DePaul University
UNIVERSITY LIBRARIES

DePaul Business and Commercial Law Journal

Volume 17
Issue 1 *Volume 17: Issue 1*

Article 1

Blowing the Whistle in the Digital Age: Are You Really Anonymous? The Perils and Pitfalls of Anonymity in Whistleblowing Law

Tanya M. Marcum J.D.

Jacob Young D.B.A.

Ethan T. Kirner

Blowing the Whistle in the Digital Age: Are You Really Anonymous? The Perils and Pitfalls of Anonymity in Whistleblowing Law

Dr. Tanya M. Marcum, J.D. & Jacob Young, D.B.A.

> "He perceives very clearly that the world is in greater peril from those who tolerate or encourage evil than from those who actually commit it." Albert Einstein's tribute to Pablo Casals[1]

I. Introduction

Suppose an employee works for a private company in a state with "at-will" employment. The employee discovers wrongdoing within the employee's organization. This employee wants to inform the organization of the wrongdoing but is afraid of doing so because they have heard horror stories about the effects of retaliation. In trying to report the wrongdoing, the employee types out the information on the employee's computer, uses the company network to print it on the printer at work and mails it to the organization. Unbeknownst to the employee, the organization was able to determine that the letter came from a company printer by examining invisible watermarks on the document. After reviewing system logs, the employee is identified as the author of the document. The employee is later terminated without any mention of the letter, leaving no clear evidence that it was in response to reporting the wrongdoing. The employee could have taken different steps to remain anonymous to avoid retaliation if he or she had been aware of methods of identification.

Laws and ethical standards created by both government and nongovernment organizations attempt to protect shareholders, managers, employees, clients, customers, the public and government from corporate corruption, fraud, and other misdeeds.[2] Ideally, corporate governance should provide for transparency, full disclosure, and accurate financial data.[3] Managerial review, internal auditing and actual

1. J. Ma. Corredor, Conversations with Casals 11 (André Mangeot trans., E.P. Dutton & Co. Inc., 1957).

2. Guhan Subramanian, *Corporate Governance 2.0,* 92 Har. Bus. Rev. 96 (2015) (explaining that these legal and ethical standards are commonly referred to as corporate governance).

3. Umang Desai, *Crying Foul: Whistleblower Provisions of the Dodd-Frank Act of 2010*, 43 Loy. U. Chi. L.J. 427, 432 (2012).

discovery are some mechanisms to discover wrongdoing within an organization. However, the single most important method to discover internal wrongdoing is with employee tips or whistleblowing.[4] Whistleblowing is defined as "the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action."[5] The results of one survey suggested that whistleblowers exposed 43% of the fraud in private corporations, while auditors uncovered a mere 19%.[6] Stephen M. Kohn, the President of the National Whistleblower Center, stated that "[t]his survey is proof that corporate shareholders directly benefit from whistleblower disclosures. Instead of firing the whistleblower, this survey demonstrates that corporate culture should change."[7]

Many companies create and operate internal whistleblower programs, which commonly include whistleblower hotlines, to create an environment that encourages the exchange of information regarding perceived wrongdoings within the organization.[8] Publicly held corporations in the U.S. must establish internal procedures to receive complaints about accounting irregularities and create procedures that will allow for anonymous and confidential submission by employees of such accounting concerns.[9] If protected internal whistleblower reporting is an available option, whistleblowers will report internally over external reporting avenues.[10] However, there is a major difference between confidential submissions by a whistleblower as compared to anonymous submissions by a whistleblower. Some laws attempt to create protection for whistleblowers. The key word here is attempt. Under the best of circumstances, those who report wrongdoings at their place of employment often run a high risk of retaliation once they report the wrongdoing. Some of these whistleblowers believe that they are anonymously reporting the wrongdoing. However, al-

4. Leonardo Labriola, *Paying Too Dearly for a Whistle: Properly Protecting Internal Whistleblowers*, 85 FORDHAM L. REV. 2839, 2846 (2017).

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

6. *Whistleblowers Still the Best at Detecting Fraud,* NAT'L WHISTLEBLOWER CTR, https://www.whistleblowers.org/news/whistleblowers-still-the-best-at-detecting-fraud/ (last visited May 19, 2018).

7. *Id.*

8. Richard Moberly, *Confidentiality and Whistleblowing,* 96 N.C. L. REV. 751, 759 (2018).

9. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered sections of 15 U.S.C (2012)).

10. Christine A. Ladwig, *A Sarbanes-Oxley and Dodd-Frank Triple Win Scenario: The Joint Benefit of an Internal-External Reporting Alliance for Corporations, Whistleblowers and Government,* 27(1) MIDWEST L. J. 79, 87 (2017).

though stated as an anonymous system for reporting fraud and abuse, many are not actually anonymous. If anonymous reporting is only confidential, then there are increased disincentives for the whistleblowers to report the violations of the law by their employer.

