California Law Review

VOL. 105 FEBRUARY 2017 NO. 1

Tailoring a Public Policy Exception to Trade Secret Protection

Peter S. Menell*

The growing importance of information resources as well as mounting threats to proprietary information in the digital age propelled federalization of trade secret protection onto the national legislative agenda during the past year. This salience provided a propitious opportunity to address a critical, overlooked failing of trade secret protection: the lack of a clear public policy exception to foster reporting of illegal activity. The same routine nondisclosure agreements that are essential to safeguarding trade secrets can be and are used to chill those in the best position to reveal illegal activity. Drawing on classic law enforcement scholarship as well as established institutions for protecting proprietary information, this Article proposes a sealed disclosure/trusted intermediary exception to trade secret protection. This approach safeguards trade secrets while promoting effective law enforcement. The Article also recommends that nondisclosure agreements prominently include notice of the law reporting safe harbor to ensure that those with

DOI: http://dx.doi.org/10.15779/Z388Z8Q

* Koret Professor of Law and Director, Berkeley Center for Law & Technology, University of California, Berkeley, School of Law. I thank Michael Birnhack, Thomas Cotter, Amos Israel, Mark Lemley, Gideon Parchomovsky, James Pooley, Claire Sylvia, and participants at workshops at Bar Ilan University, Harvard Law School, and the Bay Area IP Scholarship group for comments on this project. I also thank Andrea Hall and Matthew Malady for excellent research assistance.

An earlier draft of this Article attracted the attention of congressional staff members working on the Defend Trade Secrets Act of 2016. Section 7 of that legislation ("Immunity from Liability for Confidential Disclosure of a Trade Secret to the Government or in a Court Filing") implements the proposals set forth in this Article. I thank Alexandra Givens for reaching out to me.

knowledge of illegal conduct are aware of this important public policy limitation on nondisclosure agreements and exercise due care with trade secrets in reporting illegal activity. Based on an earlier draft of this Article, Congress adopted a whistleblower immunity provision as part of the Defend Trade Secrets Act of 2016.

INTRODUCTION

Trade secrets are the most pervasive form of intellectual property in the modern economy.[1] Nearly every enterprise—whether for-profit or not—seeks to protect information about its operations, strategy, technology, funding, personnel, and customers. Employers of all types routinely require their employees and contractors to sign restrictive nondisclosure agreements (NDAs)[2] and return confidential information upon their departure or completion of services.[3] Without such restrictions, these enterprises would jeopardize trade secret protection[4] and risk violating privacy and other laws.[5]

Notwithstanding their national importance and unlike patent, copyright, and trademark protection, trade secrets have been protected principally through state law.[6] Although most states have adopted a version of the Uniform Trade Secrets Act (UTSA),[7] there remain significant differences among state regimes as well as variations in state court systems.[8]

The confluence of an increasingly high-technology economy and rising international commercial espionage put trade secret protection on the national legislative agenda.[9] The bipartisan Defend Trade Secrets Act of 2015

---

1. *See* James Pooley, *Trade Secrets: The Other IP Right*, WIPO MAG., no. 3, June 2013, at 2.

2. A typical NDA bars employees and contractors from disclosing any confidential information, except to the extent necessary to the performance of their assigned duties, and requires that they make best efforts to safeguard confidential information against disclosure, misuse, espionage, loss, or theft. *See* JERE M. WEBB, A PRACTITIONER'S GUIDE TO CONFIDENTIALITY AGREEMENTS § X(A)–(D) (1985); *infra* text accompanying notes 210–11.

3. A typical agreement requires the employee or contractor to return all materials or copies of confidential materials to the employer promptly upon termination of employment. *See* WEBB, *supra* note 2, § X(G).

4. Trade secret law requires that companies make reasonable efforts to maintain trade secrecy. *See* UNIF. TRADE SECRETS ACT § 1(D)(ii) (UNIF. LAW COMM'N 1985).

5. *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW (5th ed. 2014) (surveying information privacy law).

6. Congress authorized federal prosecutors to pursue criminal trade secret actions in 1996. *See* James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177 (1997). Although there has been an uptick in federal economic espionage prosecutions, *see* Gary S. Lincenberg & Peter J. Shakow, *The Rise of Economic Espionage Prosecutions and How to Litigate Them*, 29 CRIM. JUST. 14 (2014), the bulk of trade secret enforcement occurs in civil proceedings pursuant to state law.

7. Only New York, North Carolina, and Massachusetts have not adopted the UTSA. North Carolina has a similar statutory regime, whereas New York and Massachusetts protect trade secrets under common law. *See infra* note 76.

8. States are not required to pass the UTSA verbatim and some states have made amendments. *See, e.g.*, CAL. CIV. CODE § 3426 (2016).

9. *See* EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS 8 (2013), http://www.whitehouse.gov/blog/2013/02/19/launch-

(DTSA)[10] sought to amend the Economic Espionage Act (EEA) to provide a private civil cause of action to enforce the EEA[11] and authorize enforcement of violations of state trade secret protections "related to a product or service used in, or intended for use in, interstate or foreign commerce" in federal court. The DTSA also sought to strengthen trade secret enforcement by authorizing federal courts to grant ex parte orders for preservation of evidence and seizure of any property used to commit or facilitate a violation of the statute.[12]

Proposals to federalize trade secret enforcement attracted broad support from business and innovation groups. Proponents pointed to the need for a unified national regime and for a federal forum to combat rising domestic and international threats to trade secret protection in the digital age.[13] In his press release announcing the 2014 version of the DTSA, Senator Coons explained:

---

administration-s-strategy-mitigate-theft-us-trade-secrets [https://perma.cc/JB3N-8275]; COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 1 (2013), http://www.ipcommission.org/report/ip_commission_report_052213.pdf [https://perma.cc/K4SQ-APSL] ("The scale of international theft of American intellectual property (IP) is unprecedented—hundreds of billions of dollars per year. . . ."); OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE 4 (2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [https://perma.cc/PKH5-KGT7] ("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 COMM'N, CHINA: EFFECTS OF INTELLECTUAL PROPERTY INFRINGEMENT AND INDIGENOUS INNOVATION POLICIES ON THE U.S. ECONOMY, at xiv (2011), http://www.usitc.gov/publications/332/pub4226.pdf [https://perma.cc/4FZP-L5EC] (estimating that in 2009, U.S. firms lost between $14.2 billion and $90.5 billion due to intellectual property infringement in China).

10. *See* Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. (2015); S. 1890, 114th Cong. (2015). As of November 4, 2015, H.R. 3326 had sixty-five cosponsors, forty-five Republican and twenty Democrat, and S. 1890 had ten cosponsors, six Republican and four Democrat. *See Cosponsors: H.R. 3326*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/3326/cosponsors [https://perma.cc/9WZZ-4HNE]; *Cosponsors: S. 1890*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/senate-bill/1890/cosponsors [https://perma.cc/N46L-E27Z].

11. *See* 18 U.S.C. § 1831(a) (2012) (economic espionage to benefit "any foreign government, foreign instrumentality, or foreign agent"); *id.* § 1832(a) (trade secret violations).

12. *See* H.R. 3326 § 2(a). The legislation also provides for treble exemplary damages for willful and malicious misappropriation. The UTSA limits exemplary damages to double the amount of damages. *See* UNIF. TRADE SECRETS ACT § 3(b) (UNIF. LAW COMM'N 1985).

13. *See* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 66–67 (2011) (finding relatively modest growth in reported state appellate trade secret decisions and suggesting that the federal courts are better equipped to harmonize and enforce trade secret protection); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 301–02 (2010) (reporting exponential growth of trade secret enforcement in federal courts from 1980 through 2009); David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769 (2009); Eric Goldman, *Congress Is Considering a New Federal Trade Secret Law. Why?*, FORBES (Sept. 17, 2014), http://www.forbes.com/sites/ericgoldman/2014/09/16/congress-is-considering-a-new-federal-trade-secret-law-why [https://perma.cc/3NWP-PJXJ]; Press Release, Congressman George Holding, Congressman Holding Introduces Bipartisan Trade Secrets Protection Act of 2014 (July 29, 2014), https://holding.house.gov/media-center/press-releases/congressman-holding-introduces-bipartisan-trade-secrets-protection-act [https://perma.cc/TNV3-8DT3]; Press Release, The Software Alliance, BSA Applauds Introduction of Trade Secrets Legislation in the House (July 28, 2014),

> In today's electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. These losses put U.S. jobs at risk and threaten incentives for continued investment in research and development. Current federal criminal law is insufficient.[14]

Opposition was limited, and it focused primarily on concerns that federalization of trade secret protection and enforcement might jeopardize state experimentation and expand remedies without adequate justification.[15]

The debate had, until recently,[16] overlooked a critical failing of trade secret protection. Unlike patent,[17] copyright,[18] trademark,[19] and right of publicity regimes,[20] trade secret law has lacked any express exceptions or

---

http://www.bsa.org/news-and-events/news/2014/july/us07292014tradesecrets [https://perma.cc/E936-R9EB].

14. Press Release, Senator Christopher Coons, Hatch, Coons Introduce Bill to Combat Theft of Trade Secrets, Protect Jobs (Apr. 29, 2014), http://www.hatch.senate.gov/public/index.cfm/2014/4/hatch-coons-introduce-bill-to-combat-theft-of-trade-secrets-protect-jobs [https://perma.cc/QH23-C55X].

15. *See* Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172 (2014); David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L.R. ONLINE 230 (2015); David S. Levine & Sharon K. Sandeen, *Open Letter to the Sponsors of the Revised Defend Trade Secrets Act*, CTR. FOR INTERNET & SOC'Y (Aug. 3, 2015), http://cyberlaw.stanford.edu/publications/open-lettersponsors-revised-defend-trade-secrets-act [https://perma.cc/K3YG-QUJ3]; *cf.* Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317 (2015) (questioning the need for full federalization of trade secret law and advocating expansion of federal courts' jurisdiction over state law trade secret claims). *But see* James Pooley, *The Myth of the Trade Secret Troll: Why We Need a Federal Civil Claim for Trade Secret Misappropriation*, 23 GEO. MASON L. REV. 1045 (2016).

16. *See* James Pooley, *New Federal Trade Secret Law Would Protect Whistleblowers*, LAW.COM (Feb. 5, 2016), http://www.law.com/sites/lawcomcontrib/2016/02/05/new-federal-trade-secret-law-would-protect-whistleblowers [https://perma.cc/8HWX-9ZNQ] (noting that the whistleblower amendment to the DTSA originated in a draft version of this Article circulated in the fall of 2015).

17. *See, e.g.*, 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, 351–52 (1863) (repair doctrine); Whittemore v. Cutter, 29 F. Cas. 1120 (C.C.D. Mass. 1813) (common law experimental use).

18. *See, e.g.*, 17 U.S.C. § 107 (2012) (copyright fair use); *id.* § 109 (first sale doctrine); *id.* §§ 110–22 (various copyright exceptions, limitations, and compulsory licenses).

19. *See, e.g.*, 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 noncommercial 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).

20. *See, e.g.*, CAL. CIV. CODE § 3344(d) (2016) (exempting any news, public affairs, or sports broadcast or account, or any political campaign use from liability for violation of California's statutory right of publicity).

defenses.[21] The effort to federalize trade secret protection created a propitious opportunity to rectify the lack of a clear public policy exception needed to prevent concealment of illegal activity.

The tobacco industry's effort to silence Dr. Jeffrey Wigand illustrates the importance of a clear safe harbor to protect those who report allegedly illegal activity. Dr. Wigand, a former tobacco company executive, played a key role in bringing the industry's deception about the dangers of tobacco products to light. After earning a Ph.D. in biochemistry and working in various research positions in the health care industry, Dr. Wigand became Vice President for Research and Development at Brown & Williamson Tobacco Corporation, a major cigarette manufacturer, in 1988. He believed that he would be leading an effort to develop a "safer cigarette."[22] In the course of his work, he became aware that his employer was misleading federal regulators as to the health dangers of its products. Instead of creating safe cigarettes, Brown & Williamson was manipulating nicotine content to increase tobacco addiction. Brown & Williamson fired Dr. Wigand in 1992, reportedly for being "difficult to work with" and for "talking too much."[23]

When Dr. Wigand sought to expose what he believed to be illegal conduct by his former employer and advise the Department of Justice and the Food & Drug Administration about the industry's practices, Brown & Williamson invoked NDAs to block Dr. Wigand's testimony. The company persuaded a Kentucky court to issue a temporary restraining order barring Dr. Wigand from disclosing any information relating to his work at Brown & Williamson.[24] Although the restraining order was eventually lifted as part of a landmark national tobacco settlement,[25] Dr. Wigand risked tremendous liability for reporting illegal conduct.[26] His courage led to much-needed, far-reaching changes in public health policy and compensation to states for tobacco-related health care costs.[27]

This controversy demonstrates how trade secret law can be and has been used to silence those in the best position to report illegal activity. Nor is the

---

21. *See* Deepa Vardarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1405, 1409–11 (2014). Trade secret law permits reverse engineering, but that limitation is a noninfringement (nonmisappropriation) doctrine, not a defense.

22. *See* Marie Brenner, *The Man Who Knew Too Much*, VANITY FAIR (May 1996), http://www.vanityfair.com/magazine/1996/05/wigand199605 [https://perma.cc/HU7R-TH8W].

23. *See id*. at 179.

24. *See* Brown & Williamson Tobacco Corp. v. Wigand, 913 F. Supp. 530 (W.D. Ky. 1996) (prohibiting Dr. Wigand from using or disclosing any "materials, trade secrets, or confidential information").

25. *See Tobacco Master Settlement Agreement*, WIKIPEDIA, https://en.wikipedia.org/wiki/Tobacco_Master_Settlement_Agreement [https://perma.cc/F65J-425H] (last visited Sept. 30, 2016).

26. *See* Brenner, *supra* note 22.

27. *See Tobacco Master Settlement Agreement*, *supra* note 25. Dr. Wigand served as an expert witness in litigation that helped to bring about the settlement. *See Jeffrey Wigand, Chemist, Scientist, Activist*, BIO (Apr. 2, 2014), http://www.biography.com/people/jeffrey-wigand-17176428 [https://perma.cc/JPN7-X33F].

problem isolated. Asbestos manufacturers knew the causal link between asbestos and lung disease well before the public and regulatory officials became aware of this serious health risk.[28] And just last year, evidence emerged that Volkswagen had programmed software in its vehicles to mask pollution violations.[29]

Unlike Dr. Wigand, many employees and contractors are not prepared to risk the tremendous personal and professional costs of reporting illegal activity,[30] especially where the law does not provide a clear safe harbor for doing so. This concern has taken on greater moment as companies accused of illegal conduct have increasingly filed lawsuits against whistleblowers and their counsel.[31] Companies increasingly discuss suing whistleblowers for disclosing proprietary information to the government as a defense strategy.[32]

---

28. *See* Morris Greenberg, *Knowledge of the Health Hazards of Asbestos Prior to the Merewether and Price Report of 1930*, 7 SOC. HIST. MED. 493, 501 (1994); ALAN F. WESTIN, *Introduction*, *in* WHISTLE BLOWING! LOYALTY AND DISSENT IN THE CORPORATION 1, 11–12 (1981).

29. *See* Russell Hotten, *Volkswagen: The Scandal Explained*, BBC (Dec. 10, 2015), http://www.bbc.com/news/business-34324772 [https://perma.cc/ZiZF-WPLR].

30. In fact, Dr. Wigand was very reluctant to come forward, and the unraveling of the tobacco industry deception may have been delayed many more years, if not decades, without the persistence of Lowell Bergman, the 60 Minutes producer who recognized the importance of bringing Wigand's story to light. *See* Brenner, *supra* note 22.

31. *See, e.g.*, J-M Mfg. Co. v. Phillips & Cohen, LLP, 129 A.3d 342 (N.J. Super. Ct. App. Div. 2015) (affirming dismissal of trade secret complaint against whistleblower and its counsel on grounds that company should have pursued this matter in the pending California whistleblower qui tam proceeding); United States *ex rel.* Ruscher v. Omnicare, Inc., No. 4:08-cv-3396, 2015 WL 4389589 (S.D. Tex. July 15, 2015) (denying relator motion to dismiss counterclaims including breach of fiduciary duty and breach of implied contract); Walsh v. Amerisource Bergen Corp., No. 11–7584, 2014 WL 2738215 (E.D. Pa. June 17, 2014) (denying relator motion to dismiss counterclaim for breach of confidentiality agreement); Siebert v. Gene Sec. Network, Inc., No. 11-cv-01987, 2013 WL 5645309 (N.D. Cal. Oct. 16, 2013); United States *ex rel.* Head v. Kane Co., 668 F. Supp. 2d 146 (D.D.C. 2009).

32. *See, e.g.*, Carlton Fields, *Employers Fight Back Against Whistleblowers*, LEXOLOGY (July 2, 2014), http://www.lexology.com/library/detail.aspx?g=b2e89afd-6e2a-4310-9139-b94176e38e13 [https://perma.cc/S6ED-N425] (noting that "[e]mployers may even have options against employees who have been successful in [false claims 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"); Amanda Haverstick, *Health Care Employers Take Note: New Weapons Are Available When Defending False Claims Act Suits*, FORBES (June 20, 2014), http://www.forbes.com/sites/theemploymentbeat/2014/06/20/health-care-employers-take-note-new-weapons-are-available-when-defending-false-claims-act-suits [https://perma.cc/EYG5-C593] (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 PHI or other confidential employer information"); 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.healthlawpolicymatters.com/2014/06/24 [https://perma.cc/6QWC-B225]; Lisa M. Noller & Brandi F. Walkowieak, *Holding Rogue Employees Accountable Under the FCA*, LAW360 (Nov. 3, 2011), https://www.foley.com/files/Publication/6e6b9e4f-38f1-457a-a7ad-c331a0757194/Presentation/PublicationAttachment/e45a77e2-8d6e-487b-80d3-c58826bdfd89/WCL36011-3-11.pdf [https://perma.cc/X32U-PMCR].

On the other side of the balance, some companies have legitimate reasons for limiting the disclosure of proprietary information that allegedly reveals illegal activity. The whistleblower might be mistaken as to the illegality of the conduct, and once trade secrets leak, those who learn of them through legitimate means are free to use them.[33] Such leaks can cause significant harm to the trade secret owner. And even if there is some illegal conduct, destruction of whatever trade secrets the whistleblower chooses to divulge might not be the appropriate remedy. Nonetheless, punishing well-meaning whistleblowers and preventing the government from evaluating potentially incriminating evidence is not justified. A public policy exception to trade secret protection must balance the interests of law enforcement with the legitimate interests of trade secret owners.

