIANCE.—If an employer does not comply with the notice requirement in subparagraph (A), the employer may not be awarded exemplary damages or attorney fees under subparagraph (C) or (D) of section 1836(b)(3) in an action against an employee to whom notice was not provided.

(D) APPLICABILITY.—This paragraph shall apply to contracts and agreements that are entered into or updated after the date of enactment of this subsection.

(4) EMPLOYEE DEFINED.—For purposes of this subsection, the term 'employee' includes any individual performing work as a contractor or consultant for an employer.

(5) RULE OF CONSTRUCTION.—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.”.

(c) TECHNICAL AND CONFORMING AMENDMENT.—Section 1838 of title 18, United States Code, is amended by striking “This chapter” and inserting “Except as provided in section 1833(b), this chapter.”¹¹⁴

Senators Leahy, Grassley, and Diane Feinstein explained the amendment in the following discussion:

Senator Leahy: “My amendment along with Senator Grassley ensures that companies do not intimidate whistleblowers by threatening them with laws for trade secret theft. Now Senator Grassley and I have worked together for years and years on whistleblower efforts and I am glad to continue the work. I have two letters of support that I would like to include for the record from the supporter groups.”

Senator Grassley: “[They] will be included.”

Senator Leahy: “[The amendment] is carefully written to ensure that the disclosures are protected or that they are made to law enforcement in confidence or filed with a court under seal. They do not protect unlawful activities. I think that it is a good amendment and I would move its adoption.

Senator Grassley: “And I have a statement in favor [of the amendment] that I will put in the record without objection. Those in favor of the amendment . . .

Senator Feinstein: “May I say one thing about this amendment.”

Senator Grassley: “Yes, please.”

114. See S. 1890, 114th Cong. (2016) (proposed amendment to Chapter 90 of Title 18 of the U.S. Code), <https://www.judiciary.senate.gov/imo/media/doc/Leahy-Grassley1%20-%20ALB16037.pdf>. In addition, Senator Leahy submitted a statement into the record stating in pertinent part:

I appreciate that the bill's sponsors worked with me to improve this legislation, which is critical for Vermont businesses. I also thank Chairman Grassley for working with me 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, provided they do so under seal. Our amendment is supported by the Government Accountability Project and the Project on Government Oversight (POGO), and I look forward to its adoption.

Executive Business Meeting, supra note 4.

Senator Feinstein: “I think that this amendment is really important. As I understand it, it doesn’t mean that the person is protected for actions that are otherwise prohibited by law, such as hacking. And I think that it is important for the record to point out.”¹¹⁵

The letters of support were submitted by the Project on Government Oversight (“POGO”)¹¹⁶ and the Government Accountability Project (“GAP”),¹¹⁷ organizations committed to rooting out corruption, promoting good government, and protecting whistleblowers within the federal government and its contractors. POGO’s letter of support praised the whistleblower immunity amendment for “explicitly protect[ing] whistleblowers who disclose trade secrets confidentially to the government or in a lawsuit filed under seal.”¹¹⁸ The letter goes on to emphasize that “[m]aking sure these whistleblowers are free to come forward without fear of retaliation or of prosecution for trade secret theft is an important and necessary clarification, given the current interpretation of relevant law.”¹¹⁹

GAPS’s letter characterized the amendment as providing “immunity for judicially-controlled disclosures of trade secrets to court in relevant lawsuits.”¹²⁰ GAP noted that the provision’s “approach to responsibly completing the record is consistent with Whistleblower Protection Act boundaries, and it should contribute to justice.”¹²¹ The GAP letter emphasized that “the amendment’s impact could be ground breaking” for “whistleblower rights advocates.”¹²²

Our nation has 58 whistleblower laws for public and private sector employees, more than any other country. But all limit protection to employment retaliation. As a result, as employment rights have strengthened, government agencies increasingly have shifted to criminal investigations and sometimes prosecutions as the most common forms of harassment.

115. *Id.* (indicating that this discussion begins at 48:48 and concludes at 50:52).