Most potential whistleblowers are worried about both their personal and professional lives and the changes that will likely take place, most of which will not be positive should they decide to blow the whistle. For many, the difficult personal and professional decision to come forward and report wrongdoing requires a reconciliation of conflicting values. On the one hand, our society celebrates team players and, on the other, it has contempt for mindless sheep that go along to get along. At times, our society champions the individual who does what is right. Too often, however, society unfairly characterizes an individual who reports problems as disloyal.[11]

A whistleblower is perceived as the "eyes and ears" of the public at large who need protection in the areas of health, safety, finances and overall public welfare.[12] Based on this definition, why are there not more whistleblowers? Unfortunately, there are several factors that might discourage those who have knowledge of wrongdoing from blowing the whistle. First, organizational insiders might be hesitant to report out of fear of retaliation[13] or to simply avoid being the bearer of bad news.[14] Retaliation against those who speak up is quite com-

11. Connor C. Turpan, *Whistleblower? More Like Cybercriminal: The Computer Fraud and Abuse Act as Applied to Sarbanes-Oxley Whistleblowers,* 42 RUTGERS COMPUTER & TECH. L.J. 120, 121 (2016).

12. *See* MARCIA P. MICELI & JANET P. NEAR, BLOWING THE WHISTLE: THE ORGANIZATIONAL & LEGAL IMPLICATIONS FOR COMPANIES AND EMPLOYEES (1992).

13. *See* Elizabeth Wolfe Morrison & Frances J. Milliken, *Organizational Silence: A Barrier to Change and Development in a Pluralistic World*, 25(4) ACAD. OF MGMT. REV. 706 (2000); MARCIA P. MICELI & JANET P. NEAR, BLOWING THE WHISTLE: THE ORGANIZATIONAL & LEGAL IMPLICATIONS FOR COMPANIES AND EMPLOYEES (1992); Michael J. Withey & William H. Cooper, *Predicting Exit, Voice, Loyalty, and Neglect*, 34(4) ADMIN. SCI. Q. 521 (1989); Susan J. Ashford et al., *Out on a Limb: The Role of Context and Impression Management in Selling Gender-equity Issues*, 43(1) ADMIN. SCI. Q. 23 (1998).

14. *See* Jayson L. Dibble & Timothy R. Levine, *Breaking Good and Bad News: Direction of the MUM Effect and Senders' Cognitive Representations of News Valence*, 37(5) COMM. RES. 703 (2010); Jayson L. Dibble & Timothy R. Levine, *Sharing Good and Bad News with Friends and Strangers: Reasons for and Communication Behaviors Associated with the MUM Effect*, 64(4) COMM. STUD. 431 (2013); Sidney Rosen & Abraham Tesser, *On Reluctance to Communicate Undesirable Information: The MUM Effect*, 33(3) SOCIOMETRY 253 (1970); ChongWoo Park et al., *Overcoming the Mum Effect in IT Project Reporting: Impacts of Fault Responsibility and Time Urgency*, 9(7) J. ASSN. FOR INFO. SYS. 409 (2008); Laura E. Marler et al., *Don't Make Me the Bad Guy: Organizational Norms, Self-monitoring, and the Mum Effect*, 24(1) J. OF MANAGERIAL ISSUES 97 (2012).

mon[15] and is "most likely and most severe when the observed wrongdoing is most systemic and most central to the operation of the agency."[16] Retaliation can be levied in many forms, such as nullification, isolation, defamation, expulsion, ostracism, demotion or termination.[17] One study reports that approximately two thirds of the whistleblowers in their study had experienced the following forms of retaliation: 69% lost their job or were forced to retire; 64% received negative employment performance evaluations; 68% had work more closely monitored by supervisors; 69% were criticized or avoided by coworkers; and 64% were blacklisted from getting another job in their field.[18]

Second, although anonymity is desired to protect whistleblowers from retaliation,[19] existing channels for soliciting reports of wrongdoing fail to provide adequate anonymity protection for naïve users of modern technology. The U.S. has passed several whistleblower protection laws, such as the Sarbanes-Oxley Act of 2002[20] and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010,[21] which provide increased regulation and oversight to address corporate misconduct. Both pieces of legislation contain whistleblowing provisions that require publicly-traded companies to establish "anonymous" reporting channels and strengthen the penalties for retaliation against those who report misconduct.[22] As a result, several technology

15. Joyce Rothschild & Terance D. Miethe, *Whistle-Blower Disclosures and Management Retaliation: The Battle to Control Information about Organization Corruption*, 26(1) WORK & OCCUPATIONS 107 (1999).

16. *Id*. at 125.