Part I of this Article traces the development of trade secret protection and laws and policies aimed at fostering effective law enforcement. Drawing on this background, Part II shows that trade secret law has lacked a reliable public policy exception to trade secret protection. As a result, the many employees and contractors who sign NDAs face substantial personal, financial, and professional risk should they report, or even investigate reporting, possible misconduct.

Part III examines the historic interplay of trade secrecy protection and reporting of illegal activity. Part IV shows that the purposes of trade secret law can be harmonized with whistleblowing through a mechanism for encouraging reporting of illegal conduct to trusted intermediaries. A sealed disclosure/trusted intermediary exception to trade secret misappropriation safeguards trade secrets while promoting effective law enforcement. As discussed in Part V, the Defend Trade Secrets Act of 2016 adopts this approach.

I.
THE TRADE SECRECY/LAW ENFORCEMENT TENSION

The Industrial Revolution brought about vast advances in technological progress as well as innovation in legal regimes for promoting such progress. Patent law played a central role in enabling inventors to appropriate a return on their investment in research and development. Nonetheless, patent protection was too costly, unwieldy, and limited to protect the full range of technological and business innovations and know-how. Factory owners and other innovative businesses came to use physical security around their facilities, nondisclosure agreements, and other techniques to secure protection for the broader range of technological advances and strategic information driving their competitive advantage. Courts recognized and reinforced these practices through the development of trade secret law built on two core principles: maintaining

33. *See infra* Part I.A.3.

commercial morality (preventing commercial espionage) and promoting technological innovation.

In contrast to patent protection, trade secrecy law could not protect those product features and techniques that were evident from publicly available information, including the products and services themselves. Nonetheless, it provided an effective means for protecting many process and product innovations and business strategies that were not readily ascertainable by the public.

But while trade secrecy can foster technological innovation and economic development, it can also conceal illegal conduct and silence the most knowledgeable sources. Therein lies the tension with the foundation of civilized society. Rule of law depends on effective criminal and civil law enforcement. At the same time, the U.S. Constitution protects citizens from unreasonable searches and seizures.[34] Without effective reporting, the government lacks the information needed to enforce the laws. Probable cause to investigate illegal activity might never come to light if the key (and perhaps only) witnesses believe that divulging incriminating evidence is illegal or fear risking the consequences of coming forward.

When trade secret protections emerged, the government occupied a relatively small presence in the general economy and social policy.[35] 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.[36] Moreover, as reflected in Figure 1, federal and state governments have taken on a much larger role as economic actors in the general economy, contracting with private enterprises for provision of goods and services, providing health insurance, and funding research and development. Relatedly, governments have increasingly

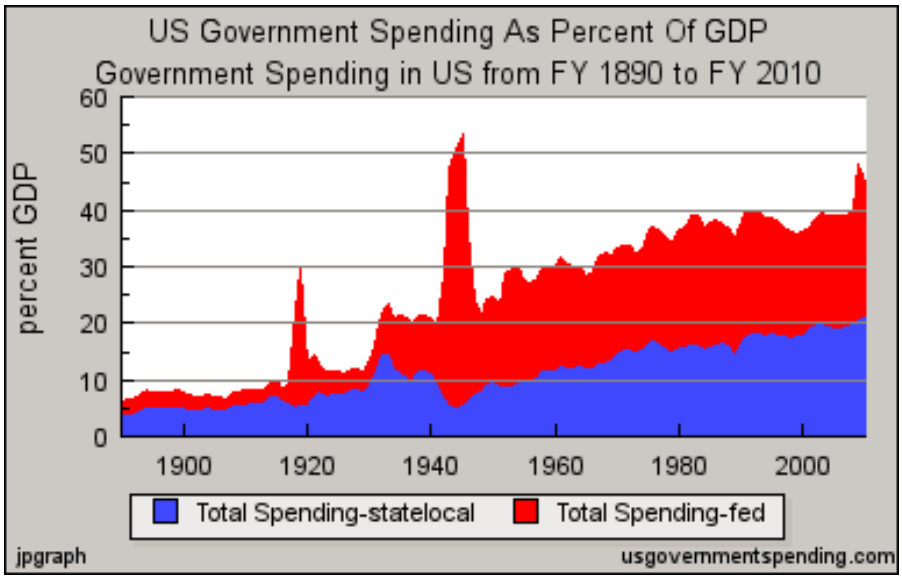
34. *See* U.S. CONST. amend. IV; Boyd v. United States, 116 U.S. 616, 627 (1886) (stating that the "sacred and incommunicable" right of property is only set aside "for the good of the whole" (quoting Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (C.P.) 1066 (Eng.))).

35. *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.").

36. *See* 3 BRUCE ACKERMAN, WE THE PEOPLE: THE CIVIL RIGHTS REVOLUTION (2014); PHILIP J. HILTS, PROTECTING AMERICA'S HEALTH: THE FDA, BUSINESS, AND ONE HUNDRED YEARS OF REGULATION (2003); RICHARD J. LAZARUS, THE MAKING OF ENVIRONMENTAL LAW (2006); Paul Stephen Dempsey, *Transportation: A Legal History*, 30 TRANSP. L.J. 235, 266 (2003); Marc T. Law & Sukkoo Kim, *The Rise of the American Regulatory State: A View from the Progressive Era*, *in* HANDBOOK ON THE POLITICS OF REGULATION 113 (David Levi-Faur ed., 2013); Kevin Werbach, *Higher Standards Regulation in the Network Age*, 23 HARV. J.L. & TECH. 179 (2009); Cynthia A. Williams, *The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197 (1999).

outsourced public functions to private enterprises.[37] Concomitantly, the government has increased taxation.[38]

Figure 1: U.S. Government Spending as Percent of Gross Domestic Product Government Spending from 1890 to 2010



As a result of this transformation, private enterprises have expanded responsibilities to comply with public health and safety, civil rights, environmental, consumer, and financial market regulations, meet contractual

37. *See* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY (Jody Freeman & Martha Minow eds., 2009); DAVID OSBORNE & TED GAEBLER, REINVENTING GOVERNMENT: HOW THE ENTREPRENEURIAL SPIRIT IS TRANSFORMING THE PUBLIC SECTOR (1992); Deirdre Fulton, *Outsourcing Public Services: Governors Push Privatization, with Disastrous Results*, COMMON DREAMS (Oct. 15, 2014), http://www.commondreams.org/news/2014/10/15/outsourcing-public-services-governors-push-privatization-disastrous-results [https://perma.cc/RUD4-CPYR] (reporting that federal, state, and local governments annually allocate $1 trillion out of a total expenditures of $6 trillion to private contractors); Mary Scott Nabers, *The Privatization of Public Services: We Have to Make It Work*, FORBES (July 13, 2012), http://www.forbes.com/sites/forbesleadershipforum/2012/07/13/the-privatization-of-public-services-we-have-to-make-it-work [https://perma.cc/A3C4-L83X]; *Privatization in the United States*, WIKIPEDIA, https://en.wikipedia.org/wiki/Privatization_in_the_United_States [https://perma.cc/F8CG-ZCK8] (last visited Sept. 30, 2016).

38. *See Amount of Revenue by Source*, TAX POL'Y CTR., http://www.taxpolicycenter.org/taxfacts/displayafact.cfm?Docid=203 [https://perma.cc/6V3A-U2WC] (last visited Sept. 30, 2016); COUNCIL ON STATE TAXATION, TOTAL STATE AND LOCAL BUSINESS TAXES 22 (2014), http://www.cost.org/WorkArea/DownloadAsset.aspx?id=87982 [https://perma.cc/2GKL-B8WA]; U.S. CENSUS BUREAU & U.S. DEP'T COMMERCE, QUARTERLY SUMMARY OF STATE AND LOCAL GOVERNMENT TAX REVENUE FOR 2014: Q4 (Mar. 24, 2015), http://www2.census.gov/govs/qtax/2014/g14-qtax4.pdf [https://perma.cc/P8R2-WG33].

obligations with the government, and shoulder tax burdens. The federal and state governments have enacted laws and established policies encouraging reporting of regulatory violations, fraud, and tax evasion. Yet overbroad trade secrecy and a norm of uncritical corporate loyalty can undermine these laws.

As background for exploring the interplay between trade secret protection and law enforcement, Part I.A traces the history of trade secret protection and explicates its underlying principles. Part I.B explores trade secret law and the landscape of law enforcement and whistleblowing policies and laws.

A. Trade Secret Protection

In contrast to copyright and patent law, which have long been grounded in federal statutes and guided by the constitutional principle of promoting progress in expressive creativity and the useful arts,[39] trade secret protection developed through business practices and common law evolution.[40] By the turn of the twentieth century, the core principles and doctrines of trade secret protection had been established through judicial decisions grounded in commercial morality.[41] This Section traces the development of trade secret protection, identifies its core principles, and surveys its modern contours.

1. Development of Trade Secret Protection

While some scholars find precursors to trade secret protection in Roman law,[42] the modern regime traces most clearly and directly to the Industrial Revolution. In preindustrial economies, craftsmen passed along their trade knowledge to their apprentices with the understanding that the know-how would be kept secret during the apprenticeship period.[43] After this training, the apprentice was free to practice the trade. These trust-based protections were reinforced by custom, trade guilds, and close-knit communities.[44]

---

39. *See* U.S. CONST. art. I, § 8, cl. 8; Patent Act of 1790, ch. 7, 1 Stat. 109–112 (1790); Copyright Act of 1790, ch. 15, 1 Stat. 124 (1790). Notwithstanding the statutory foundations of patent and copyright law, the courts have nonetheless played a significant role in delineating and evolving many aspects of these regimes. *See* Peter S. Menell, *The Mixed Heritage of Federal Intellectual Property Law and Ramifications for Statutory Interpretation*, *in* INTELLECTUAL PROPERTY AND THE COMMON LAW 63, 70–71 (Shyam Balganesh ed., 2013).

40. *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 247 (1998).

41. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995).

42. *See* MELVIN F. JAGER, TRADE SECRETS LAW § 1:3 (2013); A. Arthur Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti*, 30 COLUM. L. REV. 837 (1930) (suggesting that courts imposed liability upon those who bribed or intimidated slaves into disclosing their owners' confidential business information). *But see* Alan Watson, *Trade Secrets and Roman Law: The Myth Exploded*, 11 TUL. EUR. & CIV. L.F. 19 (1996) (questioning Schiller's account).

43. *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, 450–51 (2001).

44. *See* CARLO M. CIPOLLA, BEFORE THE INDUSTRIAL REVOLUTION: EUROPEAN SOCIETY AND ECONOMY 1000–1700 (2d ed. 1980); DAVID J. JEREMY, TRANSATLANTIC INDUSTRIAL

This informal system, governed principally through social norms, eroded as industrialization shifted production to factories and labor mobility increased.[45] Factories operated on a far larger scale than traditional craft enterprises and without the social and guild constraints on the dissemination of proprietary techniques and know-how. Whereas patents afforded protection for larger, discrete advances, smaller-bore, incremental know-how was more vulnerable to misappropriation in the impersonal, specialized factory setting. By the early nineteenth century, factory owners in England pressed for a broader form of protection for workplace trade secrets. The know-how behind industrial processes gradually gained recognition in and enforcement by common law courts.[46] The practice spread to the United States by the mid-nineteenth century and developed rapidly.[47]

Trade secret protection could encompass information that was not generally known to the public[48] 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.

Courts routinely characterized trade secrets as "property"[50] and granted injunctive relief to prevent their disclosure.[51] The nature of the "property"

REVOLUTION: THE DIFFUSION OF TEXTILE TECHNOLOGIES BETWEEN BRITAIN AND AMERICA, 1790–1830S, at 185–89 (1981).

45. *See* Margo E.K. Reder & Christine Neylon O'Brien, *Managing the Risk of Trade Secret Loss Due to Job Mobility in an Innovation Economy with the Theory of Inevitable Disclosure*, 12 J. HIGH TECH. L. 373, 386 (2012).

46. *See* Newbery v. James, 35 Eng. Rep. 1011, 1011–12 (Ch. 1817). *See generally* Fisk, *supra* note 43, at 450–88 (tracing the emergence of trade secret obligation during the Industrial Revolution).

47. *See* 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); JAGER, *supra* note 42, § 2:3.

48. *See* Nat'l Tube Co. v. Eastman Tube Co., 13-23 Ohio C.C. Dec. 468, 470 (Cir. Ct. 1902), *aff'd*, 70 N.E. 1127 (Ohio 1903). The courts did not, however, demand absolute secrecy. *See, e.g.*, Pressed Steel Car Co. v. Standard Steel Car Co., 60 A. 4, 9 (Pa. 1904).

49. *See* Eastman Co. v. Reichenbach, 20 N.Y.S. 110, 110, 116 (Sup. Ct. 1892), *aff'd sub nom.* Eastman Kodak Co. v. Reighenbach, 29 N.Y.S. 1143 (Gen. Term 1894).

50. *See, e.g.*, Tabor v. Hoffman, 23 N.E. 12, 34 (N.Y. 1889) (holding that "independent of copyright or letters patent, an inventor or author has, by the common law, an exclusive property in his invention or composition, until by publication it becomes the property of the general public"); Peabody v. Norfolk, 98 Mass. 452, 458 (1868) (recognizing a "property right" in a trade secret); McGowin v. Remington, 12 Pa. 56, 57 (1849).

51. *See* JAGER, *supra* note 42, § 2:3 (observing that "[t]he description of trade secret as 'property' was common"); O. & W. Thum Co. v. Tloczynski, 72 N.W. 140 (Mich. 1897) (holding that a trade secret is a property right that can be protected by an injunction without creating an illegal restraint of trade); Fralich v. Despar, 30 A. 521, 521–22 (Pa. 1894).

In modern times, the U.S. Supreme Court held that public disclosure of a trade secret by the federal government could constitute a taking of private property for which just compensation was required under the Fifth Amendment to the U.S. Constitution. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984). In finding that trade secrets were "property" for purposes of the Takings Clause of the Fifth Amendment, the Court reasoned in part that "[t]rade secrets have many of the characteristics of more tangible forms of property. A trade secret is assignable. A trade secret can form the res of a

interest was, however, limited by the relational character of trade secrets.[52] As the court in *Peabody* noted, if a party:

> [I]nvents or discovers and keeps secret a process of manufacture, whether a proper subject for a patent or not, he has not indeed an exclusive right to it as against the public, or against those who in good faith acquire knowledge of it, but he has property in it which a court of chancery will protect against one who, in violation of contract and breach of confidence, undertakes to apply it to his own use, or to disclose it to third persons.[53]

The court explained that courts of equity would intervene to "prevent such a breach of trust, when the injury would be irreparable and the remedy at law inadequate, is well established by authority."[54] Thus, injunctions were available for breaches of trust "in the course of confidential employment."[55]

In *E.I. duPont deNemours Powder Co. v. Masland*,[56] Justice Holmes explained that:

> The word "property" as applied to . . . trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. Whether the plaintiffs have any valuable secret or not, the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied, but the confidence cannot be. Therefore, the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs.[57]

Tort law governs injury to property, as well as personal, interests. Therefore, early commentators viewed trade secret protection, like other forms of intellectual property, as a branch of tort law.[58] The emerging law of trade

---

trust, and it passes to a trustee in bankruptcy." *Id.* at 1002–04; *see* Peter S. Menell, *Bankruptcy Treatment of Intellectual Property Assets: An Economic Analysis*, 22 BERKELEY TECH. L.J. 733, 747–48, 821 (2007) (discussing the treatment of trade secrets for bankruptcy and security interest purposes).

52. *See* Bone, *supra* note 40, at 251–60; RESTATEMENT OF TORTS § 757, cmt. a (1939) (reporting that the property conception "has been frequently advanced and rejected," concluding that the prevailing theory of liability rests on "a general duty of good faith").

53. *Peabody*, 98 Mass. at 458.

54. *Id.*

55. *See Eastman Co. v. Reichenback*, 20 N.Y.S. 110, 114–15 (Sup. Ct. 1892) (finding that "[t]he very nature of the case, the peculiar character of the injury liable to be inflicted, and the incalculable damages which may possibly result, all show most conclusively that legal relief is totally inadequate for plaintiff's protection, and that its only resort must be to a court of equity" and quoting Justice Story for the principle that "[c]ourts of equity will restrain a party from making a disclosure of secrets communicated to him in the course of a confidential employment" (citing 2 STORY, EQ. JUR. 952)).

56. 244 U.S. 100 (1917).

57. *Id.* at 102.

58. *See, e.g.*, J. F. CLERK & W. H. B. LINDELL, THE LAW OF TORTS 587 (2d ed. 1896) (containing a chapter on copyright law); *see also* Peter S. Menell & David Nimmer, *Unwinding* Sony, 95 CALIF. L. REV. 941, 994–1005 (2007).

secrets was thus collected in the *Restatement of Torts* (Restatement), published in 1939.[59] The Restatement protected as a trade secret any information "used in one's business" that gives its owner "an opportunity to obtain an advantage over competitors who do not know or use it," so long as the information was in fact a secret.[60]

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.[61] Nonetheless, the influence of the original Restatement has remained in part because so many judicial decisions had relied on it and because its teachings had been integrated into statutes and other key sources.[62] Part I.3 discusses the modern codification of trade secret law in the UTSA and the *Restatement (Third) of Unfair Competition*. Before turning to those sources, it will be useful to examine the principles undergirding trade secret protection.

2. Guiding Principles: Commercial Morality and Technological Progress

Trade secret law has long been grounded in what has been termed "commercial morality."[63] The *Eastman* case illustrates the principle in action.[64] In the late nineteenth century, Eastman (Kodak), a pioneering developer of photographic technology, brought suit against former high-level employees who departed to start a competing business using secret information that they helped develop at Eastman. They had executed assignment agreements covering all inventions, discoveries, and improvements in photography that they might make, discover, or invent while at Eastman and agreed to maintain company secrets in strict confidence and not to make improper use of them. The court enjoined 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."[65]

---

59. *See* RESTATEMENT OF TORTS §§ 757–58 (1939).

60. *See id.* § 757, cmt. b.

61. *See* RESTATEMENT (SECOND) OF TORTS, Intro. Note to Division Nine (1979).

62. *See* JAGER, *supra* note 42, § 3.01.