116. *About POGO*, PROJECT ON GOV’T OVERSIGHT, <http://www.pogo.org/about/> (last visited Dec. 5, 2017) (“Founded in 1981, POGO originally worked to expose outrageously overpriced military spending on items such as a \$7,600 coffee maker and a \$435 hammer. In 1990, after many successes reforming military spending, including a Pentagon spending freeze at the height of the Cold War, POGO decided to expand its mandate and investigate waste, fraud, and abuse throughout the federal government. Throughout its history, POGO’s work has been applauded by Members of Congress from both sides of the aisle, federal workers and whistleblowers, other nonprofits, and the media.” POGO “is a nonpartisan independent watchdog that champions good government reforms. POGO’s investigations into corruption, misconduct, and conflicts of interest achieve a more effective, accountable, open, and ethical federal government.”).

117. GOV’T ACCOUNTABILITY PROJECT, *Our History and Mission*, <https://www.whistleblower.org/our-history-and-mission> (last visited Dec. 3, 2017) (“Our mission is to ensure government and corporate accountability by advancing occupational free speech, defending whistleblowers and presenting their verified concerns to appropriate officials, groups, or journalists. GAP has become not only the most prominent whistleblower support organization, but also an important government and corporate accountability organization both domestically and internationally.”).

118. Letter from Danielle Brian, Exec. Dir., Project on Gov’t Oversight, to Chuck Grassley, Chair, U.S. Senate, & Patrick Leahy, Ranking Member, U.S. Senate (Jan. 19, 2016) (on file with the University of Missouri School of Law Business, Entrepreneurship & Tax Law Review).

119. *Id.*

120. Letter from Tom Devine, Legal Dir., Gov’t Accountability Project, to Charles Grassley, Chair, U.S. Senate, & Patrick Leahy, Ranking Member, U.S. Senate (Jan. 20, 2016) (on file with the University of Missouri School of Law Business, Entrepreneurship & Tax Law Review).

121. *Id.*

122. *Id.*

Corporations have turned to well-financed litigation ‘slap suits’ seeking bankruptcy and financial ruin, to achieve a greater chilling effect than merely firing a whistleblower.

The narrow U.S. boundaries to protect freedom of speech have become highly outdated. Almost half the world’s whistleblower laws in twelve other nations, from Australia to Serbia, now protect against civil or criminal liability. Expanding the scope of protection beyond employment harassment is necessary for whistleblower laws to remain relevant. You have GAP’s commitment to help advocate that principle not only with trade secrets, but any other context where the truth through whistleblowing can make a difference.¹²³

Immediately following this discussion, the Committee unanimously approved the amendment. Later that day, Senator Leahy released the following statement:

Leahy-Grassley Amendment to Protect Whistleblowers Earns Unanimous Support In Judiciary Committee

WASHINGTON (Thursday, January 28, 2016) – The Senate Judiciary Committee on Thursday unanimously approved an amendment coauthored by U.S. Senators Patrick Leahy (D-Vt.) and Chuck Grassley (R-Iowa) to ensure that companies cannot intimidate whistleblowers by threatening them with lawsuits for trade secret theft.

Leahy and Grassley have long worked together to strengthen whistleblower protections. Their amendment, which was added to the bipartisan Defend Trade Secrets Act, protects whistleblowers who share confidential information in the course of reporting suspected illegal activity to law enforcement or when filing a lawsuit, provided they do so under seal.

“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,” Ranking Member Leahy said.

“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,” Chairman Grassley said.

The Leahy-Grassley amendment is supported by the Government Accountability Project and the Project on Government Oversight (POGO).

The Defend Trade Secrets Act, coauthored by Senator Orrin Hatch (R-Utah) and Senator Chris Coons (D-Del.) was unanimously approved by

123. *Id.*

the committee. Results and a webcast of Thursday's executive business meeting can be found online.¹²⁴

The final version of the DTSA incorporated the Grassley-Leahy whistleblower immunity provision amendment verbatim.¹²⁵ The Senate Report accompanying the legislation explains that:

Sec. 7. Immunity [F]rom [L]iability for [C]onfidential [D]isclosure of a [T]rade [S]ecret to the Government or in a [C]ourt [F]iling