17. Muel Kaptein, *From Inaction to External Whistleblowing: The Influence of the Ethical Culture of Organizations on Employee Responses to Observed Wrongdoing*, 98(3) J. OF BUS. ETHICS 513, 514 (2010); Terry Morehead Dworkin & Melissa S. Baucus, *Internal vs. External Whistleblowers: A Comparison of Whistleblowering Processes,* 17(12) J. BUS. ETHICS 1281, 1285 (1998); Tim Barnett et al., *The Internal Disclosure Policies of Private-sector Employers: An Initial Look at Their Relationship to Employee Whistleblowing,* 12(2) J. BUS. ETHICS 127, 127-28 (1993).

18. Rothschild, *supra* note 15, at 120.

19. Susan Ayers & Steven E. Kaplan, *Wrongdoing by Consultants: An Examination of Employees? Reporting Intentions*, 57(2) J. BUS. ETHICS 121, 127 (2005); Steven E. Kaplan & Joseph J. Schultz, *The Role of Internal Audit in Sensitive Communications,* J. MGMT. STUD. 10 (2006); Steven E. Kaplan & Joseph J. Schultz*, Intentions to Report Questionable Acts: An Examination of the Influence of Anonymous Reporting Channel, Internal Audit Quality, and Setting*, 71(2) J. BUS. ETHICS 109, 112 (2007); Janet P. Near & Marcia P. Miceli, *Effective-Whistle Blowing*, 20(3) ACAD. OF MGMT. REV. 679, 692 (1995); Frederick A. Elliston, *Anonymity and Whistleblowing*, 1(3) J. BUS. ETHICS 167-177 (1982).

20. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered sections of 15 U.S.C (2012)).

21. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 (2012)).

22. STEPHEN M. KOHN, THE NEW WHISTLEBLOWER'S HANDBOOK: A STEP-BY-STEP GUIDE TO DOING WHAT'S RIGHT AND PROTECTING YOURSELF, 2 (3d ed. 2017).

firms began developing and marketing internal reporting systems to meet this new demand. However, most of the commercial reporting systems available today still fail to provide adequate anonymity protections for whistleblowers. If the use of a system could potentially compromise the identity of the user, it cannot be considered to provide anonymity. These design flaws can be traced back to lawmakers' failure to define anonymity and outline the required system characteristics necessary to achieve anonymity. This has led many whistleblowers to develop a false sense of security by believing that these systems will truly protect their anonymity. Therefore, the failure to ensure that anonymity is truly achieved has compromised the identity of numerous whistleblowers and resulted in the very retaliation that lawmakers intended to prevent.

Third, despite the passage of legislation aimed at protecting whistleblowers, existing United States laws are still limited to certain types of employees and industries.[23] Further, those who seek protection under the law are required to maintain strict compliance with the established protocol to qualify for protection,[24] which can ultimately leave employees vulnerable to retaliation.[25] What should an employee do when they have detected fraud or some other type of wrongdoing within their place of employment? Most potential whistleblowers worry about retaliation and the release of their identity to their employer. Does a reporting system truly provide anonymity as some laws require? Will a naïve reporter recognize when a system may not actually be anonymous as promised? To address these issues, this article examines whistleblowing laws with respect to anonymity, confidentiality and technological requirements. In part II of this article, we discuss federal laws protecting whistleblowers and the requirements of anonymity. In part III, we discuss the difference between anonymity versus confidentiality, motivations for and methods available to identify whistleblowers. In order to better protect whistleblowers, part IV contains the discussion of potential legislative solutions to the legal shortcomings of current federal laws.

---

23. *Id*. *See also* TOM DEVINE & TAREK F. MAASSARANI, THE CORPORATE WHISTLEBLOWER'S SURVIVAL GUIDE 149 (2011).

24. *Id*. *See also* MARCIA P. MICELI & JANET P. NEAR, BLOWING THE WHISTLE: THE ORGANIZATIONAL & LEGAL IMPLICATIONS FOR COMPANIES AND EMPLOYEES 188 (1992); Janet P. Near, Terry M. Dworkin & Marcia P. Miceli, *Explaining the Whistleblowing Process: Suggestions from Power Theory and Justice Theory*, 4(3) J. ORGANIZ. SCI. 393 (1993).

25. TOM DEVINE & TAREK F. MAASSARANI, THE CORPORATE WHISTLEBLOWER'S SURVIVAL GUIDE 149 (2011); *see also* KOHN, *supra* note 22.

II. THE FEDERAL LAWS THAT SEEM TO PROTECT WHISTLEBLOWERS

> "Bad men need nothing more to compass their ends, than that good men should look on and do nothing." John Stuart Mill, philosopher[26]

The checks and balances in the United States Government were established in such a way as to encourage individuals to report what he or she might perceive as a legal wrong. This is true about fraud and abuse within both the government and corporate America. The premise is that those working within the organizations will come forward to report the perceived abuse because these individuals are the in the best position to report misconduct within their organizations.[27]

A potential whistleblower is faced with a major legal and ethical dilemma from the onset, whether to go public with the information, provide the information confidentially or to proceed with disclosure using a channel that allows anonymous reporting. With the fragmented federal whistleblower laws, finding the applicable law that may protect the whistleblower is a daunting task. Whistleblowers can be placed in three different categories: (1) the corporate employee whistleblower; (2) a public whistleblower; and/or (3) the government employee whistleblower.[28] The federal laws discussed in this article will focus on all three types of whistleblowers.