63. *See id.* § 1:3 (observing that "[t]he Anglo-American common law . . . began to develop protection for business secrets to enhance commercial morality and good-faith dealings in business"); Bone, *supra* note 40, at 244 (concluding that trade secret law is grounded in "relationally specific duties," such as "disloyal employees who use or disclose their employers' secrets in violation of a duty of confidence stemming from the employer-employee relationship").

64. *See* Eastman Co. v. Reichenbach, 20 N.Y.S. 110, 110, 116 (Sup. Ct. 1892), *aff'd sub nom.* Eastman Kodak Co. v. Reighenbach, 29 N.Y.S. 1143 (Gen. Term 1894).

65. *Id.* at 116.

This theme pervades trade secret law.[66] As the Supreme Court recognized in its landmark decision *Kewanee Oil Co. v. Bicron Corp.*,[67] federal patent law does not preempt state trade secret protection. The Court held that "[t]he maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law. 'The necessity of good faith and honest fair dealing is the very life and spirit of the commercial world.'"[68]

The *Kewanee Oil* opinion also recognized a second guiding principle of trade secret protection: encouraging research and development.[69] The Court recognized that:

> [E]ven though a discovery may not be patentable, that does not destroy the value of the discovery to one who makes it, or advantage the competitor who by unfair means, or as the beneficiary of a broken faith, obtains the desired knowledge without himself paying the price in labor, money, or machines expended by the discoverer.[70]

The Court emphasized "the importance of trade secret protection to the subsidization of research and development and to increased economic efficiency within large companies through the dispersion of responsibilities for creative developments."[71] This aligns with Justice Gray's declaration, in an early seminal case, that "it is the policy of the law, for the advantage of the public, to encourage and protect invention and commercial enterprise."[72]

3. Modern Contours of Trade Secret Protection

By the mid-twentieth century, "the body of state and federal law that ha[d] traditionally coped with [industrial espionage] languish[ed] in a deepening maze of conflict and confusion."[73] Recognizing this doctrinal muddle and the growing economic importance of trade secret protection, the American Bar Association established a special committee in 1968 to investigate the drafting of a uniform trade secret act to harmonize protection among the states.[74] Over the course of the next decade, that committee drafted

---

66. *See* JAGER, *supra* note 42, § 1:3 n.16 (citing numerous cases).

67. 416 U.S. 470 (1974).

68. *Id.* at 481–82 (quoting Nat'l Tube Co. v. Eastman Tube Co., 13-23 Ohio C.C. Dec. 468, 470 (Cir. Ct. 1902), *aff'd*, 70 N.E. 1127 (Ohio 1903)).

69. *See id.* at 482.

70. *See id.* (quoting A. O. Smith Corp. v. Petrol. Iron Works Co., 73 F.2d 531, 539 (6th Cir. 1934)).

71. *See id.* (citing Wexler v. Greenberg, 160 A.2d 430, 434–35 (Pa. 1960)).

72. Peabody v. Norfolk, 98 Mass. 452, 457 (1868).

73. *See* Comment, *Theft of Trade Secrets: The Need for a Statutory Solution*, 120 U. PA. L. REV. 378 (1971).

74. *See* UNIF. TRADE SECRETS ACT, prefatory note (1979) (UNIF. LAW COMM'N, amended 1985) (noting that "[u]nder technological and economic pressures, industry continues to rely on trade secret protection despite the doubtful and confused status of both common law and statutory remedies. Clear, uniform trade secret protection is urgently needed. . . .") (quoting *Theft of Trade Secrets*, *supra* note 73, at 380–81).

and refined the UTSA,[75] which the National Commission on Uniform State Laws promulgated in 1979. The UTSA has since been adopted by forty-seven states and the District of Columbia.[76]

In addition, some states adopted criminal statutes addressing misappropriation of trade secrets.[77] In response to growing concerns about trade secret misappropriation in the digital age, the United States Congress enacted the Economic Espionage Act of 1996 (EEA),[78] which authorizes the federal government to pursue criminal charges against those who misappropriate trade secrets with the knowledge or intent that the theft will benefit a foreign power or injure the owner of the trade secret.[79]

The UTSA defines the scope of eligible trade secret protection expansively and imposes liability on those who misappropriate trade secrets. *Any* information, "including a formula, pattern, compilation, program, device, method, technique, or process," can be protected as a trade secret so long as it meets two requirements: (1) it derives independent economic value from not being generally known or readily ascertainable by proper means; and (2) it "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[80] A trade secret owner need not apply for trade secret protection, register trade secrets, or even specifically identify them. In order to pursue a trade secret action, however, the plaintiff must establish that the information at issue derives independent economic value from not being generally known and is subject to reasonable precautions to maintain its secrecy.

The latter requirement motivates companies to require all employees and contractors with access to confidential information to sign NDAs upon commencement of employment and return trade secret documents upon

75. *See* UNIF. TRADE SECRETS ACT § 1(D)(ii) (UNIF. LAW COMM'N 1985).

76. Massachusetts, New York, and North Carolina have not adopted the UTSA, *see Trade Secrets Act*, UNIFORM L. COMMISSION, http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act [https://perma.cc/QD6W-92L8], although North Carolina's trade secret statute borrows heavily from the UTSA. *See* N.C. GEN. STAT. ANN. § 66-152 (2015). Some states have enacted variations of the UTSA. JAGER, *supra* note 42, § 3:29. In addition, the RESTATEMENT (THIRD) OF UNFAIR COMPETITION, published in 1994, includes sections on the law of trade secrets (§§ 39–45) that parallel the structure and substance of the UTSA with slight modifications.

77. *See* Pooley et al., *supra* note 6, at 186; *see, e.g.*, CAL. PENAL CODE § 499c (West 2009).

78. Pub. L. 104-294, 110 Stat. 3488 (1996) (codified at 18 U.S.C. §§ 1831–39 (2012)).

79. As reflected in the Department of Justice prosecution policy, the EEA was:

> [N]ot intended to criminalize every theft of trade secrets for which civil remedies may exist under state law. It was passed in recognition of the increasing importance of the value of intellectual property in general, and trade secrets in particular to the economic well-being and security of the United States and to close a federal enforcement gap in this important area of law.

U.S. ATTORNEYS' MANUAL § 9-59.000 (2015). The policy identifies various factors, such as the scope of the criminal activity, the degree of economic injury, the effectiveness of civil remedies, and the potential deterrent effect to guide the exercise of prosecutorial discretion.

80. *See* UNIF. TRADE SECRETS ACT § 1(4) (definition of "trade secret").

termination of employment.[81] Executing such agreements has little cost, and failure to have such safeguards in place risks leaks of confidential information and jeopardizes being able to prove that there exists a valid trade secret in particular information. Furthermore, various privacy regimes requiring safeguarding of health care and personnel records, financial information, and national security information reinforce the practice of requiring employees and contractors to sign NDAs.

Misappropriation of trade secrets can occur in two ways: (1) acquisition of the trade secret by improper means and (2) disclosure of the trade secret through breach of confidence.[82] Improper means includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[83] It does not, however, encompass reverse engineering of a product available to the public.[84] Breach of confidence includes violations of express NDAs as well as implied duties of confidence.[85]

In contrast to other forms of intellectual property law,[86] the UTSA lacks exceptions or defenses to liability. Part II explores the extent to which courts have recognized a public policy exception to trade secret liability.

The UTSA authorizes courts to enjoin actual or threatened misappropriation[87] as well as award compensation for actual damages and unjust enrichment.[88] Courts may also award exemplary damages of up to double the compensatory amount and attorneys' fees in cases of willful and malicious misappropriation.[89]

Notwithstanding the broad potential scope of trade secret protection and lack of any express defense, trade secret protection has a notable Achilles' heel. Once a trade secret leaks, it can be lost for most practical purposes and monetary damages are often inadequate or unavailable to stanch the loss. Although the trade secret owner can pursue the person who misappropriated the trade secret and can typically enjoin their future usage and seek damages, competitors who obtain the information legitimately are free to use it.[90] Like

81. Absolute secrecy is not generally required. *See* Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1200 (5th Cir. 1986); Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L.J. 1, 43 (2007).

82. *See* UNIF. TRADE SECRETS ACT § 1(2) (defining "misappropriation").

83. *See id.* § 1(1) (defining "improper means").

84. *See* Kadant, Inc. v. Seeley Machine, Inc., 344 F. Supp. 2d 19 (N.D.N.Y. 2003); Chicago Lock Co. v. Fanberg, 676 F.2d 400 (9th Cir. 1982).

85. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (1995).

86. *See supra* notes 17–20.

87. *See* UNIF. TRADE SECRETS ACT § 2.

88. *See id.* § 3.

89. *See id.* §§ 3(b), 4(iii).

90. *See* Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425 (2009); Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1 (2007).

the proverbial genie in a bottle, once the secret escapes, it cannot be controlled. And the misappropriating party may well be judgment-proof. Thus, the remedies for trade secret misappropriation can be inadequate to compensate for the economic harm.

B. Law Enforcement and Whistleblowing Policies

While robust trade secret protection makes economic sense in a contemporary business environment marked by high employee mobility and cybercrime, uncritical protection of all secret business information can conflict with effective law enforcement. As the previous Section explained, blanket restrictions on information disclosure have become standard operating procedure in many business environments. Such practices can suppress reporting of illegal conduct, thereby undermining civil rights, public health, environmental protection, and compliance with government contracts.

Since the nation's founding, the federal, state, and local governments have encouraged reporting of illegal conduct to ensure a properly functioning society. Perhaps most fundamentally, the American civil and criminal justice systems rely on discovery and evidence-gathering models consistent with Fourth Amendment protections against unreasonable searches and seizures. Without reporting of illegal activity and access to documentary evidence supporting investigation, the government and the courts are severely hampered in their ability to enforce the law.

The need for such reporting has grown concomitantly with the government's increased role in the economy—through, for example, military procurement, infrastructure, and health care—and expanded protections for civil rights, worker safety, public health, the environment, and the integrity of financial markets.

Though it may seem inconceivable today, the federal government played almost no role in regulating business activities before the late nineteenth century.[91] The bulk of economic oversight came in the form of common law tort guidelines, with some supplementation from state and local regulations.[92] Growing economic power resulting from industrialization and economic concentration produced a populist backlash, called for fairer wages and working hours, and limited monopoly power.[93] This led to regulations that protected workers and limited unfair business practices, such as the Interstate Commerce Act, the Sherman Antitrust Act, and the Bureau of Corporations.

---

91. *See* Rabin, *supra* note 35, at 1196 ("[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.").

92. *See id.* at 1192. The Interstate Commerce Act of 1887, though fairly limited in scope and ultimately diluted by the courts, marked a sea change in the federal government's approach to regulating business sectors having national impact. It also served as a sign of what was to come.

93. *See id.* at 1216–18.

The Interstate Commerce Act,[94] passed in 1887, aimed to regulate the monopolistic practices of the railroad industry.[95] Three years later, Congress enacted the landmark Sherman Antitrust Act to combat the growing power of trusts and corporations.[96] Congress created the Bureau of Corporations (Bureau) in 1903 to study and report on monopolistic practices.[97] The Bureau's work laid the groundwork for regulating a range of industrial practices. The first decade of the twentieth century saw passage of the Federal Meat Inspection Act,[98] the Pure Food and Drugs Act,[99] and other legislation regulating business operations. Congress expanded upon the Bureau's activities by establishing the Federal Trade Commission, a general agency with broad investigatory and enforcement powers to address unfair competition.[100]

Following the onset of the Great Depression, FDR's ill-fated National Industrial Recovery Act of 1933[101] ushered in the New Deal era that would facilitate further federal intervention into the economy through the Securities and Exchange Act,[102] the Federal Deposit Insurance Corporation (FDIC),[103] the Social Security Act,[104] and the National Labor Relations Act.[105] As the century advanced, so did the extent of governmental regulation, which by the late 1970s had expanded to regulate a broad range of business activities to protect civil rights, consumers, workers, and the environment.

The expansion of government-funded programs and activities during the twentieth century spurred efforts to ramp up the information-gathering and enforcement roles of private citizens who, if properly motivated, could be vital to detecting and deterring illegal activity. The federal and state governments have sought to harness the knowledge of whistleblowers through provisions shielding them from retaliation, and, in some cases, rewarding them for providing useful information for enforcing the law.

---

94. Ch. 104, 24 Stat. 379 (1887).

95. *See* Dempsey, *supra* note 36, at 266 ("The Interstate Commerce Act was the first comprehensive regulation of any industry in the United States. It was the first time in American legal history that an industry was regulated by a structure outside the courts and the common law. . . .").

96. Ch. 647, 26 Stat. 209 (1890).

97. *See* Elizabeth Kimball MacLean, *Joseph E. Davies: The Wisconsin Idea and the Origins of the Federal Trade Commission*, 6 J. GILDED AGE & PROGRESSIVE ERA 248 (2007).

98. Ch. 3913, 34 Stat. 674 (1906).

99. Ch. 3915, 34 Stat. 768 (1906).

100. Federal Trade Commission Act, ch. 311, 38 Stat. 717 (1914); *see* Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L.J. 1 (2003).

101. Ch. 90, 48 Stat. 195 (1933).

102. Ch. 404, 48 Stat. 881 (1934).

103. The FDIC was created in 1933 as part of the Banking Act of 1933, ch. 89, 48 Stat. 162 (1933).

104. Ch. 531, 49 Stat. 620 (1935).

105. Ch. 372, 49 Stat. 449 (1935).

For example, the Civil Rights Act of 1964 includes protection for any employee who has "opposed any practice made an unlawful employment practice by this subchapter, or because he has made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under this subchapter."[106] After the creation of the Environmental Protection Agency (EPA) in 1970, Congress passed six major environmental laws,[107] each of which included protection for whistleblowers. In 1974, the Safe Drinking Water Act (SDWA) included a provision that empowered citizens to bring civil actions against water systems that did not meet the SDWA's standards.[108] The SDWA also protected employees of water systems who provided information about drinking water violations.[109] Revelations about manufacturers' attempts to cover up studies that linked asbestos to lung cancer paved the way for the passage of the Toxic Substances Control Act in 1976,[110] which also contains a provision that protects employees who provide regulators with information about toxic substances.

The same broad NDAs that promote commercial morality and protect technological innovation can be subverted to silence employees and contractors who become aware of fraud, regulatory noncompliance, and other illegal conduct. While the evasion of these responsibilities may well enhance a corporation's profitability, it undermines the greater good. As the Supreme Court has recognized:

> [C]orporations can claim no equality with individuals in the employment of a right to privacy. They are endowed with public attributes. They have a collective impact upon society, from which they derive the privilege of acting as artificial entities. The Federal Government allows them the privilege of engaging in interstate commerce. Favors from government often carry with them an

106. 42 U.S.C. § 2000(e)(3) (2012).

107. *See* Richard E. Condit, *Providing Environmental Whistleblowers with Twenty-First Century Protections*, 2 AM. U. LAB. & EMP. L.F. 31, 39 (2011) (noting that the Toxic Substances Control Act; Clean Water Act; Safe Drinking Water Act; Resource Conservation and Recovery Act; Clean Air Act; and Comprehensive Environmental Response, Compensation, and Liability Act contain forty-seven separate whistleblower provisions).

108. 42 U.S.C. § 300j-8.

109. *Id.* § 300j-9(i).

110. EPA Administrator Russell Train summed up this new suspicion of corporations in a 1976 speech:

> Most Americans had no idea, until relatively recently, that they were living so dangerously. They had no idea that when they went to work in the morning, or when they ate their breakfast—that when they did the things they had to do to earn a living and keep themselves alive and well—that when they did things as ordinary, as innocent and as essential to life as eat, drink, breathe or touch, they could, in fact, be laying their lives on the line. They had no idea that, without their knowledge or consent, they were often engaging in a grim game of chemical roulette whose result they would not know until many years later.

S. REP. NO. 94-698, at 3 (1976), *as reprinted in* 1976 U.S.C.C.A.N. 4491, 4493.

enhanced measure of regulation.[111]

Thus, the law must strike a balance between trade secrecy protection and reporting of illegal conduct. This Section surveys the counterweights to blanket trade secrecy protection. The first Subsection examines general considerations regarding reporting of illegal activity. The second Subsection explores the reward systems that the federal government has put in place to ferret out fraud against the government, securities violations, and violations of the tax code.

1. The Rule of Law and Reporting of Illegal Activity

The ability to detect and punish violations of its laws is central to a stable, effective, and just government. Because the government is not omniscient, and because the Fourth Amendment limits its powers and protects the privacy of the public,[112] private enforcement and citizen cooperation serve to supplement governmental efforts to ensure rule of law. American citizens supply law enforcement with tips about criminal activity,[113] bring civil suits, and provide testimony that advances the pursuit of justice.[114]

In the law enforcement setting, for instance, governments rely on community cooperation, eyewitness testimony, and the sharing of citizen-held information to detect and prosecute crimes. Local police forces often include community policing efforts as part of their overall law enforcement strategy.[115] Community policing is based on the realization that for society to function properly, law enforcement needs the help and resources of the citizenry to deter criminal activity.[116] Although community policing can cover a broad range of endeavors, it most commonly promotes engagement, collaboration, and

111. United States v. Morton Salt Co., 338 U.S. 632, 652 (1950).

112. Fourth Amendment rights are not absolute. *See* Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1460–61 (1996) ("The intuition that those who conceal evidence of crime forfeit the privacy used in such concealment is one shared by prominent liberals and conservatives alike. . . . [T]o the extent that privacy in one's 'person[], houses, papers and effects' is a substantive right that is intimately connected to the individual and how he or she is using that right, the guilty seem undeserving, even unworthy, of the privacy they have abused, much like the hypothetical person who uses a speech to incite a riot.").

113. *See, e.g.*, Melanie D. Wilson, *Prosecutors "Doing Justice" Through Osmosis—Reminders to Encourage a Culture of Cooperation*, 45 AM. CRIM. L. REV. 67, 71 n.18 (2008) (detailing a marked uptick in anonymous tips supplied to local police after a 2007 homicide death in Richmond, Virginia, and noting that the increased volume of tips was "credited with identifying numerous criminal wrongdoers," leading to a decrease in criminal activity).

114. At common law, every person has a duty to take reasonable steps, including arrest, to prevent a breach of the peace that is being, or reasonably appears about to be, committed in his presence. Graham Gooch & Michael Williams, *Citizen's Arrest*, A DICTIONARY OF LAW ENFORCEMENT (2015).

115. *See* Tracey L. Meares, *Praying for Community Policing*, 90 CALIF. L. REV. 1593 (2002).