Section 7 of the Act amends § 1833 of title 18 by adding a new subsection (b). The new § 1833(b)(1) provides for criminal and civil immunity for anyone who discloses a trade secret under two circumstances. Subparagraph (A) addresses disclosures in confidence to a Federal, State, or local government official, or to an attorney, for the purpose of reporting or investigating a suspected violation of the law. Subparagraph (B) applies to disclosure in a complaint or other document filed under seal in a judicial proceeding. The Committee stresses that this provision immunizes the act of disclosure in the limited circumstances set forth in the provision itself; it does not immunizes [sic] acts that are otherwise prohibited by law, such as the unlawful access of material by unauthorized means.

Section 1833(b)(2) created by this Act provides that an individual who files a lawsuit against an employer for retaliation for reporting a suspected violation of the law may disclose a trade secret to an attorney for use in the proceeding, provided the individual files any document containing the trade secret under seal and does not disclose the trade secret other than pursuant to a court order.

Section 1833(b)(3) requires notice of the immunity in this subsection to be set forth in any employment contract that governs the use of trade secrets, although an employer may choose to provide such notice by reference to a policy document setting forth the employer's reporting policy for a suspected violation of the law that provides notice of the immunity. An employer may not be awarded exemplary damages or attorney's fees under this Act against an employee to whom such notice was not provided. The notice requirements apply to contracts entered into or updated after the date of enactment of this subsection.

Section 1833(b)(4) defines the term 'employee' to include any individual performing work as a contractor or consultant.¹²⁶

On April 4, 2016, the Senate passed the DTSA on a unanimous vote.¹²⁷ Senator Leahy's remarks on the Senate floor that day summarized the whistleblower immunity provision's rationale and notes a source for its approach and language:

124. Press Release, *supra* note 4.

125. Defend Trade Secrets Act, Pub. L. 114-153, § 7, 130 Stat. 376, 384–85 (2016) (to be codified at 18 U.S.C. § 1833).

126. S. REP. NO. 114-220, at 13 (2016). The House Report contains identical explanatory language. *See* H.R. REP. NO. 114-529, at 16–17 (2016).

127. Richard Cowan & Andrew Chung, *Senate Unanimously Approves Trade Secret Bill*, REUTERS (Apr. 4, 2016, 12:53 PM), <https://www.reuters.com/article/us-usa-trade-secrets/senate-unanimously-approves-trade-secrets-bill-idUSKCN0X11Y3>.

Today, the Senate voted on legislation that will provide a valuable tool to protect against trade secret theft. This legislation is supported by businesses from diverse sectors of our economy, including companies large and small. . . . The Defend Trade Secrets Act contains a bipartisan provision I offered with Senator Grassley to ensure that employers and other entities cannot bully whistleblowers or other litigants by threatening them with a lawsuit for trade secret theft. The provision protects disclosures made in confidence to law enforcement or an attorney for the purpose of reporting a suspected violation of law and disclosures made in the course of a lawsuit, provided that the disclosure is made under seal. It requires employers to provide clear notice of this protection in any nondisclosure agreements they ask individuals to sign. This commonsense public policy amendment is supported by the Project on Government Oversight and the Government Accountability Project and builds upon valuable scholarly work by Professor Peter Menell.¹²⁸

On April 27, 2017, the House of Representatives passed the DTSA by a margin of 410 to 2.¹²⁹ President Obama signed the DTSA into law on May 11, 2016.¹³⁰

VI. INTERPRETING THE WHISTLEBLOWER IMMUNITY PROVISION

As reflected in the foregoing legislative history, Congress built the DTSA's whistleblower immunity provision on the scholarly foundation laid in "Tailoring a Public Policy Exception to Trade Secret Protection."¹³¹ Hence, companies, whistleblowers, counsel, and courts can best understand the meaning, scope, and intention behind the immunity provision by reference to the analysis set forth in that article.

Most importantly, the whistleblower immunity provision is structured as an *immunity* and not a defense. By characterizing the safe harbor as an immunity, Congress shifted the law and legal process from the employer's advantage to the employee and the public's advantage. The immunity is based on the concern that corporations can "bully" and deter potential whistleblowers through the threat of costly trade secret litigation.¹³² Hence, courts should allocate the burden of proof on the trade secret owner seeking to impose liability on a potential whistleblower and resolve the applicability of the immunity provision expeditiously.