A. *Laws with the Primary Focus on Whistleblower Protection*

It is important to understand some of the sources of whistleblower laws in the United States. The U.S federal and state laws surrounding the concept of whistleblowing are fragmented. There are many laws that appear to govern this area rather than one comprehensive whistleblower protection law. Some laws focus on whistleblowers, other focus on another area with whistleblowing as a secondary focus. Most of the whistleblower laws do not mandate that an employee first report the wrongdoing to the employer using an internal compliance system before they report to the applicable federal or government authority.[29] One source suggests that there are over 55 different laws

---

26. NICHOLAS CAPALDI, JOHN STUART MILL: A BIOGRAPHY 330 (Cambridge Unv. Press, 2004).

27. Gerard Sinzdak, *An Analysis of Current Whistleblower Laws: Defending a More Flexible Approach to Reporting Requirements*, 96 CAL. L. REV. 1633, 1635 (2008).

28. Candice Delmas, *The Ethics of Government Whistleblowing,* 41(1) SOC. THEORY & PRACT. 77, 81 (2015).

29. Ellen C. Brotman & Erin C. Dougherty, *Blue Collar Tactics in White Collar Cases,* 35 THE CHAMPION 16, 18 (2011).

that protect whistleblowers from retaliation[30] and some of these laws have been around for nearly a century.[31]

The False Claims Act (FCA) was the first federal whistleblower statute that ctually focused on whistleblower[32]. Whistleblowers have used this law since the Civil War to inform the federal government of fraud and abuse.[33] Originally in the FCA, whistleblowers were labeled as relators.[34] The FCA states that any person who knowingly submitted a false claim[35] to the government was liable for double the damage to the government plus a $2,000 penalty for each false claim. The requirement that the relator have knowledge of the falsity of the claim was a necessary element under this statute.[36] In 1986 when this statute was amended to change the double damages provision to treble damages, it increased the penalties to not less than $5,000 and not more than $10,000,[37] and incentivized whistleblowers to sue on behalf of the federal government.[38] The statute specifically does not apply to federal tax claims.[39] There is no provision for anonymous whistleblowers under the False Claim Act, so all whistleblowing to the federal government is confidential, not anonymous. Additional amendments were made in 2009[40] and 2010.[41]

According the U.S. Justice Department, monetary recoveries under the FCA for the 2015 fiscal year exceeded $3.5 billion dollars.[42] Principal Deputy Assistant Attorney General Benjamin C. Mizer stated "[t]he False Claims Act has again proven to be the government's most effective civil tool to ferret out fraud and return billions to taxpayer-funded programs."[43]

---

30. KOHN, *supra* note 22 (discussing various federal laws related to whistleblowers).

31. Norm D. Bishara et al., *The Mouth of Truth,* 10 N.Y.U. J.L. & BUS. 37, 40 (2013).

32. False Claims Act, ch. 67, 12 Stat. 696 (1863) (codified as amended at 31 U.S.C. §§ 3729 *et seq.* (2012)). This Civil War era statute was created due to a concern that suppliers of goods to the Union Army committed fraud against the government.

33. Brotman, *supra* note 29, at 17.

34. *See* United States *ex rel.* v. Karvelas v. Melrose-Wakefield Hosp., 360 F.3d 220, 226 (1st Cir. 2004) (defining a relator as someone who relates fraudulent action on behalf of the government).

35. § 3729(a) (defining the creation of the liability).

36. § 3729(b)(1) (defining knowledge of false information).

37. False Claims Amendments Act of 1986, Pub. L. 99-562, 100 Stat. 3153 (1986).

38. Press Release, U.S. Dep't of Justice, Justice Department Recovers Over $3.5 Billion From False Claims Act Cases in Fiscal Year 2015 (Dec. 3, 2015), https://www.justice.gov/opa/pr/justice-department-recovers-over-35-billion-false-claims-act-cases-fiscal-year-2015.

39. § 3729(d).

40. Fraud Enforcement and Recovery Act of 2009, Pub. L. No. 111-21, 123 Stat. 1617 (2009).

41. Patient Protection and Affordable Care Act, Pub. L. 111-148, 124 Stat. 119 (2010) (extending the reach of the False Claims Act, 31 U.S.C. §§ 3729-33).