116. *See* Sahar F. Aziz, *Policing Terrorists in the Community*, 5 HARV. NAT'L SECURITY J. 147, 155 (2014) ("Community policing was introduced in the 1960s as an alternative to the traditional paramilitary policing model that soured relationships between law enforcement and minority communities.").

partnering among officers and members of a community.[117] Toward that end, law enforcement departments and officers across the country hold meetings with community groups and engage with community members while on duty to jointly reduce crime and ensure public safety.

Beyond public prosecution, many legal rules vital to a properly functioning society depend on citizens for law enforcement. In the regulatory context, state and federal agencies, such as the Securities and Exchange Commission (SEC), EPA, and Occupational Safety and Health Administration (OSHA), increasingly rely on private enforcement and private evidence gathering.[118]

Civil liability plays a critical role in deterring illegal conduct and compensating victims. In most instances, the reported illegal conduct has directly harmed the individual or group that initiated the civil action. The American system of pretrial discovery[119] promotes the disclosure of information that will help bring about compliance with all manner of law—from statutes to contractual commitments.[120] The benefits of this information access accrue to individual litigants—who can proceed without fear that an adversary can block access to information related to the case at hand[121]—but may also result in a more expansive impact.

The revelation that tobacco consumption causes serious health hazards illustrates the critical role of civil discovery.[122] After years of denials by tobacco executives about the addictiveness and human health impacts of nicotine, mandatory civil discovery played a large role in breaking through a well-fortified corporate wall of silence.[123] Had companies not been required to hand over millions of documents requested in civil discovery, it is possible that many more years could have passed before the truth about tobacco came to

117. *See* Meares, *supra* note 115, at 1598.

118. *See* Yuval Feldman & Orly Lobel, *Decentralized Enforcement in Organizations: An Experimental Approach*, 2 REG. & GOVERNANCE 165, 167–68 (2008).

119. American civil discovery includes pretrial depositions, requests for document production, interrogatories, and physical and mental examinations. *See* FED. R. CIV. P. 26–37.

120. *See* FED. R. CIV. P. 26, advisory committee notes ("The purpose of discovery is to allow a broad search for facts, the names of witnesses, or any other matters which may aid a party in the preparation or presentation of his case.").

121. *See* Ellen E. Sward, *Values, Ideology and the Evolution of the Adversary System*, 64 IND. L.J. 301, 317 (1989) (noting that the adversarial system "encourages people actively to cover up facts that could lead to a more accurate portrayal of truth").

122. *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 99 n.231 (2003).

123. *See id.* ("Through dogged discovery efforts, the State of Minnesota was able to compel the tobacco industry to surrender thirty-five million pages of documents. The $246 billion settlement between the tobacco industry and forty-six states in 1998 can be tied directly to the court-ordered production of these documents.").

light,[124] further delaying life-saving public health measures and victim compensation.

Although a freer flow of relevant information can benefit law enforcement efforts and the pursuit of justice in the civil litigation context, thereby advancing the public good, the opposite can be true when secrecy becomes the dominant posture. Examples abound of societal harms that result from heightened levels of secrecy. In a broad range of scenarios, access to information has proved critical to the capacity of government to protect its citizenry and maintain a properly functioning society.

A prime example of how extreme secrecy can hinder law enforcement is the government's struggle with, and eventual cracking of, the mafia's Omerta code of silence. Prior to 1963 and the testimony of Joseph Valachi, the government had failed to obtain testimony from the Cosa Nostra crime family, which had been destabilizing major American labor organizations and industrial sectors through extortion, price fixing, money laundering, bribery, fraud, drug dealing, and theft, among other crimes.[125] The Omerta-enforced silence meant that law enforcement was left in the dark with respect to the mafia membership, organization, and criminal enterprises. But once law enforcement broke through the code of secrecy, the mafia's organization unraveled.[126] With credible offers of prosecutorial leniency and witness protection in exchange for credible testimony, the floodgates opened, and by the 1980s, what had seemed like an unstoppable criminal enterprise collapsed.[127]

The tragic terrorist attacks of September 11, 2001, brought about greater awareness of the importance of citizens' role in reporting suspicious activity. The government released an online guide urging Americans to "[g]et to know your neighbors at home and while traveling," "be on the lookout for suspicious activity," and "report [the possibility of terrorist activity] to law enforcement immediately."[128] Regardless of one's views of the Uniting and Strengthening

124. Previous efforts to get at this information proved unsuccessful at nearly every turn. *See* Michael V. Ciresi, Roberta B. Walburn & Tara D. Sutton, *Decades of Deceit: Document Discovery in the Minnesota Tobacco Litigation*, 25 WM. MITCHELL L. REV. 477, 480 ("There are many reasons why the tobacco industry has been so difficult to defeat in so many forums—legal and legislative—for so many decades. One principal reason has been the tobacco industry's ability to keep hidden millions of pages of internal documents which contain damning admissions.").

125. *See* James B. Jacobs & Lauryn P. Gouldin, *Cosa Nostra: The Final Chapter?*, 25 CRIME & JUST. 129, 131 (1999).

126. *See id.* ("Beginning in the late 1970s . . . Cosa Nostra's much vaunted code of omerta began to disintegrate and, by the late 1980s and early 1990s, many high-ranking organized crime figures agreed to testify for the government in exchange for leniency and placement in the federal Witness Protection Program. . . .").

127. *See id.* at 130 ("Since the late 1970s, the federal, state, and local government attack on Cosa Nostra, using criminal, civil, and regulatory strategies, has been one of the most successful law enforcement campaigns in U.S. history.").

128. *See* Karen Engle, *Constructing Good Aliens and Good Citizens: Legitimizing the War on Terror(ism)*, 75 U. COLO. L. REV. 59, 102 (2004); *see also* Peter P. Swire, *Privacy and Information in*

America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) and the National Security Agency's surveillance programs, there is little question that the reporting of alleged illegal activity plays a critical and increasingly important role in modern societies.

2. Encouraging Reporting of Illegal Conduct: Whistleblowing Laws

The government has relied on citizen reporting information to assist law enforcement in other areas as well. For well over a century, the federal government has encouraged citizens to come forward with information revealing fraud against the government. The following Sections trace the development of the False Claims Act and more recent expansions of whistleblowing laws aimed at ferreting out fraud and other illegal conduct, such as securities and tax law violations.

a. The False Claims Act

Laws authorizing individuals to bring suit in the name of the government in return for a bounty originated in England in the thirteenth century.[129] Such laws, known as "qui tam" actions, base the bounty on the damages recovered, with the remainder going to the government.[130] American colonies instituted similar statutes to deter corruption and graft,[131] and the first laws adopted by the Congress of the newly formed United States included qui tam provisions.[132]

The most enduring of such laws was enacted during the Civil War. As the size of government grew and as state expenditures drove economic expansion, opportunities for fraud against the government increased. A congressional committee investigating fraud found that contractors who sold the government defective rifles and ammunition filled with sawdust faced little risk of detection or punishment.[133] In response, Congress passed the False Claims Act (FCA)[134] to deter fraud and to reward those who came forward with insider information.

---

the War on Terrorism, 51 VILL. L. REV. 951, 957 (2006) ("In a period of asymmetrical threats . . . those charged with homeland security have a strong desire to get information immediately, to help prevent the attack that might come at any moment. This desire to get information translates directly into the greater prominence of information sharing as a policy goal.").

129. Note, *The History and Development of Qui Tam,* 1972 WASH. U. L.Q. 81, 86 (1972).

130. "'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.'" *See* Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 768 n.1 (2000) (citing 3 WILLIAM BLACKSTONE, COMMENTARIES *160).

131. *The History and Development of Qui Tam*, *supra* note 129, at 94–95. Qui tam actions ultimately fell into disuse in England, and all remaining such laws were repealed by 1951. *Id.* at 88 & n.44.

132. *See Vt. Agency of Nat. Res.*, 529 U.S. at 776.

133. *See* CONG. GLOBE, 37th Cong., 3d Sess. 952, 955 (1863) (statement of Senator Jacob Howard).

134. 12 Stat. 696 (1863).

The statute prohibited soldiers and civilians from making or presenting false claims, false vouchers, false oaths, and forged signatures, in addition to proscribing theft, embezzlement, and conspiracy. Violators faced one to five years of imprisonment and fines ranging from $1,000 to $5,000. They also faced civil liability of $2,000, double the amount of damage to the government, and related litigation costs. Under the FCA, anyone with sufficient evidence could bring suit in the name of the United States and, if successful, receive half the recovered penalty in addition to their costs.

Following the FCA's passage, and through the first four decades of the twentieth century, whistleblowers brought a wide range of fraud claims—involving everything from defense to agriculture to postal subsidies. But in 1943, concern about FCA cases that merely copied criminal indictments and did not uncover original insider information led Attorney General Francis B. Biddle to seek repeal of the FCA.[135] While resisting Biddle's call to repeal the FCA, Congress nonetheless reformed it in ways that undermined its efficacy. The amended FCA cut rewards by half and limited whistleblower involvement in cases that the government chose to investigate.[136] As a result of these changes, few qui tam cases were pursued successfully after 1943 and the FCA went into disuse.

Growing problems of fraud by government contractors reemerged during the Reagan Administration. Cold War defense spending, paired with the reduced incentives for whistleblowers, created a fertile environment for fraud against the government. By the mid-1980s, Congress estimated that fraud cost taxpayers at least $10 billion annually.[137] For instance, Boeing billed the Pentagon $748 for a pair of duckbill pliers similar to those that a government engineer testified he could purchase at a hardware store for $7.61.[138] Employees of defense contractors testified about a "conspiracy of silence" that made them afraid to report fraud against the government, and thus made such fraud difficult to detect.[139]

135. CLAIRE M. SYLVIA, THE FALSE CLAIMS ACT: FRAUD AGAINST THE GOVERNMENT § 2:8 (2d ed. 2010).

136. Ch. 377, Pub. L. No. 213 (1943). The amended FCA also barred actions if the complaint was based on evidence or information within the government's possession. *See* 31 U.S.C. § 3730(b)(4) (1982) (superseded).

137. S. REP. No. 99-345, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 5266, 5268 ("The Department of Justice has estimated fraud as draining 1 to 10 percent of the entire Federal budget. Taking into account the spending level in 1985 of nearly $1 trillion, fraud against the Government could be costing taxpayers anywhere from $10 to $100 billion annually.").

138. *See* Fred Hiatt & Rick Atkinson, *Air Force Victory Is Illusory in the Case of $748 Pliers*, WASH. POST (Mar. 22, 1985), http://www.washingtonpost.com/archive/politics/1985/03/22/air-force-victory-is-illusory-in-the-case-of-748-pliers/a81ecb4b-721b-405f-9fb0-a89e4feea373 [https://perma.cc/Q7DC-SE4J].

139. *See* S. REP. NO. 99-345, at 5, *as reprinted in* 1986 U.S.C.C.A.N. at 5270.

In response, Congress amended the FCA in 1986 to reengage whistleblowers by removing barriers to reporting and providing greater incentives for coming forward. The revised FCA made three notable changes.

First, the amended FCA affords relators a role in the case. No longer can the government "neglect evidence, cause . . . delay, or drop the false claims case without legitimate reason."[140] The FCA provides that the relators' complaint must be filed under seal and served on the government, but not the defendant, to provide the government an opportunity to investigate the allegations and decide whether to join the case without tipping off the defendant.[141] To assist the government in evaluating the case, the relator must provide the government with "written disclosure of substantially all material evidence and information the person possesses."[142]

If the government joins the case, it has primary responsibility for prosecuting the action, but the relator may remain involved, with the rights of a party subject to certain limitations.[143] If the government does not join, the relator has the right to proceed without the government, although the government may intervene at a later time for "good cause" and must approve a settlement or dismissal.[144]

Second, the 1986 amendments reform the bounty that whistleblowers receive for thwarting their employers' "conspiracy of silence." The amendments provided that a relator is entitled to a guaranteed minimum reward of 15 percent of the proceeds of the action if the government joins the case and up to 25 percent depending on the relator's contribution. If the government declines to join the case and the relator succeeds on his or her own, the relator is entitled to between 25 and 30 percent of the proceeds depending upon his or her contribution.[145] The amendments also provided that in addition to any award, a prevailing relator is entitled to reasonable attorneys' fees, payable by the defendant.[146]

Third, the amendments protect employees from employer retaliation. Defense contractor employees testified that few could afford to "put their head

---

140. *See id.* at 26, *as reprinted in* 1986 U.S.C.C.A.N. at 5291.

141. 31 U.S.C. § 3730(b)(2) (2012); S. REP. NO. 99-345, at 23–24, *as reprinted in* 1986 U.S.C.C.A.N. at 5288–89.

142. 31 U.S.C. § 3730(b)(2).

143. *Id.* § 3730(c).

144. *Id.* §§ 3730(b)(1), 3730(c)(3).

145. *Id.* § 3730(d); S. REP. NO. 99-345, at 27, *as reprinted in* 1986 U.S.C.C.A.N. at 5266, 5292. To address concerns about awarding certain types of whistleblowers, the amended act restricts awards to persons who were the planners and initiators of the fraud or were convicted of the underlying conduct. 31 U.S.C. § 3730(d)(3).

146. 31 U.S.C. § 3730(d); S. REP. NO. 99-345, at 29, *as reprinted in* 1986 U.S.C.C.A.N. at 5294. To discourage frivolous suits, if the relator proceeds without the government, a prevailing defendant is eligible for fees if a court finds that the action was "clearly frivolous, vexatious, or brought for purposes of harassment." 31 U.S.C. § 3730(d)(4); *see* S. REP. NO. 99-345, at 29, *as reprinted in* 1986 U.S.C.C.A.N. at 5294.

on the chopping block" without some assurance that their risk would pay off.[147] To address this problem, the amended FCA created a cause of action for employees who suffer retaliation as a consequence of reporting information about a potential violation of the FCA.[148] Section 3730(h) protects employees from harassment, demotion, loss of employment, or other retaliation in the workplace and entitles them to whatever remedy will make them whole, including reinstatement, double back pay, and attorneys' fees.[149]

Numerous states and the District of Columbia have followed the federal government's lead, adopting their own versions of the FCA authorizing whistleblowers to bring suits in the name of the state government.[150] Such statutes typically also provide protection from workplace retaliation for pursuing these claims.[151]

b. Dodd-Frank Securities Whistleblower Incentives and Protections

In 2000 and 2001 massive accounting fraud at several large corporations rocked securities markets, costing shareholders and employees billions of dollars and undermining the public's trust in financial markets.[152] Tracing the complex financial machinations proved especially difficult. Thus, as part of a larger effort to stem corporate wrongdoing, Congress passed the "Public Company Accounting Reform and Investor Protection Act," commonly known as the Sarbanes-Oxley Act (SOX) of 2002.[153] SOX imposed stronger reporting requirements and stiffer criminal penalties to prevent corporate fraud. SOX also established a whistleblower program to pierce the "corporate code of silence" by encouraging well-placed insiders to assist in unraveling these complex schemes.[154]

---

147. *False Claims Reform Act: Hearing on S. 1562 Before the Subcomm. on Administrative Practice and Procedure*, 99th Cong., 1st Sess. (1985).

148. S. REP. NO. 99-345, at 5, *as reprinted in* 1986 U.S.C.C.A.N. at 5280 (noting the concern of employees of defense contractors breaching the "conspiracy of silence" that made them afraid to report fraud against the government and thus made that fraud difficult to detect).

149. 31 U.S.C. § 3730(h).

150. *See States with False Claims Acts*, TAF EDUC. FUND, www.taf.org/states-false-claims-acts [https://perma.cc/GK33-M46C] (last visited Sept. 30, 2016) (collecting state false claims acts).

151. *See, e.g.*, CAL. GOV'T CODE § 12653 (2016); N.Y. STATE FIN. LAW § 191 (2010); NEV. REV. STAT. § 357.250 (2015).

152. *See* KURT EICHENWALD, CONSPIRACY OF FOOLS (2005); Dan Ackman, *Worldcom, Tyco, Enron—R.I.P*, FORBES (July 2, 2002), http://www.forbes.com/2002/07/01/0701topnews.html [https://perma.cc/N93K-S8CX].

153. Pub. L. No. 107-204, 116 Stat. 745 (2002).

154. Senator Patrick Leahy noted that:

> [W]e include meaningful protections for corporate whistleblowers. . . . We learned from Sherron Watkins of Enron that these corporate insiders are the key witnesses that need to be encouraged to report fraud and help prove it in court. Enron wanted to silence her as a whistleblower because Texas law would allow them to do it. . . . There is no way we could have known about this without that kind of a whistleblower.

SOX provides a cause of action to employees who suffer retaliation for reporting wrongdoing.[155] SOX further punishes any harmful action against anyone who engages in lawful acts to provide "to a law enforcement officer any truthful information relating to the commission or possible commission of any federal offense."[156] In addition, SOX requires companies to create internal reporting systems through which employees can report information about misconduct.

In 2008, another wave of scandals at the largest financial institutions and investment funds revealed greater need for financial regulation and better information about fraudulent activities.[157] In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), which created a bounty for whistleblowers who report violations of securities laws and commodities and futures trading laws.[158] Under Dodd-Frank, whistleblowers who voluntarily provide the SEC or the Commodity Futures Trading Commission (CFTC) with "original information" that "leads to successful enforcement" with more than $1 million in sanctions recovered by the agency receive up to 30 percent of the amount recovered by the agency and in related actions.[159] Like those in the FCA, the Dodd-Frank whistleblower provisions protect whistleblowers from retaliation in the employment context. Unlike the FCA, however, Dodd-Frank does not provide private individuals the right to file a suit in the name of the government, but rather creates a process for reporting information to the agency.

To implement the Dodd-Frank whistleblower provisions, the SEC and CFTC have promulgated regulations designed to protect and encourage whistleblowers. For example, SEC rules provide a mechanism for whistleblowers to report anonymously.[160] Rule 21F-17 prohibits any interference with providing information to the SEC, even when the restriction is done through legal means, such as the enforcement of confidentiality

148 CONG. REC. S7350 (2002). *Time* named "The Whistleblowers," including Sherron Watkins of Enron and Cynthia Cooper of WorldCom, as "Persons of the Year." *See* Richard Lacayo & Amanda Ripley, *Persons of the Year 2002: The Whistleblowers*, TIME (Dec. 30, 2002), http://content.time.com/time/magazine/article/0,9171,1003998,00.html [https://perma.cc/3Z9Z-KMAJ].

155. *See* STEPHEN M. KOHN ET AL., *Legislative History of SOX Whistleblower Protections*, *in* WHISTLEBLOWER LAW 1, 5 (2004).