Bare allegations that a current or former employee or contractor possesses trade secret information and might disclose such information to the press or a competitor is not a sufficient basis for allowing a trade secret action to proceed. Nor is the assertion that the defendant is unaware that the former employee has provided any information to the government a sufficient basis to allow a trade secret action to proceed. The False Claims Act, the Dodd–Frank Act, and various other whistle-

128. 162 CONG. REC. S1636 (2016) (statement of Sen. Leahy).

129. Jacob Gershman, *Congress May Be About to Shake Up Trade Secret Law: Is That a Good Thing?*, WALL STREET J. (Apr. 27, 2016, 4:24 PM), <https://blogs.wsj.com/law/2016/04/27/congress-may-be-about-to-shake-up-trade-secret-law-is-that-a-good-thing/>.

130. The White House, *supra* note 2.

131. See Menell, *supra* note *.

132. 162 CONG. REC. S1636 (2016).

blower statutes and protections specifically authorize the government and whistleblowers to investigate potential violations of law without the knowledge or interference of the target company.¹³³

Thus, the court's role at the outset of a trade secret case is to decide whether immunity applies, with due regard for the DTSA's protected activities and public purposes. Where the employee asserts under oath that she or he disclosed company documents to government officials or an attorney in confidence solely for the purpose of reporting or investigating a suspected violation of law, the DTSA whistleblower regime requires the employer-trade secret owner to come forward with concrete evidence that the employee or contractor has shared trade secret information outside of the protected categories or for an impermissible purpose. Absent such evidence, the employee or contractor remains free to work with counsel to investigate and report alleged violations of law and immune from suit for trade secret violations.¹³⁴

Furthermore, although the DTSA whistleblower immunity provision does not bar suit for a violation of the Computer Fraud and Abuse Act ("CFAA"), theft, trespass, or hacking,¹³⁵ the scope of the DTSA whistleblower immunity provision extends to trade secret-based harms. Thus, companies cannot impose trade secret damages on a potential whistleblower who falls within the DTSA immunity ambit through a theft or trespass cause of action. If DTSA immunity applies, then the harm in such other causes of action is limited to the cost of the paper, ink, or laptop computer that was allegedly stolen or damaged, and cannot extend to the value associated with information contained on such media or device. Otherwise, the very chilling effects that Congress sought to prevent through the DTSA whistleblower immunity provision would be circumvented through these other causes of action.

133. See 31 U.S.C. § 3730(b)(2) (2012) ("The complaint shall be filed in camera, shall remain under seal for at least 60 days, and shall not be served on the defendant until the court so orders."); 15 U.S.C. § 78u-6(h)(2) (2012) (subject to certain exceptions "the Commission and any officer or employee of the Commission shall not disclose any information, including information provided by a whistleblower to the Commission, which could reasonably be expected to reveal the identity of a whistleblower" and requiring other regulatory entities with which information is shared to also maintain the confidentiality of information).

134. Unfortunately, the first reported case to address the DTSA whistleblower immunity provision improperly treated the safe harbor as a defense. See *Unum Group v. Loftus*, 220 F. Supp. 3d 143, 147 (D. Mass. 2016); Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, 1 NEV. L. REV. F. 92, 97 (2017).

135. See 18 U.S.C.A. § 1833(b)(5) (West 2016). Indeed, civil and even criminal allegations under the CFAA are sometimes raised when no actual "hacking" is involved. This practice was questioned by the Ninth Circuit where the court interpreted the CFAA narrowly, emphasizing that the text and legislative history of the CFAA suggest its "general purpose is to punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets." *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012). This view was adopted by the Fourth Circuit where the court declined "to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012). Although the proper interpretation of the CFAA in this context is still a matter of controversy (including a circuit split), and beyond the scope of this article, the logic of the DTSA whistleblower immunity provision extends to circumstances in which an employer asserts criminal or civil liability under the CFAA based on an employee breach of contractual restrictions.