42. Justice Dep't Recovers Over $3.5 Billion, *supra* note 38.

43. Justice Dep't Recovers Over $3.5 Billion, *supra* note 38.

One attorney has indicated that under the False Claim Act, whistleblowers with their information under seal will eventually need to reveal their identity in court, but their identity can remain under seal and known only to a few within the government agency during the government investigation stage.[44]

The Whistleblower Protection Act of 1989 (WPA) has whistleblower protection as its primary objective, thus making it the second federal law focusing on whistleblowers.[45] Congress wanted federal employees to speak up if they saw something inappropriate in the government workplace and wanted to protect these whistleblowers from retaliation. The WPA focuses on federal employees that may become whistleblowers that report, with a reasonable belief that waste, fraud, or abuse by an agency has occurred. The WPA was amended by the 2012 Whistleblower Protection Enhancement Act (WPEA). The WPA protects federal employees from retaliation in the form of a negative personnel action because they reported waste, fraud, or abuse. This statute required the appointment of a Whistleblower Protection Ombudsman by the Inspectors General.

All federal employees of agencies are not covered by the WPA or the WPEA. As just one example, postal workers are not covered. The WPA as amended by the WPEA provides for confidential reporting of waste, fraud, or abuse. Several court cases narrowed the applicability of the WPA to "job-duty whistleblowers" and the lack of First Amendment protections to these whistleblowers as well.[46] The protections are there for those who speak out about a matter of public concern. Thus the need for additional uniform whistleblower protections.

B. *Early Federal Laws with Secondary Whistleblower Protections*

There are many federal laws with a focus on whistleblower protection within the law. Some of these laws will be discussed within this

---

44. Tony Munter, Can You Remain Anonymous While Blowing the Whistle on Fraud?, Price Benowitz, LLP, https://whistleblower-quitam-attorney.net/whistleblower/the-experience/can-you-remain-anonymous/ (last visited June 27, 2018).

45. Whistleblower Protection Act of 1989, Pub. L. No 101-12, 103 Stat. 16 (1989) (codified as amended in scattered sections of 5 U.S.C.).

46. *See* Garcetti v. Ceballos, 547 U.S. 410 (2006); Borough of Duryea, Pennsylvania v. Guarnieri, 564 U.S. 379 (2011); Wintraub v. Bd. of Ed., 593 F.3d 196 (2nd Cir. 2010); Ruotolo v. City of New York, 514 F.3d 184 (2nd Cir. 2008); Nichols v. Dancer, 657 F.3d 929 (9th Cir. 2011) (where the courts have determined that government employees that act within their official duties do not have a First Amendment right of free speech and are not protected from retaliation when they blow the whistle on their government employers); see also Richard Moberly, Sarbanes-Oxley's Whistleblower Provisions: Ten Years Later, 64 S.C. L.R. 1, 15 (2012).

section, but not all of them.[47] We will also not discuss state laws protecting whistleblowers.

The Lloyd-LaFollette Act of 1912 was created by Congress to overrule two Executive Orders of two presidents[48] which both forbade federal employees from communicating directly with Congress without the permission of the supervisors. These executive orders occurred during a period where the employees were unsatisfied with their working conditions and pay. The Lloyd-La Follette Act states, "[n]o person in the classified civil service of the United States shall be removed or suspended without pay therefrom except for such cause as will promote the efficiency of such service and for reasons given in writing." In addition, federal employees could provide confidential information to Congress, individual congressional members, or committees and not be denied or interfered with.

The Freedom of Information Act of 1966 (FOIA) was passed in order to give more transparency to the public and to allow the public greater access to governmental records.[49] A FOIA request can be a valuable tool for the whistleblower to obtain documents and records that they might not otherwise obtain from a government agency. In addition, a provision in the FOIA provides an exemption from disclosure of any record that would disclose a confidential source used for purposes of law enforcement.[50] This provision could protect the whistleblower that provides information to a governmental entity. Exemption 7(D) ensures that "confidential sources are not lost through retaliation against the sources for past disclosure or because of the sources' fear of future disclosure."[51]

---

47. *See* Jon O. Shimabukuro & L. Paige Whitaker, *Whistleblower Protections Under Federal Law: An Overview,* CONG. RES. SERV. (Sept. 13, 2012), https://fas.org/sgp/crs/misc/R42727.pdf (discussing nineteen federal laws with whistleblower provisions protecting both the federal worker and private citizen).

48. Theodore Roosevelt, Exec. Order No. 163 (1902); William H. Taft, Exec. Order No. 1142 (1909).

49. Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 522 (2016)).

50. *Id*. at § 522 (b)(7)(D); *See* Billington v. D.O.J., 301 F. Supp. 2d 15, 22 (D.D.C. 2004) (stating that "Exemption 7(D) has long been recognized as affording the most comprehensive protection of all FOIA's law enforcement exemptions" (citing Voinche v. F.B.I., 940 F. Supp. 323, 331 (D.D.C. 1996)); *See also* Irons v. F.B.I., 880 F.2d 1446, 1451 (1st Cir. 1989).