156. *See* PRACTISING LAW INST., CORPORATE WHISTLEBLOWING IN THE SARBANES-OXLEY/DODD-FRANK ERA (2d ed. 2011).

157. *See* HARRY MARKOPOLOS, NO ONE WOULD LISTEN: A TRUE FINANCIAL THRILLER (2011) (detailing the Madoff Ponzi scheme); ANDREW ROSS SORKIN, TOO BIG TO FAIL: THE INSIDE STORY OF HOW WALL STREET AND WASHINGTON FOUGHT TO SAVE THE FINANCIAL SYSTEM—AND THEMSELVES (2010).

158. Pub. L. No. 111-203, §§ 748, 922, 124 Stat. 1376, 1739, 1841 (2010).

159. 15 U.S.C. § 78u-6 (2012); 7 U.S.C. § 26 (2012).

160. *See* 17 C.F.R. § 240.21F-7 (2016); *see also id.* § 165.4 (anonymous reporting to the CFTC).

agreements.[161] The chief of the SEC's Office of the Whistleblower made clear that protecting the public from financial fraud was more important than preserving trade secrets in NDAs, warning that: "[W]e are actively looking for examples of confidentiality agreements, separat[ion] agreements, employee agreements that . . . , in substance say 'as a prerequisite to get this benefit you agree you're not going to come to the commission or you're not going to report anything to a regulator.'"[162]

c. IRS Whistleblower Informant Awards Program

In an effort to detect and prosecute violations of the Internal Revenue Code, which falls outside of the ambit of the FCA,[163] Congress adopted a tax fraud whistleblower provision as part of the Tax Relief and Health Act of 2006.[164] Under these whistleblower provisions, persons who provide information to the IRS about tax fraud or underpayments that exceed $2 million are eligible for an award of 15 to 30 percent of the amount the IRS collects as a result of the information provided. Unlike those in the FCA, the IRS whistleblower provisions do not provide individuals the right to file suit in the name of the government. The IRS whistleblower provisions also do not include an antiretaliation provision. Whistleblowers are, however, shielded from exposure by provisions protecting confidential informants.[165]

II.
THE AMORPHOUS STATE OF THE PUBLIC POLICY EXCEPTION

The routine use of blanket NDAs by a broad swath of enterprises throughout the economy undermines society's interest in reporting illegal activity. This practice jeopardizes protection of civil rights, public health, workplace safety, integrity of securities markets, tax compliance, and adherence to government contracts. Employees and contractors are often in the best position to know of illegal activity, yet typical NDAs and corporate onboarding practices[166] discourage activities that might be seen to subtract from the company's bottom line. Furthermore, as reflected in the FCA's

161. *Id.* § 240.21F-17(a) ("No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce a confidentiality agreement . . . with respect to such communications.").

162. *See* Brian Mahoney, *SEC Warns In-House Attys Against Whistleblower Contracts*, LAW360 (Mar. 14, 2014), http://www.law360.com/articles/518815/sec-warns-in-house-attys-against-whistleblower-contracts [https://perma.cc/AWZ2-S44B].

163. *See* 31 U.S.C. § 3729(d) (2012).

164. *See* 26 U.S.C. § 7623 (2012).

165. *See Confidentiality and Disclosure for Whistleblowers*, IRS (Feb. 20, 2016), https://www.irs.gov/uac/Confidentiality-and-Disclosure-for-Whistleblowers [https://perma.cc/6BLL-RTMR].

166. *See infra* Part III.A.

material evidence provision,[167] the government needs concrete evidence—typically documents—to investigate illegal activity effectively.

This Section explores how the law and the courts have historically addressed the tension between trade secret protection and reporting of illegal activity. Part II.A looks within trade secrecy and contract law for recognition of a public policy exception for reporting violations of law. Part II.B explores whistleblower laws and their interpretation.

A. Trade Secrecy and Contract Law

Although the UTSA lacks any express exceptions to trade secret liability,[168] courts have long recognized that trade secret protection can "implicate the interest in freedom of expression or advance another significant public interest"[169] and developed a limited privilege to disclose trade secrets.[170] This privilege, however, is murky. The *Restatement (Third) of Unfair Competition* notes that the exception:

> [D]epends 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.[171]

This framing, however, 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 even to the government could be sued over their breach of an NDA. The prospective whistleblower would likely have to consult an attorney, with the attendant costs, and could still face some exposure. Moreover, most prospective whistleblowers will not even be aware of this exception to their NDA without such a consultation.

Similarly, courts sometimes look to general contract law principles, which hold that "bargains tending to stifle criminal prosecution, whether by suppressing investigation of crime or by deterring citizens from their public

---

167. *See supra* Part I.B.2.i.

168. *See supra* Part I.A.3.

169. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40, cmt. c (1995).

170. *See* JERRY COHEN & ALAN S. GUTTERMAN, TRADE SECRETS PROTECTION AND EXPLOITATION (1997); JAGER, *supra* note 42, § 3:14; DAVID W. QUINTO & STUART H. SINGER, 1 TRADE SECRETS: LAW AND PRACTICE § 3.02 (2d ed. 2012). Some other nations expressly provide for a public policy exception. *See, e.g.*, Israel Commercial Torts Law, § 7(2)(2), 5759-1999 ("A person shall not be liable for misappropriation of a trade secret if . . . [u]se of the trade secret is justified as a matter of public policy.").

171. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40, cmt. c.

duty of assisting in the detection or punishment of crime, are void as against public policy."[172] Nonetheless, like the *Restatement (Third) of Unfair Competition* balancing test, whistleblowers have to evaluate myriad ambiguous and subjective factors—including what constitutes a criminal law violation—to determine whether they will be excused from compliance with their NDA.

The next Section considers whether whistleblower statutes provide reliable insulation from trade secret violations for reporting illegal activity.

B. Whistleblower Laws

Along with rewarding those who report evidence of illegal behavior, many whistleblower laws protect employees from retaliation for reporting alleged violations of law to the government. The FCA prohibits discrimination in the terms and conditions of employment for engaging in lawful acts related to pursuit of a qui tam action and entitles the person being discriminated against to "all relief necessary to make the [person] whole."[173] In addition to the FCA, many other statutes that reward whistleblowing also protect whistleblowers against retaliation.[174] The Clean Water Act of 1972 was the first environmental regulation to protect whistleblowers against retaliation.[175] More recently, the American Recovery and Reinvestment Act of 2009[176] and the Pipeline Safety Improvement Act of 2002[177] have included similar provisions.

These statutory protections, however, do not expressly immunize whistleblowers who breach NDAs by reporting illegal activity to the government.[178] While several cases have recognized a public policy protecting

---

172. 7 WILLISTON ON CONTRACTS § 15:8 (4th ed. 1990) (citing Armstrong v. Sexson, No. S-06-2200, 2007 WL 1219297 (E.D. Cal. Apr. 25, 2007), where the court found that the evidentiary value of photographs outweighed a pharmacy's contractual promise to keep customers' information private); *cf.* Lachman v. Sperry-Sun Well Surveying Co., 457 F.2d 850, 852–54 (10th Cir. 1972) (affirming the district court's dismissal of a breach of NDA claim on the ground that "that public policy 'will never penalize one for exposing wrongdoing . . . ;'" the defendant-employee revealed that the plaintiff drilling company was illegally slant-drilling an adjoining property).

173. 31 U.S.C. § 3730(h) (2012). In response to court decisions narrowly interpreting the provision, Congress amended the provision in 2009 to clarify that the law protects agents and contractors as well as "employees" and to make clear that conduct short of filing a False Claims Act case was protected. Pub. L. No. 111-21, § 4(d), 123 Stat. 1616, 1623–24 (2009). A 2010 amendment added a three-year statute of limitations. Pub. L. No. 111-203, § 10279A, 124 Stat. 1376, 2079 (2010).

174. *See* 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).

175. 33 U.S.C. § 1251 (2012) (discussing the broad scope of the legislation and its goal of restoring and maintaining the integrity of the country's waters); *id.* § 1367(a) (prohibiting an employer from firing an employee for instituting a proceeding under the Clean Water Act); *see* FREDERICK D. LIPMAN, WHISTLEBLOWERS: INCENTIVES, DISINCENTIVES, AND PROTECTION STRATEGIES 185 (2012).

176. Pub. L. No. 111-5, § 1553(a), 123 Stat. 115, 297 (2009).

177. Pub. L. No. 107-355, § 6, 116 Stat. 2985, 2989 (2002) (codified at 49 U.S.C. § 60129 (2012)).

178. *See* Michael R. Grimm et al., *Courageous Whistleblowers Are Not "Left Out in the Cold": Legitimate Justifications Exist for Collecting Evidence of False Claims Act Violations*, 39 FALSE CLAIMS ACT & QUI TAM Q. REV. 113 (2005); SYLVIA, *supra* note 135, § 11:94.

such whistleblowers,[179] the contours of the defense are unclear. As with trade secrecy and contract law, courts tend to use balancing tests to assess whether an exception should apply in a paricular case.[180] The factors to be balanced vary across tests and can be subjective.

Not only do differing tests lead to uncertain consequences for the whistleblowers who risk their livelihoods,[181] but the application of a balancing test, as opposed to a clear safe harbor, is itself problematic. A whistleblower considering reporting information about misconduct to the government will not necessarily be represented by counsel at the time they need to decide what information to provide to a lawyer or to the government and is 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*,[182] 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.[183] She reported these concerns internally, but her warnings went unheeded. Upon learning that her position was being eliminated, she hurriedly downloaded a large number of confidential files that could support her suspicion. 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. Shortly thereafter, Cafasso filed a qui tam action. 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 and reviewing these documents with her attorney.

---

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

180. *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).

181. *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).

182. *See* No. CV06-1381, 2009 WL 1457036 (D. Ariz. May 21, 2009), *aff'd*, 637 F.3d 1047 (9th Cir. 2011).

183. *See id.* at *2.

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

> Public 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.[184]

The court granted GDC4S summary judgment on its breach of contract claim. It also held that Cafasso's actions caused irreparable harm and were not immunized by the FCA.[185]

The court ordered Cafasso to pay $300,000 in attorneys' fees for the breach of contract action.[186] Ironically, 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.[187]

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.

The Ninth Circuit affirmed the district court rulings.[188] The court declined to adopt a public 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.[189] The court emphasized the overbreadth of the document retrieval, notwithstanding that Cafasso was

184. *Id.* at *14.

185. *Id.* at *15.

186. *See* 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 as a result of Cafasso having devoted over 5,000 hours during the prior three years to the litigation and the depletion of her savings. *Id.*

187. *Id.* at *7.

188. *Cafasso*, 637 F.3d at 1047.

189. *Id.* at 1062.

under substantial time pressure in gathering the documents. The court expressed concern about the sensitivity of the information,[190] yet it was all information that Cafasso was authorized to view. She limited disclosure to her attorney (who was also duty-bound to protect the information) and the government through a sealed qui tam filing. The court concluded that:

> An 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.[191]

Such a "particularized showing" puts whistleblowers in the unenviable position of having to carefully screen documents, often under 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 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.[192] However, the court allowed the parties to determine through discovery if the relator took documents unrelated to the FCA claim.[193] 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 wrongdoing to the government. Having to respond to discovery, pay a lawyer to do so, and face possible liability would be enough to discourage many whistleblowers from reporting at all.

---

190. *See id.*

191. *Id.*

192. *See* No. 11-cv-01987, 2013 WL 5645309, at *25–26 (N.D. Cal. Oct. 16, 2013); *see also* United States *ex rel.* Head v. Kane Co., 668 F. Supp. 2d 146, 152 (D.D.C. 2009) ("Enforcing a private agreement that requires a qui tam plaintiff to turn over his or her copy of a document, which is likely to be needed as evidence at trial, to the defendant who is under investigation would unduly frustrate the purpose [of the FCA]".).

193. *See Siebert*, 2013 WL 5645309, at *25–26.

By contrast, the court in *United States ex. rel. Ruhe v. Masimo Corp.*[194] held that the FCA's policy purpose outweighed the company's interest in preserving its trade secrets. Three former sales representatives filed an FCA case against the corporation for misrepresenting the accuracy of medical tests billed to Medicare. To prove their assertions and meet the pleading requirements of Federal Rule of Civil Procedure 9(b), the relators attached documents, copied from company hard drives, to an amended complaint. The company moved to strike as scandalous any use of the documents in the FCA case because the relators violated their NDA by copying the documents.

While citing *Cafasso*, the court emphasized the general law reporting public policy exception.[195] The court did not inquire into whether the appended documents were the only documents that the relators copied. Instead, the court found that the documents could not be "scandalous." They were the opposite: they aimed to serve the public good by exposing the company's fraud against the government and consumers. "The strong public policy in favor of protecting whistleblowers who report fraud against the government" dwarfed the corporation's interest in enforcing its confidentiality agreement.[196] The court remained silent on *Cafasso*'s reasonableness analysis and instead cited the Ninth Circuit to show "that public policy merits finding individuals such as relators to be exempt from liability for violation of their nondisclosure agreement."[197] The court concluded that "an exemption is necessary given that the FCA requires that a relator turn over all material evidence and information to the government when bringing a qui tam action."[198]

C. A Catch-22 for Whistleblowers

While some cases recognize a public policy exception, the contours of the exception are murky. In a recent case addressing counterclaims against a relator for providing documents to the government, the court observed that "both sides" had attempted to persuade the court that the matter was resolved by "settled law."[199] In the court's view, however, "a close examination of the cases suggests that this matter is by no means settled, and that the status of counterclaims against FCA relators often turns on fine distinctions in the defendant's pleadings."[200]

Thus, while there are potential defenses to breach of contract and trade secret claims against whistleblowers who use proprietary information solely for

194. 929 F. Supp. 2d 1033 (C.D. Cal. 2012).
195. *Id.* at 1039.
196. *Id.* (citing United States v. Cancer Treatment Ctrs. of Am., 350 F. Supp. 2d 765, 773 (N.D. Ill. 2004)).
197. *Id.*
198. *Id.* (citing 31 U.S.C. § 3730(b)(2)).
199. *See* United States *ex rel.* Ruscher v. Omnicare, Inc., No. 4:08-cv-3396, 2015 WL 4389589, at *3 (S.D. Tex. July 15, 2015).
200. *Id.* at *3; *see also id.* at *5.

reporting allegedly illegal activity, the prospect of having to hire a lawyer to defend against such claims has a significant deterrent effect on whistleblowers.[201] As the *Cafasso* case illustrates, the act of sharing the allegedly incriminating information with an attorney who is duty-bound to maintain the proprietary status of trade secret information can expose the whistleblower to liability, even though the very test for assessing availability of a public policy defense requires the careful assessment that lawyers are uniquely qualified to evaluate.

Lawyers for both companies and employees have recognized that the legal landscape is murky and varies by jurisdiction. Lawyers who advise companies about enforcing trade secret protections have expressed concern about the uncertainty around whether pursuing counterclaims will be deemed retaliatory, and lawyers for whistleblowers have had to navigate the uncertain landscape when advising clients about providing documents that support allegations of misconduct.[202] And many whistleblowers do not have the benefit of legal advice at the time they take documents in support of their allegations. While taking documents to support a qui tam action has been characterized dismissively as merely "self-help" discovery, the reality is that without documents, it may be difficult to persuade the government of the merits of the allegations, adequately support a complaint, or even ensure that such documents exist at the time the allegations are investigated.[203]

The lack of clarity on what is a "reasonable" disclosure of protected information highlights the importance of reforming trade secret law to provide clearer protection for whistleblowers and guidance for courts.

III.
THE INTERPLAY OF TRADE SECRECY AND WHISTLEBLOWING

Both law enforcement and trade secrecy play vital roles in a well-functioning society. As initially conceived and developed, trade secret protection augments other intellectual property protections in promoting innovation. It encourages companies to invest in their workforce and facilitates a productive environment for technological progress. At the same time, overly broad trade secrecy protection interferes with law enforcement. The lack of an

---

201. Such counterclaims are also viewed as a way to defend against the underlying FCA action. *See supra* note 31.

202. *See* Ben James, *5 Questions to Ask Before Suing over Whistleblower Theft*, LAW360 (May 21, 2014), http://www.law360.com/articles/533633/5-questions-to-ask-before-suing-over-whistle blower-theft [https://perma.cc/QU9D-GQWW] (reporting views of counsel for defendants and whistleblowers that the law is unclear).

203. Documents reflecting misconduct can disappear, and the prospects of a successful spoliation claim later can be slim. *See, e.g.*, United States *ex rel.* Aflatooni v. Kitsap Physicians Serv., 314 F.3d 995 (9th Cir. 2002) (affirming rejection of plaintiff's spoliation claim where defendant contended documents were destroyed in the normal course of business according to record retention policies and that defendant was not on notice of litigation because outside counsel investigation concluded there was no fraud).

unambiguous safe harbor for reporting illegal conduct can discourage those who become aware of wrongdoing from coming forward with credible evidence.

This Section uses the lens of psychology to explore the interplay between trade secret protection and reporting of illegal activity by company employees and contractors. Part III.A describes the array of forces affecting many employees and contractors in today's business environment. Part III.B examines empirical studies of whistleblowing.

A. The Psychology of Whistleblowing

Those considering whether to report corporate fraud or malfeasance have historically faced several daunting challenges and risks.[204] 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 the firm. 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.[205]

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. In order to ensure compliance with trade secret law,[206] companies routinely require that corporate employees and contractors sign an NDA before they can begin work.[207] This process is typically handled through

204. *See* Yuval Feldman & Orly Lobel, *The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegality*, 88 TEX. L. REV. 1151 (2010).

205. *See* Alexander Dyck et al., *Who Blows the Whistle on Corporate Fraud?*, 65 J. FIN. 2213, 2240–45 (2010).

206. As noted previously, *see supra* Part I.A.3, trade secret law requires that the enterprise take reasonable precautions to prevent disclosure of trade secret information. Execution of NDAs by all employees and contractors who might come in contact with trade secrets is widely considered to be a critical element in establishing trade secrecy protection.