51. *See generally* Department of Justice Guide to the Freedom of Information Act, U.S. DEP'T OF JUST., https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption-7d.pdf (last visited Mar. 19, 2018), (citing relevant precedent, Ortiz v. HHS, 70 F.3d 729, 732 (2d Cir. 1995) (stating that "Exemption 7(D) is meant to protect confidential sources from retaliation that may result from the disclosure of their participation in law enforcement activities"); McDonnell v. United States, 4 F.3d 1227, 1258 (3d Cir. 1993) (finding that "goal of Exemption 7(D) [is] to protect the ability of law enforcement agencies to obtain the cooperation of persons having relevant information and who expect a degree of confidentiality in return for their coopera-

The Civil Service Reform Act of 1978[52] is also known as the Federal Service Labor-Management Relations Statute and allows for non-postal government workers to unionize, but includes important whistleblower provisions.[53] The whistleblower provision in this statute states:

> "the authority and power of the Special Counsel should be increased so that the Special Counsel may investigate allegations involving prohibited personnel practices and reprisals against Federal employees for the lawful disclosure of certain information and may file complaints against agency officials and employees who engage in such conduct."[54]

This provision gives non-postal federal whistleblowers the right to appeal to the Merit System Protection Board if they believe they have suffered retaliation for disclosing information and a complaint in the court system was not successful. The Whistleblower Protection Act of 1989 strengthened the whistleblower provisions.

According to the Occupational Safety and Health Act of 1970 (OSHA), if an employee believes that working conditions are unsafe or unhealthful, a confidential complaint can be filed.[55] OSHA will

---

tion"); Providence Journal Co. v. U.S. Dep't of the Army, 981 F.2d 552, 563 (1st Cir. 1992) (explaining that Exemption 7(D) is intended to avert "drying-up" of sources) (citing Irons, 880 F.2d at 1450-51); Nadler v. D.O.J., 955 F.2d 1479, 1486 (11th Cir. 1992) (observing that "fear of exposure would chill the public's willingness to cooperate with the FBI . . . [and] would deter future cooperation" (citing Cleary v. F.B.I., 811 F.2d 421, 423 (8th Cir. 1987); Shaw v. F.B.I., 749 F.2d 58, 61 (D.C. Cir. 1984) (holding that purpose of Exemption 7(D) is "to prevent the FOIA from causing the 'drying up' of sources of information in criminal investigations"); Schoenman v. F.B.I., 763 F. Supp. 2d 173, 200 (D.D.C. 2011) (concluding that F.B.I. properly invoked Exemption 7(D) because as it stated in its declaration "public disclosure of [confidential] source information would have a chilling effect on the cooperation of other sources and thereby hinder its ability to gather confidential information"); Sellers v. D.O.J., 684 F. Supp. 2d 149, 161 (D.D.C. 2010) (noting that exemption "not only protects confidential sources, but also protects the ability of law enforcement agencies to obtain relevant information from such sources"); Miller v. D.O.J., 562 F. Supp. 2d 82, 122 (D.D.C. 2008) (recognizing that "[e]xperience has shown the F.B.I. that its sources must be free to provide information 'without fear of reprisal' and 'without the understandable tendency to hedge or withhold information out of fear that their names or their cooperation with the FBI will later be made public'" (quoting agency declaration)); Wilson v. D.E.A., 414 F. Supp. 2d 5, 15 (D.D.C. 2006) (concluding that release of names of D.E.A. sources could jeopardize D.E.A. criminal investigative operations and deter cooperation of future potential DEA sources); Garcia v. D.O.J., 181 F. Supp. 2d 356, 375 (S.D.N.Y. 2002) (holding that "Exemption 7(D) [en]sures that confidential sources are protected from retaliation in order to prevent the loss of valuable sources of information").

52. Civil Service Reform Act of 1978, Pub. L. 95-454, 92 Stat. 1111 (codified as amended in scattered sections of 5 U.S.C. § 1101 (2012)).

53. The Statute, U.S. Fed. Lab. Relations Auth., https://www.flra.gov/about/introduction-flra/statute (last visited June 19, 2018).

54. 5 U.S.C. § 1101.

55. *How to File a Safety and Health Complaint*, OCCUPATIONAL SAFETY AND HEALTH ADMIN., www.osha.gov/workers/file_complaint.html (last visited Feb. 20, 2018) (the form itself allows the reporting employee to check a box indicating, "Do NOT reveal my name to my Employer").

keep the complaint confidential.[56] It is also illegal for an employer to retaliate against an employee that has filed a complaint with OSHA. If retaliation has occurred, the employee can file a whistleblower complaint with OSHA.

The Occupational Safety and Health Administration recently published a final rule reinforcing the current requirement that employers must have a reasonable procedure for employees to report workplace safety injuries or illnesses without employees being subject to discipline or discrimination.[57] The rule precludes employers from using or threatening drug testing to retaliate against employees who report injuries or illnesses.

The Internal Revenue Code (IRC) also has a provision for whistleblowers.[58] Of course the main purpose of the IRC is the collection of taxes to fund the government, but there is a secondary goal to financially reward those who report delinquent or evasive taxpayers.[59] The IRS protects the identity of a tax fraud whistleblower to the fullest extent that is allowable under the law.[60]

Finally the Inspectors General Act of 1978 established hotlines to report waste, fraud, and abuse.[61] However, in 1989, the Project on Military Procurement testified to the General Accounting Office that they feared hotlines led "unsuspecting sources towards potential professional suicide" due to a lack of confidence in the effectiveness of hotlines and anonymity protections.[62]

C. *Recent Laws with Whistleblower Provisions*

The Public Company Accounting Reform and Investor Protection Act, known as the Sarbanes-Oxley Act[63] (SOX), was passed by Congress as a result of the scandals surrounding Enron, WorldCom, and

56. OSHA Online Complaint Form, Occupational Safety and Health Admin., www.osha.gov/pls/osha7/eComplaintForm.html (last visited June 4, 2018) (the form itself allows the reporting employee to check a box indicating, "Do NOT reveal my name to my Employer").

57. Memorandum from Dorothy Dougherty, Deputy Assistant Secretary OSHA (Oct. 19, 2016), avaiable at www.osha.gov/recordkeeping/finalrule/interp_recordkeeping_101816.html; 29 U.S.C § 660(c).

58. Tax Relief and Health Act of 2006, Pub. L. No. 109-432, § 406(a)(1), 120 Stat. 2922, 2958-59 (2006) (codified as amended at 26 U.S.C § 7623 (2012)).

59. 26 U.S.C. § 7623(b)(1) (2006).

60. *Confidentiality and Disclosure for Whistleblowers*, INTERNAL REVENUE SERV., https://www.irs.gov/compliance/confidentiality-and-disclosure-for-whistleblowers (last visited June 4, 2018).

61. ROBERTA ANN JOHNSON, WHISTLE-BLOWING: WHEN IT WORKS—AND WHY 106 (2003).

62. *Id*. at 107-108.

63. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered sections of 15 U.S.C (2012)).

other companies, which led to the need to reform Wall Street and financial reporting requirements.[64] SOX amended the Securities Exchange Act to embody important whistleblower provisions.[65] "Congress intended that the law would "play a crucial role in restoring trust in the financial markets" by ensuring that "corporate fraud and greed" would be "better detected, prevented and prosecuted."[66] SOX requires publicly held companies in the U.S. to establish "procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters."[67] Thus, SOX provides for "top-down internal control measures that forced securities issuers and public companies to create and maintain internal compliance mechanisms."[68]

Whistleblowers now have a civil cause of action[69] under SOX for retaliation, as well as it a crime to punish or retaliate against whistleblowers.[70] SOX is often referred to as the whistleblower provision because it refers to those who "refuse to engage in and/or report illegal or wrongful activities of their employer or fellow employees,"[71] thus providing a definition for the whistleblower.

SOX mandates that a channel for anonymous whistleblowing is maintained. The audit committees of companies that are covered under SOX must establish procedures where employee whistleblowers can anonymously report issues of concern regarding accounting or auditing matters.[72] Procedures must be in place to treat and retain these whistleblower reports.[73]

---

64. Labriola, *supra* note 4 (discussing the recent cases involving internal business corruption and fraud).

65. *See* Sarbanes-Oxley Act, 15 U.S.C. § 301.

66. Labriola, *supra* note 4, at 2848, (citing STEPHEN M. KOHN ET AL., WHISTLEBLOWER LAW: A GUIDE TO LEGAL PROTECTIONS FOR CORPORATE EMPLOYEES, at xi (2004)).

67. § 301(4)(B).

68. Labriola, *supra* note 4, at 2849.

69. § 806.

70. § 1107 (creating a broad rule covering all whistleblowing activities, not just those for security fraud).

71. ROBERT T. BEGG, WHISTLEBLOWER LAWS AND ETHICS, ETHICAL STANDARDS IN THE PUBLIC SECTOR: A GUIDE FOR GOVERNMENT LAWYERS, CLIENTS, AND PUBLIC OFFICIALS 187 (Patricia Salkin, ed A.B.A. 2008).

72. Terry Morehead Dworkin, *SOX and Whistleblowing,* 105 MICH. L. REV. 1757, 1760-61 (2007).

73. *Id.* at 1761(citing Jennifer Bjorhus, *Hot Lines Hot: Watchdog Law Has Companies Scrambling to Line Up Off-site Services to Record Anonymous Employee Comments*, ST. PAUL PIONEER PRESS, at D1 (Oct. 12, 2004)).