207. *See* Steven D. Maurer & Michael T. Zugelder, *Trade Secret Management in High Technology: A Legal Review and Research Agenda*, 11 J. HIGH TECH. MGMT. RES. 155, 162 (2000) ("Perhaps the most fundamental and most successful administrative strategy for protecting trade secrets is to require employees, vendors, and others to sign a 'non-disclosure' agreement."). *See generally* 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 4.02 (2016) (citing a 1965 survey of Employee Patent and Secrecy agreements finding that 83 percent of corporations required employees to sign NDAs); Terry Morehead Dworkin & Elletta Sangrey Callahan, *Buying Silence*, 36 AM. BUS. L.J. 151 (1998) (noting the increase in the corporate use of employee NDAs and that such agreements are especially common among large corporations). Because most employment contracts are not available to the public, the extent of NDA use is difficult to assess accurately on a general level. A recent study examining 874 employment contracts of chief executive officers (CEOs) at S&P 1500 public corporations, which are required by law to make those agreements publicly available, showed that 87.1 percent included NDA language. *See* Norman D. Bishara et al., *An Empirical Analysis of*

a human resources employee who explains the terms of the agreement.[208] Many larger enterprises use formal orientation programs.[209] 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 confusing, intimidating documents, and employees who sign them often lack any leverage to negotiate terms.[210]

The express terms of NDAs appear to bar whistleblowing. Aside from being formal and often fairly technical, the typical NDA is broadly worded.[211] Such agreements expressly reference and bar the disclosure of every conceivable form of information that might be deemed confidential. They often

---

Noncompetition Clauses and Other Restrictive Postemployment Covenants, 68 VAND. L. REV. 1, 4 (2015).

208. *See* Eric Ostroff, *The One Question All Businesses Must Ask About Protecting Trade Secrets*, ENTREPRENEUR.COM (Jan. 29, 2015), http://www.entrepreneur.com/article/242358 [https://perma.cc/RH3Y-HLWY] (recommending "trade-secrets training [be] included in the onboarding process and repeated regularly").

209. *See* TALYA N. BAUER, ONBOARDING NEW EMPLOYEES: MAXIMIZING SUCCESS 2, 9–10 (2010) (reporting that 93 percent of organizations use a new employee orientation program).

210. *See* Bishara et al., *supra* note 207, at 20 (noting the "relative ease" with which corporations can secure NDAs from incoming employees).

211. *See id.* at 43 ("[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." *See* Rich Stim, *Sample Confidentiality Agreement (NDA)*, NOLO, http://www.nolo.com/legal-encyclopedia/sample-confidentiality-agreement-nda-33343.html [https://perma.cc/NB4U-A2C8] (last visited Sept. 30, 2016); *see also* 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) ("[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 overbreadth. *Id.* Such challenges, however, are exceedingly rare. Mounting such a challenge is expensive.

list a broad range of specific types of information—such as customer lists, marketing plans, production methods, formulas, techniques, budgets, data, programs, and financial statements—and include a catch-all category of any information deemed proprietary by the employer. NDAs do 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 explaining their concerns to an attorney could potentially breach the NDA. And based on the murkiness of a 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 will be to never disclose information about the company's business practices. The end result, likely intended by the company, is that the NDA fosters 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 NDA signing occurs during a comprehensive and meticulously planned "onboarding" process aimed at inculcating loyalty and corporate pride among new employees.[212] This process can extend for months, or even years.[213] 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.[214] These efforts can be in the form of training sessions, expanded compensation opportunities based on employee engagement, and specifically focused evaluation criteria.[215] The overarching goal is to create

212. *See* BAUER, *supra* note 209, at 2.

213. *See id.* at 2, 9 (highlighting Zappos's "intensive" onboarding course that lasts for five weeks and L'Oreal's two-year process).

214. *See* 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.").

215. *See id.* at 1201–02.

lasting bonds between the company and its workers such that employees align their thinking with that of the owners of the firm.[216] In some instances, these programs have been compared to religious conversions or indoctrinations into cults.[217]

One commentator has noted that it is common, for instance, for workers who identify with their employer on this level to proceed as if they were part of "an intimate relationship with the firm, not simply a contractual exchange of money for labor."[218] These employees tend to see their identities and self-worth as being directly tied to the employer and are often more willing to make personal sacrifices that benefit the firm.[219] United Parcel Service employees are said to "bleed brown,"[220] those working at Yahoo! are referred to as "Yahoos,"[221] Google employees are "Googlers,"[222] and so on. The hope is that managers and coworkers become like family, and trust permeates every element of the employer/employee relationship, thereby discouraging any member of the "family" from undermining the cohesion of those bonds by exposing corporate wrongdoing.

Even the most fervent onboarding and internal branding efforts, however, may fail to prevent some employees from questioning what they perceive to be fraudulent activity by or on behalf of the firm.[223] But there is much to consider

---

216. *See 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.").

217. *See 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 ("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.").

218. Crain, *supra* note 214, at 1228.

219. *See id.*; *see also* Daniel M. Cable at al., *Reinventing Employee Onboarding*, MIT SLOAN MGMT. REV., Mar. 19, 2013, at 24 ("When newcomers are 'processed' to accept an organization's identity, they are expected to downplay their own identities, at least while they are at work.").

220. *See* Crain, *supra* note 214, at 1228.

221. *See* Libby Sartain, *Branding from the Inside out at Yahoo!: HR's Role as Brand Builder*, 44 HUM. RESOURCE MGMT. 89, 91 (2005). In 2005, the senior vice president of human resources and chief people officer at Yahoo! Inc. noted: "By branding the meaning, promise, and overall employee experience, organizations can engage and enchant employees, giving deeper meaning to the promise that lies behind their daily efforts. This gives jobs a deeper resonance and results in an emotional connection that compels commitment." *Id.* at 90.

222. *See Life at Google*, GOOGLE CAREERS, http://www.google.com/about/careers/lifeatgoogle [https://perma.cc/N2B3-3NL4] (last visited Sept. 30, 2016).

223. Life within corporations and other bureaucracies is far more complex than these family metaphors can capture. Competition and personalities often produce multifaceted internal politics and fractured loyalties. *See* Henry Mintzberg, *The Organization as a Political Arena*, 22 J. MGMT. STUD.

in such circumstances. For the vast majority of whistleblowers, the act of coming forward with evidence of corporate wrongdoing represents a perilous, inherently risky endeavor fraught with the potential for adverse professional consequences.[224] Whistleblowers must reconcile their desire to do what they believe is right with bleak potential consequences. Many will lose their jobs, be demoted, and jeopardize their potential to work in that industry or any position that depends on unconditional corporate loyalty. Those coming forward also risk the continued access to company health insurance, bonuses, and a variety of other corporate benefits.[225] At the same time, many whistleblowers experience deleterious health issues, stress-related psychological challenges, and severe relationship strains.[226] For those who have signed an NDA, and even for some who have not, there is also the substantial risk that the company will respond to accusations by suing the individual who brought the evidence of alleged corporate wrongdoing to light.[227]

Beyond the direct financial and career consequences of reporting illegal company conduct, whistleblowers must often contend with serious psychological, marital, and social consequences. It is not uncommon for whistleblowers to be shunned by coworkers and workplace friends concerned with maintaining good standing with supervisors,[228] or to be blacklisted with respect to subsequent job opportunities.[229] In addition, whistleblowers may face varying forms of harassment, accusations of dishonesty, and, ultimately, the need to relocate. In especially ugly cases, whistleblowers' family members and friends experience threats and other forms of retaliation as a result of the

133 (1985); Janet P. Near & Marcia P. Miceli, *Organizational Dissidence: The Case of Whistle-Blowing*, 4 J. BUS. ETHICS 1 (1985).

224. *See, e.g.*, Geoffrey Christopher Rapp, *Mutiny by the Bounties? The Attempt to Reform Wall Street by the New Whistleblower Provisions of the Dodd-Frank Act*, 2012 B.Y.U. L. REV. 73, 113 (noting that most whistleblowers ultimately lose their jobs, and citing two studies finding that 82 percent and 90 percent of whistleblowers, respectively, were fired or otherwise experienced negative job-related repercussions subsequent to blowing the whistle).

225. *See id.*

226. *See* Richard D. Fincher, *Mediating Whistleblower Complaints: Integrating the Emotional and Legal Challenges*, 64 DISP. RESOL. J. 62, 65 (2009).

227. *See* Rapp, *supra* note 224, at 114 ("Up to twenty-seven percent of whistleblowers are sued by their employers.").

228. *See* MARCIA P. MICELI & JANET P. NEAR, BLOWING THE WHISTLE: THE ORGANIZATIONAL & LEGAL IMPLICATIONS FOR COMPANIES AND EMPLOYEES 79–89 (1992); Jennifer M. Pacella, *Inside or out? The Dodd-Frank Whistleblower Program's Antiretaliation Protections for Internal Reporting*, 86 TEMP. L. REV. 721, 754 (2014) (noting that if a whistleblower's identity becomes known within the workplace, she may be exposed to "psychological pressure, social ostracism, exclusion from social gatherings, emails, or carpools, silent treatment, transfers to other locations, and workplace harassment or threats").

229. *See* Dyck et al., *supra* note 205, at 2240–45; James Gobert & Maurice Punch, *Whistleblowers, the Public Interest, and the Public Interest Disclosure Act 1998*, 63 MOD. L. REV. 25, 35 (2000) (characterizing whistleblowing as "professional suicide").

employee's decision to bring corporate malfeasance to light.[230] The stresses of whistleblowing severely test family relationships.

B. Empirical Research on Whistleblowing

Despite the costs and risks of reporting illegal activity by employers, some employees and consultants step forward. "The surprising part," note the authors of a recent empirical study examining 230 corporate fraud scenarios at large U.S. companies, is "not that most employees do not talk; it is that some talk at all."[231] We would ideally like to know the effect of NDAs (and related company policies) on the full range of employees' and consultants' propensities to report illegal conduct, but for the same reasons that these actors are discouraged from reporting, it is difficult to survey the target audiences. There have, however, been several studies that focus on those employees and consultants that overcome the costs and risks and come forward. These studies show that it takes a strong-willed and courageous person to blow the whistle on her or his company. Whistleblowers do so for a number of mostly altruistic, moral, and well-meaning reasons, and many suffer serious consequences.

A 2008 study[232] assessing how whistleblower motivation should influence regulatory regimes identified three principal drivers: (1) a moral, or "conscience cleansing" rationale that results in employee action so as not to "go along with" immoral activity;[233] (2) a desire to benefit society as a whole;[234] and (3) a desire to punish bad actors or those who have done wrong by the employee in the past.[235] Similarly, a 2010 study[236] drawing on interviews with twenty-six whistleblowers[237] who initiated federal qui tam cases in the pharmaceutical industry found four principal factors: integrity, altruism/public safety, justice, and self-preservation.[238]

---

230. *See* Orly Lobel, *Citizenship, Organizational Citizenship, and the Laws of Overlapping Obligations*, 97 CALIF. L. REV. 433, 486–87 (2009).

231. *See* Dyck et al., *supra* note 205, at 2245.

232. *See* Anthony Heyes & Sandeep Kapur, *An Economic Model of Whistle-Blower Policy*, 25 J.L. ECON. & ORG. 157, 164 (2008).

233. *See id.* (noting that decisions based on this motivation "may depend on cultural, religious, and other forces"); C. Fred Alford, *Whistle-Blower Narratives: The Experience of Choiceless Choice*, 74 SOC. RES. 223, 226 (2007).

234. *See* Heyes & Kapur, *supra* note 232, at 167–68.

235. *See id.* at 168 (suggesting that those driven by this motivation often tend to be "unhappy for reasons unconnected with the firm[']s planned noncompliance with the regulation, but opportunistic in blowing the whistle when doing so creates sufficiently substantial discomfort (cost) for their employer").

236. *See* Aaron S. Kesselheim et al., *Whistle-Blowers' Experiences in Fraud Litigation Against Pharmaceutical Companies*, 362 NEW ENG. J. MED. 1832 (2010).

237. Of those twenty-six, twenty-two were employees of the company that was being sued, while four of those interviewed were "outsiders." *See id.* at 1832.

238. *Id.* at 1834.

In the latter study, 82 percent of the inside whistleblowers came forward only after first raising the relevant issue(s) with supervisors, to no avail.[239] Those interviewed also tended to note that the investigatory process was both extremely time-consuming and exceptionally stressful.[240] Several relators felt as though they were left in the dark during what they deemed to be slow-moving government investigations.[241] More than anything else, though, these whistleblowers' insights coalesced around the issue of personal harm and damage experienced as a result of their actions.[242] Relators reported feeling as though they had "put their career on the line."[243] Some lost their homes and 401(k) retirement saving plans, others divorced their spouses, and 50 percent experienced "stress-related health problems, including shingles, psoriasis, autoimmune disorders, panic attacks, asthma, insomnia, temporomandibular joint disorder, migraine headaches, and generalized anxiety."[244] More than half of those interviewed said their monetary recovery was small when compared with the effort, disruption, stress, and career damage they experienced.[245] In delineating the policy implications of their study, the authors concluded that "the strain the process places on individuals' professional and personal lives may make prospective whistle-blowers with legitimate evidence of fraud reluctant to come forward."[246]

A 2010 study conducted by the National Whistleblowers Center[247] focused on the impact of monetary rewards on potential whistleblowers.[248] The study found that the overwhelming majority of whistleblowers sought to pursue

239. *See id.* These individuals speak of being "shooed aside" and about insistence from management that they follow orders and "do what they were told." *Id.*

240. *See id.* at 1836.

241. *See id.*

242. *See id.* ("The experience of being involved in troubling corporate behavior and a qui tam case had substantial and long-lasting effects for nearly all of the insiders. . . . Eighteen insiders (82 [percent]) reported being subjected to various pressures by the company in response to their complaints. . . . For at least eight insiders, the financial consequences were reportedly devastating." (parentheticals omitted)).

243. *Id.*

244. *Id.*

245. *Id.*

246. *Id.* at 1837. The authors further noted that FCA antiretaliation provisions may not be enough to adequately protect whistleblowing employees. *Id.*; *see also* Aaron S. Kesselheim & David M. Studdert, *Whistleblower-Initiated Enforcement Actions Against Health Care Fraud and Abuse in the United States, 1996–2005*, 149 ANNALS INTERNAL MED. 342, 347 (2008).

247. The National Whistleblowers Center "is a nonprofit, nonpartisan organization dedicated to protecting employees' lawful disclosure of waste, fraud, and abuse." *See About Us*, NAT'L WHISTLEBLOWERS CTR., http://www.whistleblowers.org/about-us [https://perma.cc/CHZ6-J3N7] (last visited Sept. 30, 2016).

248. *See* NAT'L WHISTLEBLOWERS CTR., IMPACT OF QUI TAM LAWS ON INTERNAL COMPLIANCE: A REPORT TO THE SECURITIES EXCHANGE COMMISSION (2010), http://www.whistleblowers.org/index.php?option=com_content&task=view&id=1169 [https://perma.cc/BG94-UDCP]. The study was completed in response to a Securities and Exchange Commission request for comments on "the potential impact of the Dodd-Frank Wall Street Reform Act's whistleblower reward provisions on internal corporate compliance programs." *See id.* at 1.

their concerns through internal channels.[249] The report concluded that the prospects of substantial financial rewards do not primarily drive decisions by employees about reporting corporate fraud and are unlikely to interfere with employee use of internal compliance programs.[250]

A 2013 survey of 6,420 employees across numerous business sectors conducted by the Ethics Resource Center (ERC)[251] came to similar conclusions, finding that 92 percent of those reporting workplace misconduct do so to someone at the company first, with only 9 percent of employees ever reporting issues to the government.[252]

These studies indicate that the overwhelming majority of whistleblowers are loyal employees simply looking to do what they perceive to be the right thing.[253] Yet they face a gauntlet of legal impediments, indoctrination policies, financial risks, and workplace and social pressures discouraging reporting of illegal conduct.[254] In this stressful decision-making setting, the lack of a clear safe harbor from trade secret liability could tip the scales toward silence. The next Section proposes a mechanism for raising this shield without jeopardizing legitimate trade secrecy protection.

IV.
TAILORING A TRADE SECRET PUBLIC POLICY EXCEPTION

The uncertainty surrounding whistleblowers' exposure to trade secrecy violations adds to the corporate, economic, and social pressures discouraging reporting of potentially illegal conduct. At the same time, trade secret owners have reason to be concerned about even well-intentioned, but erroneous, disclosure of commercially significant confidential information. Once such secrets are disclosed, they are very difficult, if not impossible, to protect—competitors who come by the information legitimately are free to use it.[255] Hence, care must be taken to ensure that a public policy exception does not unduly jeopardize appropriate and effective trade secret protection.

---

249. *See id.* at 4 (reporting 89.7 percent of FCA filers had first reported their concerns to supervisors or compliance departments).

250. *See id.* at 24.

251. The Ethics Research Center, founded in 1922, is "America's oldest nonprofit organization devoted to independent research and the advancement of high ethical standards and practices in public and private institutions." *Mission Statement*, ETHICS & COMPLIANCE INITIATIVE, http://www.ethics.org/about/mission-statement [https://perma.cc/VD55-MBLS] (last visited Sept. 30, 2016).

252. *See* ETHICS RESEARCH CTR., NATIONAL BUSINESS ETHICS SURVEY OF THE U.S. WORKFORCE 29 (2013).

253. *See, e.g.*, Terry Morehead Dworkin & Elletta Sangrey Callahan, *Internal Whistleblowing: Protecting the Interests of the Employee, the Organization, and Society*, 29 AM. BUS. L.J. 266, 300–01 (1991) ("Most individuals who blow the whistle are long-time employees, fairly high in the organization, who have a strong sense of organizational loyalty.").

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

255. *See supra* note 90.

It is important to recognize, however, that most whistleblowers are not interested in undermining an employer's lawful commercial advantage.[256] 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.[257] 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.

The roots of the dilemma lie in the evolution of economic and social progress in the century following the Industrial Revolution. Trade secret protection emerged during an era in which the government's role was relatively modest. The requirement that companies undertake reasonable precautions to prevent disclosure of trade secret information naturally led enterprises to require employees and contractors to sign broad NDAs.[258] During the late nineteenth and early twentieth centuries, trade secret protection aligned closely with competitive and innovative progress. The emergence of robust protection for public health, civil rights, workplace safety, privacy, securities regulation, and environmental protection and the expansion of government involvement in the economy—from military procurement to public infrastructure, public health institutions, public safety institutions, and innovation research—has increased the need for employees and contractors to assist in policing private activities. Thus, the blanket protection afforded by the NDA has increasingly come into tension with other important values, such as law enforcement and oversight of compliance with government contracts.

It became imperative to establish a clear safe harbor within trade secret law for employees, contractors, and any other signatories of NDAs to communicate evidence of possible illegal conduct to the government without risk of negative repercussions. Such actors are often in the best position to know about illegal conduct and are uniquely positioned to provide the evidentiary basis, consistent with Fourth Amendment protections, for the government to investigate allegations. Such a safe harbor goes a long way toward deterring illegal activity without undermining legitimate trade secret protection.

Building on legal scholarship regarding law enforcement, Part IV.A develops a legal rule that both insulates whistleblowers from liability and ensures that legitimate trade secrets will not be jeopardized. By authorizing whistleblowers to disclose allegedly illegal conduct to government officials through a confidential channel, the law can balance public interests in law

256. *See supra* Part III.B.
257. *See supra* Part I.A.2.
258. *See supra* Part I.A.1.

enforcement with promoting innovation. Part IV.B shows that the government already has institutions and safeguards in place to effectuate such a safe harbor. Part IV.C proposes draft language for implementing a sealed disclosure/trusted intermediary public policy exception to trade secret protection. Part IV.D explores potential concerns, compares this approach to alternatives, and discusses limitations of the proposed safe harbor.

A. Reconciling Law Enforcement and Trade Secrecy Protection

The *Restatement (Third) of Unfair Competition* balancing test[259] and the *Cafasso* decision[260] needlessly chill reporting of illegal activity by subjecting whistleblowers to a murky balancing framework that does not safeguard trade secrets. Government officials and attorneys are 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 seriously jeopardize trade secrecy.[261] Employees and contractors face termination, retaliation, ostracization, psychological stress, and legal defense costs by even considering blowing the whistle. The law can reconcile these concerns by affording whistleblowers a clear safe harbor for reporting illegal activity through sealed disclosure to counsel and government authorities bound by obligations to maintain the sanctity of true commercial trade secrets.

This approach can be seen as a variant of the seminal conceptual framework that has long formed the basis for law enforcement scholarship. Professors Guido Calabresi and Douglas Melamed divided the law enforcement domain into two sets of choices: (1) who should be entitled to a resource or right and (2) how the entitlement or right should be enforced. The framework considered three enforcement regimes: (a) a property rule, whereby the holder of the entitlement or right could exclude others from violating or invading the interest—i.e., injunctive relief; (b) a liability rule, whereby the holder could enforce their right by an award of compensatory damages; and (c) an inalienability rule, whereby the holder could enforce their right by exclusion, but would not be able to market the right.[262]

As between a company that maintains trade secrets and an employee who has signed an NDA, trade secret law allocates the entitlement to the trade secret information to the company and enforces that entitlement through both

259. *See supra* Part II.A.

260. *See supra* Part II.B.

261. While there is always risk of improper disclosure of information as the circle of people who hold the information grows, we have decades of experience with attorneys, judges, and government officials serving as reliable custodians of trade secrets.

262. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972). The article's title references Claude Monet's series of paintings of the Rouen Cathedral in suggesting that the authors' framework is but one view of a famous edifice.

property and liability rules. Unfortunately, once a secret is divulged to the public, it is not possible to obtain an injunction against those who have learned of the trade secret legitimately—i.e., without engaging in misappropriation. Moreover, although the employee bears liability for the breach, it is unlikely that a liability award will be adequate to compensate for the loss of a significant trade secret. It is often difficult to estimate the full loss, and the employee may well be judgment-proof when confronted with massive liability.

Yet reporting of illegal conduct by a person bound by an NDA might well be addressed at the first stage of the Calabresi and Melamed analysis. The law should allocate the entitlement to report illegal conduct—even if the underlying information is confidential—to the employee or contractor. The problem lies in determining whether the conduct or practices are illegal. The employee or contractor cannot always easily determine whether the law has been or will be violated. And given the evident risks to the whistleblower associated with reporting on the company and disclosing confidential information, the employee or contractor is in a bind.

The problem can be solved through a hybrid entitlement/enforcement rule whereby employees and contractors subject to NDAs would have the absolute entitlement to report evidence of alleged misconduct—even if based on confidential information—to an appropriate government enforcement institution so long as the reporting is done through a confidential communication. The government officials would then be in a position to determine whether the allegations justify further investigation or action. Such action could be undertaken, as is common in administrative (e.g., patent prosecution or FDA review of drugs) and legal (e.g., patent or trade secret litigation) proceedings, subject to appropriate safeguards to protect any legitimate trade secrets.

This mechanism would fully insulate the reporting employee or contractor from liability so long as they used the confidential channel and did not otherwise disclose or use the information outside of NDA limits. Thus, they would not be able to disclose the information in a way that jeopardized its commercial value. Nor would they be able to go to the press or other outlets until such time as the government has determined that the information is not protected by trade secret law. Such a regime obviates the complexity and confusion of the *Restatement (Third) of Unfair Competition* and *Cafasso* standards without jeopardizing trade secret protection.

Two further elements are needed to optimize this exception to trade secret protection. First, it will be important to extend the safe harbor to attorneys with whom potential whistleblowers consult. Such counsel can provide advice on how to navigate the safe harbor and can serve as a confidential communication channel with the government. Second, it will be important to provide signatories of NDAs with notice of the law reporting safe harbor and their entitlement to disclose such information confidentially to the government and

outside counsel. The next Section explores existing institutions that support the implementation of a sealed disclosure/trusted intermediary exception to trade secret protection.

B. Supporting Institutions and Models

Much of the institutional and legal infrastructure for implementing a sealed disclosure/trusted intermediary exception to trade secret protection is already in place. As explored below, the first section establishes that the federal government already has effective safeguards in place for protecting legitimate trade secrets. The second section explains attorney responsibility and judicial process rules for protecting trade secrets. Finally, the third section examines alternative models for insulating whistleblowers from trade secret liability. The privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[263] provide an especially good framework for a sealed disclosure/trusted intermediary exception to trade secret protection. And the SEC's whistleblower program provides useful insight in ensuring that employees and contractors know that NDAs do not shield illegal activity.

1. Governmental Trade Secrecy Law and Policy

Government agencies routinely deal with trade secrets and follow strict rules for ensuring that this information remains confidential.[264] For example, patent applications "shall be kept in confidence by the Patent and Trademark Office and no information concerning the same given without authority of the applicant or owner" subject to limited exceptions.[265] Similarly, the Food and Drug Administration (FDA) conducts its review of drug applications confidentially, preserving trade secrets in manufacturing methods and clinical trial data.[266] The SEC also ensures protection of confidential business

263. Pub. L. 104–191, 110 Stat. 1936 (1966).

264. *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).

265. 35 U.S.C. § 122 (2012).

266. *See* Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 331(j) (2012) (prohibiting the use of "any information acquired under authority of section 344 . . . concerning any method or process which as a trade secret is entitled to protection"). Notwithstanding initiatives to increase transparency at the agency, the FDA maintains protection for trade secrets. *See* TRANSPARENCY TASK FORCE, U.S. DEP'T OF HEALTH & HUMAN SERVS., FDA TRANSPARENCY INITIATIVE: DRAFT PROPOSALS FOR PUBLIC COMMENT REGARDING DISCLOSURE POLICIES OF THE U.S. FOOD AND DRUG ADMINISTRATION 13 (2010) ("Trade secrets include such things as a company's manufacturing processes and precise product formulations. The Task Force believes that trade secrets have limited value for public disclosure, and that the value for public disclosure of other types of data, such as clinical trial results and adverse event reports, is significantly greater. The Task Force believes that data relating to manufacturing methods and processes, which is the direct result of innovative efforts, deserves protection because keeping trade secret information confidential maintains investment in new product development and thus is important to fostering innovation.").

information.[267] The Freedom of Information Act exempts trade secrets from public disclosure.[268]

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 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.[269]

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.[270] The Supreme Court held in *Ruckelshaus v. Monsanto Co*.[271] that trade secrets constitute property interests pursuant to the Takings Clause of the Fifth Amendment.[272] The Court held 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.[273]

---

267. *See* 17 C.F.R. § 200.83(c)(1) (2016) ("Any person who, either voluntarily or pursuant to any requirement of law, submits any information or causes or permits any information to be submitted to the Commission, which information is entitled to confidential treatment . . . , may request that the Commission afford confidential treatment under the Freedom of Information Act to such information for reasons of personal privacy or business confidentiality, or for any other reason permitted by Federal law. . . .").

268. *See* 5 U.S.C. § 552(b)(3)–(4) (2012).

269. 18 U.S.C. § 1905 (2012).

270. *See* Demodulation, Inc. v. United States, 103 Fed. Cl. 794, 811–12 (2012); Tucker Act, 28 U.S.C. § 1491 (2012) (discussing waiver of sovereign immunity with respect to certain lawsuits).

271. 467 U.S. 986 (1984).

272. U.S. CONST. amend. V; *see* Zoltek Corp. v. United States, 442 F.3d 1345, 1352 n.3 (Fed. Cir. 2006) (per curiam) (recognizing that *Monsanto* holds that "government interference with interests 'cognizable as trade-secret property right[s]' could constitute a taking depending on the circumstances" (quoting *Monsanto*, 467 U.S. at 1003–04)).

273. *Monsanto*, 467 U.S. at 1020. The Court's decision focuses on statutory language in the applicable regulatory statute that created an expectation that the agency would protect its trade secrets.

2. Attorney Responsibility and Litigation Protective Orders

Attorneys generally operate in a confidential work environment. They have a responsibility to protect the confidences of their clients[274] and deal with a broad range of proprietary, confidential, and sensitive material. They bear responsibility for knowingly disclosing trade secret information.

The way in which attorneys and courts deal with the crime-fraud exception to the attorney-client privilege[275] serves as a model for the proposed sealed disclosure/trusted intermediary safe harbor. The crime-fraud exception is an evidentiary rule that permits a court to review privileged attorney-client communications where a party establishes that the alleged privileged communications were intended by the client to further a future or ongoing crime or fraud.[276] If this burden is met, the court may examine the communications *in camera*.[277] If the court determines that the privilege does not apply, it may authorize use of the documents in the litigation. Similarly, Federal Rule of Civil Procedure 26(b)(5)(B) provides an *in camera* procedure for review of inadvertently disclosed documents.

Courts routinely deal with the safeguarding of trade secrets in litigation. Without such procedures, the broad scope of discovery of the Federal Rules of Civil Procedure and the public nature of trials would jeopardize all manner of trade secrets in patent, commercial, privacy, and other forms of litigation. Federal Rule of Civil Procedure 26(c) authorizes courts to enter orders "that a trade secret or other confidential research, development, or commercial information not be disclosed or be disclosed only in a designated way." Federal Rule of Civil Procedure 45 authorizes courts to modify a subpoena or specify the conditions of production if the subpoena seeks trade secrets or other confidential information. Courts may conduct *in camera* proceedings to protect trade secrets from public disclosure.[278]

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 served on the defendant until the court so orders."[279] The seal enables the government to investigate the allegations without tipping off the defendant.[280]

---

274. *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").

275. *See* David J. Fried, *Too High a Price for Truth: The Exception to the Attorney-Client Privilege for Contemplated Crimes and Frauds*, 64 N.C. L. REV. 443 (1986) (reviewing the history of the crime-fraud doctrine).

276. *See* United States v. Zolin, 491 U.S. 554 (1989).

277. *See id.* at 565–72.

278. *See* Premiere Lab Supply, Inc. v. Chemplex Indus., Inc., 791 So. 2d 1190 (Fla. Dist. Ct. App. 2001) (customer lists disclosed to court *in camera*); Air Prods. & Chems., Inc. v. Johnson, 442 A.2d 1114 (Pa. 1982); Curtis, Inc. v. District Court, 526 P.2d 1335 (Colo. 1974) (en banc).

279. *See* 31 U.S.C. § 3730(b)(2) (2012).

280. *See* S. REP. NO. 99-345, at 24 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 5266, 5289.

Once the government has decided to intervene, the seal is lifted and the complaint is served in accordance with the Federal Rules of Civil Procedure.[281] Violation of the seal order can have serious consequences.[282]

3. Whistleblower Protection Models

Federal and state legislature and regulatory authorities have experimented with a variety of approaches to insulate whistleblowers while protecting trade secrets.

a. State Law Models

Several state false claims acts expressly insulate whistleblowers from liability for providing trade secret documents to the government. For example, New York's False Claims Act, like the federal FCA, provides that a person may not be discriminated against for lawful acts in pursuit of a qui tam action.[283] The New York statute, however, includes provision of documentary evidence to the government as a "lawful act."[284] The New Jersey False Claims Act adopts another approach, including a provision that prohibits an employer from making or enforcing any:

> [R]ule, regulation, or policy preventing an employee from disclosing information to a State or law enforcement agency or from acting to further a false claim action, including investigating, initiating, testifying, or assisting in an action filed or to be filed under [the New Jersey False Claims Act].[285]

Massachusetts includes a similar provision and also expressly prohibits an employer from requiring that an employee, contractor, or agent "accept or sign an agreement that limits or denies the rights of such employee, contractor or agent to bring an action or provide information to a government or law enforcement agency" pursuant to the Massachusetts False Claims Act.[286] These state statutes thus provide valuable models.

---

281. *See* 31 U.S.C. § 3730(b)(2).

282. *See, e.g.*, United States *ex rel.* Pilon v. Martin Marietta Corp., 60 F.3d 995 (2d Cir. 1995) (upholding the dismissal of qui tam claims for failure to file and serve the complaint in accordance with the FCA).

283. *See* N.Y. STATE FIN. LAW §§ 187, 191(1) (2010).

284. *See id.* § 191(2) ("For purposes of this section, a 'lawful act' shall include, but not be limited to, obtaining or transmitting to the state, a local government, a qui tam plaintiff, or private counsel solely employed to investigate, potentially file, or file a cause of action under this article, documents, data, correspondence, electronic mail, or any other information, even though such act may violate a contract, employment term, or duty owed to the employer or contractor, so long as the possession and transmission of such documents are for the sole purpose of furthering efforts to stop one or more violations of this article.").

285. *See* New Jersey False Claims Act, N.J. STAT. ANN. § 2A:32C-10(a) (2008).

286. Massachusetts False Claims Act, MASS. GEN. LAWS ANN. ch. 12, § 5J (2012).

b. HIPAA Whistleblower Protection Provisions

The federal government thoughtfully confronted the balance between protecting confidential records and reporting alleged legal violations in crafting HIPAA.[287] Title I facilitates maintenance of health insurance coverage by regulating the availability and breadth of group health plans and individual health insurance policies. Title II protects the privacy and security of individuals' health information. Such protections, however, could complicate the enforcement of the law if employees reporting violations could themselves be liable for revealing private health information.

As reflected in the following provisions, HIPAA regulations immunize employees and business associates of "covered entities" from liability for reporting alleged violations of the privacy:

> § 164.502 Uses and disclosures of protected health information: General rules.
>
> (j) Standard: Disclosures by whistleblowers and workforce member crime victims
>
> (1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:
>
> i. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
>
> ii. The disclosure is to:
>
> A. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
>
> B. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.[288]

This provision carefully balances the privacy interests of patients with the public interest in ensuring compliance with health privacy protections.

287. *See* Pub. L. No. 104-191, 110 Stat. 1936 (1996).
288. 45 C.F.R. § 164.502 (2016).

Employees and business associates of covered entities are well positioned to detect violations of this law. Yet, if they could be liable for violations of the law by reporting violations, there would be little effective monitoring of compliance. The regulations wisely address this challenge by immunizing employees and business associates from liability for reporting violations to a trusted and responsible official or oversight agency. In addition, the regulation provides for the employee or business associate to consult with an attorney.

c. SEC Regulations

The SEC has taken a strong stance against the use of confidentiality agreements to prevent whistleblowers from reporting to the government. For example, the SEC recently brought an enforcement action against KBR, Inc. for using overly restrictive language in confidentiality agreements that potentially inhibited whistleblowers from reporting misconduct.[289] The SEC charged the company with violating Rule 21F-17, which prohibits employers from taking measures through confidentiality, employment, severance, or other type of agreements that may silence potential whistleblowers before they can reach out to the SEC.[290] The offending provision had required witnesses in internal company investigations to agree that they could not discuss the subject of the interview without prior authorization from the legal department and that disclosure could be grounds for discipline including termination of employment. As remedial steps, the company amended its statement to include the following statement:

> Nothing in this Confidentiality Statement prohibits me from reporting possible violations of federal law or regulation to any governmental agency or entity, including but not limited to the Department of Justice, the Securities and Exchange Commission, the Congress, and any agency Inspector General, or making other disclosures that are protected under the whistleblower provision of federal law or regulation. I do not need the prior authorization of the Law Department to make any such reports or disclosures and I am not required to notify the company that I have made such reports or disclosures.

Although the company maintained that the agreement did not say employees could not report misconduct to the SEC, the SEC believed that an employee reading such an agreement would reasonably understand its broad language that disclosure could be grounds for discipline to mean that they could not disclose the information to anyone without the permission of the legal department.

289. *In re* KBR, Inc., SEC Admin. Proceeding No. 3-16466 (Apr. 1, 2015).
290. *See* 17 C.F.R. § 240.21F-17 (2016).

Lawyers for some companies protested that the SEC had exceeded its authority.[291] Nonetheless, the SEC pursued its effort to assure employees that overbroad and vague confidentiality agreements did not stand in the way of reporting allegedly illegal activity.

C. The Sealed Disclosure/Trusted Intermediary Safe Harbor

Drawing on the state law models, the HIPAA protocol for reporting violations while protecting private information, and the SEC's efforts to inform potential whistleblowers that NDAs do not stand in the way of careful reporting of allegedly illegal activity, I proposed the following public policy exception to trade secret protection in November 2015:

> **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 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

291. *See, e.g.*, Eugene Scalia, *Blowing the Whistle on the SEC's Latest Power Move*, WALL ST. J. (Apr. 5, 2015), http://www.wsj.com/articles/eugene-scalia-blowing-the-whistle-on-the-secs-latest-power-move-1428271250 [https://perma.cc/NK7H-A9CW].

> provide notice of the public policy exception shall bar recovery of exemplary damages and attorneys' fees in any trade secret misappropriation action.

This statutory exception to trade secret liability would provide clear assurance and notice to potential whistleblowers that they cannot be held liable for violation of an NDA merely by seeking legal counsel regarding reporting of allegedly illegal conduct by an employer or by reporting such information to a responsible government official through a confidential channel. In addition, this safe harbor would insulate lawyers advising potential whistleblowers about their options and serving as a conduit for presenting the information of allegedly illegal conduct to the government.

The notice provision includes a balanced incentive to ensure that employees are aware of the public policy exception. Failure to include reasonable notice of the safe harbor would bar the company from enforcing the NDA in federal court—including non-whistleblower cases. In addition, the provision would bar award of exemplary damages and attorneys' fees in a state court action. This proposed provision would likely ensure that standard NDAs would include effective notice of the safe harbor.

A provision barring enforcement of the NDA entirely could be seen as going too far. Companies that are not immediately aware of this requirement should be given some time to adapt to the new regime. The benefit of federal enforcement provides a carrot for companies to include notice of the public policy safe harbor. We would expect the notice provision to become standard in all NDAs. But should companies resist providing such notice, the remedy for failing to provide notice could be revisited.

This regime could be augmented by including a procedural mechanism that would permit whistleblowers and their attorneys to obtain prompt dismissal and recovery of attorney's fees against companies that assert trade secret claims in violation of the sealed disclosure/trusted intermediary safe harbor. State anti-SLAPP (Strategic Lawsuits Against Public Participation) statutes provide a useful model.[292]

D. Stress Testing the Sealed Disclosure/Trusted Intermediary Safe Harbor

This immunity/notice approach ensures that employees and contractors understand that NDAs do not stand in the way of their reporting illegal conduct by their employers. At the same time, this safe harbor provides ample safeguards against public disclosure of legitimate trade secrets. It realigns trade secret protection with its guiding principles of promoting commercial morality and encouraging technological advance. NDAs cannot be used to silence whistleblowers. This Section explores potential objections, alternatives, and

292. *See, e.g.*, CAL. CODE CIV. P. §§ 425.16, 425.18.

limitations of this approach to promoting reporting of allegedly illegal conduct without jeopardizing legitimate trade secret protection.

1. Potential Leakage

Trade secret owners could see the safe harbor as a Trojan horse whereby employees and contractors would be liberated from the bounds of NDAs. Such a view misapprehends the carefully tailored contours of the exception. The only persons who would be brought into the trade secret's confidential zone would be attorneys and government officials who would be bound by secrecy. Furthermore, the safe harbor would immunize only those employees and contractors who used the sealed disclosure channel. They would not be able to disclose the information in a way that jeopardized its commercial value. In particular, the proposed safe harbor would not authorize divulging trade secrets to the media.

Thus, trade secret owners would retain the same protections that they currently have against employers and contractors who disclose legitimate trade secrets to the public or competitors. Companies would, however, face greater risk that illegal activity would be disclosed to government officials who are in a position to take corrective action. Notice of the safe harbor would reduce the *in terrorem* effect of NDAs that companies have come to expect. That expectation, however, goes well beyond the commercial morality and encouragement of innovation principles that undergird trade secret protection. Removing the threat of sanctions for sealed disclosure would deter the use of NDAs to mask illegal conduct. The net effect would be higher costs of engaging in illegal conduct.

The sealed disclosure/trusted intermediary safe harbor could reduce the risks of inappropriate trade secret disclosure by encouraging whistleblowers to use secure channels for reporting illegal activity as opposed to publicizing the information on the Internet or in the media. Furthermore, the safe harbor fosters access to legal counsel. Attorneys would be able to provide the whistleblower with a balanced understanding of the options and the benefits of confidential reporting. The safe harbor notice provisions reinforce the salutary effects of maintaining trade secrecy during the reporting process.

2. Alternatives and Complements

Scholars have proposed other approaches to discourage the silencing of whistleblowers through overbroad trade secret protection. The sealed disclosure/trusted intermediary safe harbor is complementary to these proposals, but it provides a clearer and more robust solution to the chilling effects of overbroad NDAs. Government agencies can also put a public policy safe harbor clause into their procurement contracts.

False Claims Act Zone of Protection. Professor Joel Hesch takes aim at a broader array of contract and tort claims that have been asserted against

employees who have provided incriminating documents to the government.[293] He contends that the FCA establishes a zone of protection that preempts state law causes of action that interfere with disclosure of trade secret documents. He emphasizes that the FCA requires relators to supply the government with a statement of material evidence containing all information and documents that support the FCA allegations, including company documents within their control.[294] Moreover, the FCA mandates that the relator protect against public disclosure of information by filing the complaint under seal and only serve the complaint and the statement of material evidence upon the Attorney General,[295] thereby providing protection against public disclosure of information. The FCA further discourages public disclosure of proprietary information by barring the whistleblower from sharing in the government's recovery if "substantially the same allegations or transactions as alleged in [the complaint] were publicly disclosed" unless the relator is "an original source of the information" on which the allegations are based.[296] Furthermore, the FCA protects employees from retaliation for reporting and assisting in the government's efforts to uncover fraud.[297]

Based largely on these considerations, Professor Hesch traces a zone of federal protection that:

> [I]mmunizes or exempts a whistleblower from all contract and tort claims bound up with or flow from an act of reporting suspected fraud against the government so long as the employee possesses a reasonable belief that suspected fraud or FCA violations occurred and regardless of whether fraud or violations of the FCA are ultimately established.[298]

His proposal extends more broadly than the sealed disclosure/trusted intermediary safe harbor in that it would immunize whistleblowers from causes of action beyond the trade secret domain. The zone of interests standard is also narrower in that it applies only to reporting of FCA violations. Beyond the difference in scope, proving "reasonable belief" as to suspected FCA violations creates uncertainty. Whistleblowers might not be able to get these matters dismissed without discovery, significant litigation costs, and exposure. Furthermore, the zone of protection approach does not provide a built-in notice mechanism ensuring that signatories of NDAs are aware of a law-reporting safe harbor.

The sealed disclosure/trusted intermediary safe harbor provides a more secure and clear solution to the particular problems posed by the overbreadth and *in terrorem* effects of trade secret law. A public policy exception extends

293. *See* Hesch, *supra* note 181.
294. *See* 31 U.S.C. § 3730(b)(2) (2012).
295. *See id.*
296. *See id.* § 3730(e)(4)(A).
297. *See id.* § 3730(h).
298. Hesch, *supra* note 181, at 393.

well beyond the FCA context to all reporting of allegedly illegal conduct. It would complement the zone of interests backstop.

Trade Secret Fair Use. Professor Deepa Vardarajan approaches the problem from the trade secret side of the divide.[299] Focusing on cumulative innovation, public safety,[300] and free expression, her analysis highlights the lack of balancing doctrines in trade secret law in comparison with patent and copyright law.[301] She proposes that trade secret law recognize a fair use defense,[302] roughly along the lines of copyright's multifactor fair use balancing test.[303]

While this proposal would provide added flexibility to rein in the breadth of trade secret protection, it is not well adapted to the challenges facing employees and contractors seeking a clear safe harbor. Like copyright law's fair use doctrine, a fair use approach to trade secret law would likely prove far too uncertain to be of great service to many potential whistleblowers.[304] The uncertainty of copyright law has fostered a norm in many creative communities of "if in doubt, leave it out,"[305] which is the type of chilling effect that we seek to avoid in the law enforcement domain. A public policy exception to trade secret law should be clear and known to potential whistleblowers.

Technology-Specific Safe Harbors. Professor David Levine has proposed that trade secret protection should not be available for "private entities engaged in activities such as providing voting or breathalyzer machines to the

299. *See* Vardarajan, *supra* note 21.

300. *See, e.g.*, Rebecca S. Eisenberg, *Data Secrecy in the Age of Regulatory Exclusivity*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 467 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) [hereinafter TRADE SECRECY HANDBOOK] (dealing with clinical data used in approving drugs); Mary L. Lyndon, *Trade Secrets and Information Access in Environmental Law*, *in* TRADE SECRECY HANDBOOK 442 (dealing with access to discharge of hazardous materials); Margaret Witherup Tindall, *Breast Implant Information as Trade Secrets: Another Look at FOIA's Fourth Exemption*, 7 ADMIN. L.J. AM. U. 213, 224 (1993).

301. *See* Vardarajan, *supra* note 21, at 1420–38.

302. *See id.* at 1445–49.

303. *See* 17 U.S.C. § 107 (2012).

304. *See* Joseph P. Liu, *Two-Factor Fair Use?*, 31 COLUM. J.L. & ARTS 571, 574–78 (2008) (arguing that the fair use test exemplifies how "notoriously difficult" it is to predict accurately the outcomes of multifactor balancing tests); *see also* PATRICIA AUFDERHEIDE & PETER JASZI, UNTOLD STORIES: CREATIVE CONSEQUENCES OF THE RIGHTS CLEARANCE CULTURE FOR DOCUMENTARY FILMMAKERS (2004) (exploring the copyright-clearance challenges faced by documentary filmmakers); Barton Beebe, *An Empirical Study of U.S. Copyright Fair Use Opinions, 1978–2005*, 156 U. PA. L. REV. 549 (2008) (systematically evaluating published fair use decisions); Michael W. Carroll, *Fixing Fair Use*, 85 N.C. L. REV. 1087, 1095 (2007) ("[T]he fair use doctrine produces significant ex ante uncertainty."); PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT § 12.1 (3d ed. 2005) ("No copyright doctrine is less determinate than fair use."); David Nimmer, *"Fairest of Them All" and Other Fairy Tales of Fair Use*, 66 L. & CONTEMP. PROBS. 263, 281 (2003) (lamenting that "Congress included no mechanism for weighing divergent results against each other and ultimately resolving whether any given usage is fair").

305. *See* Peter S. Menell & Ben Depoorter, *Using Fee Shifting to Promote Fair Use and Fair Licensing*, 102 CALIF. L. REV. 53, 69–71 (2014).

government."[306] Such technology-specific safe harbors could complement the sealed disclosure/trusted intermediary safe harbor but cannot address the full range of law reporting contexts.

Government Contract-Based Safe Harbor. Government agencies can directly condition research and procurement contracts on companies consenting to a trade secret public policy exception. For example, the EPA and the National Institutes of Health condition their grants on various public policy requirements.[307] The SEC has essentially required its regulated community to provide securities industry employees with information that NDAs do not stand in the way of reporting illegal activity.[308] Thus, the proposed safe harbor can be partially implemented without federal legislation.

Nonetheless, such piecemeal implementation of a public policy exception would be needlessly complex and incomplete. Establishing a public policy exception through federal trade secret legislation would be far more effective in reining in pervasive, overbroad NDAs and educating the public about the importance and legitimacy of reporting illegal activity.

3. Limitations: The Challenge of Whistleblowing When the Intermediary Is Not Trustworthy

The sealed disclosure/trusted intermediary safe harbor depends critically on the trustworthiness of government agencies or officers. This is a reasonable assumption in many law enforcement contexts. Law enforcement authorities, government agencies, and their officials generally want to serve their mission and the public trust. In addition, supervisory authorities (oversight committees and courts), inspector generals, the public, and the media help to ensure that the responsible officials are faithful to agency mission and are fiscally responsible.

Yet many corrupting forces can influence government actors. Contractors can develop cozy relationships with the agencies with whom they work. The revolving door of hiring government officials as well as lobbying of political officials can undermine an agency's objectivity. Various anticorruption laws, however, counteract those forces.[309] In addition, the FCA brings in the

306. *See* David S. Levine, *The Impact of Trade Secrecy on Public Transparency*, *in* TRADE SECRECY HANDBOOK, *supra* note 300, at 435; David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 151–55 (2007).

307. *See* NAT'L INSTITUTES OF HEALTH, NIH GRANTS POLICY STATEMENT IIA-3–46 (Oct./Nov. 2015), http://grants.nih.gov/grants/policy/nihgps/nihgps.pdf [https://perma.cc/9FEL-LPFS]; U.S. EPA, EPA GENERAL TERMS AND CONDITIONS 11–12 (Oct. 6, 2016), http://www.epa.gov/sites/production/files/2015-10/documents/general_tc_as_of_10-6-2015.pdf [https://perma.cc/U8X3-BCWY].

308. *See supra* Part IV.B.3.iii.

309. *See* SUSAN ROSE-ACKERMAN, CORRUPTION AND GOVERNMENT: CAUSES, CONSEQUENCES, AND REFORM (1999); U.S. OFFICE OF GOV'T ETHICS, UNDERSTANDING THE REVOLVING DOOR: HOW ETHICS RULES APPLY TO YOUR JOB SEEKING AND POST-GOVERNMENT EMPLOYMENT ACTIVITIES (Oct. 2007), http://www.oge.gov/uploadedFiles/Education/Education_Resources_for_Ethics_Officials/Resources/phrevdoor_07.pdf [https://perma.cc/9DUR-TVM8];

Department of Justice as a more neutral party in evaluating fraud allegations. Furthermore, the FCA authorizes the relator to pursue an action even if the government does not join the case, which can expose questionable decision making by government officials.

Nonetheless, a government agency can be the source of the misconduct. Many of the open government laws and regulations Ralph Nader spearheaded in the 1960s and 1970s grew out of these concerns.[310] Edward Snowden faced such problems when he learned that the National Security Agency was engaging in widespread surveillance of U.S. citizens and foreign governments that went well beyond constitutional and acknowledged diplomatic limits.[311] It seems unlikely that sealed disclosure would have produced sufficient attention and corrective action. Hence, Mr. Snowden faced a stark choice: reporting his findings internally, risking a cover-up and retaliation, or going to the media and facing criminal prosecution.[312]

The sealed disclosure/trusted intermediary safe harbor cannot solve these types of challenges. At a minimum, however, it can provide greater accountability. In the specific context of the FCA and the SEC types of whistleblower programs, it would expand the pool of whistleblowers. Furthermore, the FCA's provision authorizing relators to go forward with a fraud claim even without the government serves to police government decision makers. It also affords Department of Justice attorneys with greater clout in addressing potential agency capture or coziness with contracting entities.

Nonetheless, the fact that the sealed disclosure/trusted intermediary safe harbor cannot fully address all of the accountability challenges does not mean that it would not provide a great step forward in aligning trade secret law with the modern age. A public policy exception along the lines proposed would promote the public interest in law enforcement. It would also ferret out and deter fraud without jeopardizing the core goals of trade secrecy protection.

Ethics in Government Act of 1978, Pub. L. No. 95-521 (1978) (codified at 5 U.S.C. app. §§ 101–505 (2012)) (describing financial disclosure requirements for federal personnel); 18 U.S.C. § 207 (2012) (discussing restrictions on former officers and employees representing persons before government after leaving office).

310. *See, e.g.*, Civil Service Reform Act, Pub. L. No. 95-454, 92 Stat. 111 (1978); Robert G. Vaughn, *Statutory Protection of Whistleblowers in the Federal Executive Branch*, 1982 U. ILL. L. REV. 615 (1982); ROBERT G. VAUGHN, THE SPOILED SYSTEM: A CALL FOR CIVIL SERVICE REFORM (1975); RALPH NADER ET AL., WHISTLEBLOWING: THE REPORT OF THE CONFERENCE ON PROFESSIONAL RESPONSIBILITY (1972). *See generally* ROBERT G. VAUGHN, THE SUCCESSES AND FAILURES OF WHISTLEBLOWER LAWS (2012) (providing a broad retrospective review of the emergence and development of government whistleblower protections and institutions).

311. *See* Editorial, *Edward Snowden, Whistle-Blower*, N.Y. TIMES, Jan. 2, 2014, at A18.

312. *Cf.* Daniel Ellsberg, *NSA Leaker Snowden Made the Right Call*, WASH. POST (July 7, 2013), https://www.washingtonpost.com/opinions/daniel-ellsberg-nsa-leaker-snowden-made-the-right-call/2013/07/07/0b46d96c-e5b7-11e2-aef3-339619eab080_story.html [https://perma.cc/T8MW-D9HH].

V.
IMPLEMENTING A TRADE SECRET PUBLIC POLICY SAFE HARBOR: THE DEFEND TRADE SECRETS ACT OF 2016

The Senate amended the draft Defend Trade Secrets Act in January 2016 to include the following provision:[313]

> (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 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

313. Defend Trade Secrets Act of 2015, § 7 (codified at 18 U.S.C. § 1833 (2012)).

> 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.

This provision incorporates the key elements of the sealed disclosure/trusted intermediate safe harbor: (1) immunity from liability for trade secret misappropriation for confidential reporting of illegal activity to the government (federal, state, or local) or an attorney for the purpose of reporting or investigating a suspected violation of law; (2) immunity from liability for trade secret misappropriation for confidential law-reporting as part of an antiretaliation action; and (3) a requirement that employers provide notice of the sealed disclosure/trusted intermediate safe harbor.

The full Senate unanimously passed the amended bill in early April 2016.[314] The House of Representatives passed an identical version of the Senate bill by a nearly unanimous vote a short time later.[315] President Obama signed the DTSA into law on May 11, 2016.[316] It became effective immediately.

CONCLUSION

The core principles underlying trade secret protection—promoting commercial morality and technological progress—trace back two centuries to the Industrial Revolution and continue to serve economic growth today. Yet the uncritical breadth of trade secret protection and routine use of blanket NDAs has not kept pace with the greater protections for civil rights, workplace safety, public health, and environmental protection, as well as the expanded role of the government in the economy—from military procurement to public

314. Daniel Wilson, *Senate Passes Bill for Federal Trade Secrets Protection*, LAW360 (Apr. 4, 2016), http://www.law360.com/articles/779729/senate-passes-bill-for-federal-trade-secrets-protection [https://perma.cc/ZD6M-TLGQ].

315. *See* Bill Donohue, *House Overwhelmingly Passes Federal Trade Secrets Bill*, LAW360 (Apr. 27, 2016), http://www.law360.com/articles/788378/house-overwhelmingly-passes-federal-trade-secrets-bill [https://perma.cc/6WM8-8F2F].

316. Bill Donohue, *Obama Signs Federal Trade Secrets Bill into Law*, LAW360 (May 11, 2016), http://www.law360.com/articles/795051/obama-signs-federal-trade-secrets-bill-into-law [https://perma.cc/X6AU-575E].

infrastructure, health, and safety, and regulation of financial markets. Company employees and contractors are often in the best position to report violations of law and fraud against the government. Yet they are indoctrinated to believe that they may not come forward with evidence of such illegal conduct without violating their employment agreements. State law surrounding a public policy exception to trade secret law is murky, adding to the many other forces discouraging employees and contractors from reporting illegal conduct.

The inclusion of a sealed disclosure/trusted intermediary safe harbor in the Defend Trade Secrets Act of 2016 vindicated an important principle: employees and contractors should be able to report suspected illegal activity without risk of trade secret liability and should know that they can do so notwithstanding that they signed an NDA. But given the potential risks to legitimate trade secrets, they must report alleged misconduct confidentially in order to qualify for the liability shield. Furthermore, employees and contractors should know that they may obtain legal counsel to advise them on the law and the reporting process. This approach promotes lawful reporting without jeopardizing trade secrets. It will also deter companies from engaging in illegal activity and using trade secret law to shield such activity.