The adopting release for Rule 10A-3 (Release No. 33-8220) specifically provides flexibility for the audit committees to develop "procedures appropriate for their circumstances" and does not mandate specific procedures or a "one-size-fits-all" approach. However, nearly all public companies have chosen to include a whistleblower hotline as part of their SOX 301 compliance. SOX also "contains an antiretaliation provision providing a civil cause of action by an employee against the employer that has retaliated against the employee due to the whistleblowing."[74]

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank),[75] was considered a game changer for whistleblower protections.[76] The Securities and Exchange Commission (SEC) recently made statements regarding the importance of whistleblowers in a settled case that involved the reporting of bribes and accounting irregularities related to the bribes. A "[t]hreat of financial punishment for whistleblowing is unacceptable."[77] "We will continue to take a hard look at these types of provisions and fact patterns."[78] Similarly, the SEC has stated that the agency is "committed to protecting identity to the fullest extent possible."[79] According to research, the single best way to combat fraud is to provide a way for employees to report anonymously.[80]

"The whistleblower program was designed to complement, rather than replace, existing corporate compliance programs. While it provides incentives for insiders and others with information about unlawful conduct to come forward, it also encourages them to work within their company's own compliance structure, if appropriate."[81] The SEC is prohibited from disclosing "any information, including information

74. Richard Moberly, *Sarbanes-Oxley's Whistleblower Provisions: Ten Years Later*, 64 S.C. L.R. 1, 7 (2012).

75. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010).

76. *See* KOHN, *supra* note 22 (exploring federal and state whistleblower laws).

77. *See* Press Release, U.S. Sec. and Exch. Comm'n, SEC Charges Anheuser-Busch inBev With Violating FCPA and Whistleblower Protection Laws (Sept. 28, 2016) (available at https://www.sec.gov/news/pressrelease/2016-196.html) (discussing a $6 million settle agreement after an investigation uncovered inadequate accounting methods which allowed for third-party bribes in India and an agreement to quiet the whistleblower).

78. *Id*.

79. *Frequently Asked Questions*, U.S. SEC. AND EXCH. COMM'N, https://www.sec.gov/about/offices/owb/owb-faq.shtml (last visited May 19, 2018).

80. *2016 ACFE Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study*, ASS'N OF CERTIFIED FRAUD EXAM'RS (Feb. 21, 2017), http://www.acfe.com/rttn2016/about/executive-summary.aspx (reporting a study of 2,410 cases of occupational fraud that occurred in 114 countries exceeding $6.3 billion dollars).

81. *Frequently Asked Questions*, *supra* note 79.

provided by a whistleblower to the Commission, which could reasonably be expected to reveal the identity of a whistleblower."[82] Whistleblower information should remain confidential.[83]

In addition, under the SEC program rules, whistleblowers who voluntarily provide original information that leads to an enforcement actions with monetary sanctions over one million dollars will enable the whistleblower to receive an award of 10-30 percent of the money collected by the SEC.[84] "Any whistleblower who anonymously makes a claim for an award . . . shall be represented by counsel if the whistleblower anonymously submits the information upon which the claim is based. Prior to the payment of an award, a whistleblower shall disclose the identity of the whistleblower and provide the information as the Commission [SEC] may require, directly or through counsel for the whistleblower."[85] Of course the attorney will know the identity of the whistleblower, but due to attorney-client confidentiality provisions, there are few circumstances in which the attorney can divulge the information without client consent.[86] "By law, the SEC protects the confidentiality of whistleblowers and does not disclose information that might directly or indirectly reveal a whistleblower's identity."[87] As an example, the law firm of Katz, Marshall & Banks represented an anonymous whistleblower that received an award of approximately $2.5 million for the whistleblower's role in stopping the illegal activity of a mutual fund company.[88]

In the case of *Kansas Gas & Electric v. Brock*, the U.S. Court of Appeals for the Tenth Circuit set precedent to protect whistleblowers that report internally.[89] This case involved an employee who was fired for filing an internal safety complaint about the results of a nuclear facility inspection, and subsequently reported it to the Department of

82. 15 U.S.C. § 78u-6(h)(2)(A) (2010).

83. *Id*.

84. *Office of the Whistleblower*, SEC, www.sec.gov/whistleblower (last visited Mar. 19, 2018).

85. 15 U.S.C. § 78u-6(d)(2).

86. Kathleen Clark & Nancy J. Moore, *Buying Voice: Financial Rewards for Whistleblowing Lawyers,* 56 B.C. L. REV. 1697 (2015) (discussing the various attorney-client confidentiality provisions and appropriate whistleblowing by lawyers); Jennifer M. Pacella, *Advocate or Adversary? When Attorneys Act as Whistleblowers,* 28 GEO. J. LEGAL ETHICS 1027 (2015) (discussing SEC rules under Dodd-Frank requiring attorneys to blow the whistle).

87. Press Release, U.S. Sec. And Exch. Comm'n, SEC Announces $2.5 Million Whistleblower Award, (July 25, 2017) (available at https://www.sec.gov/news/press-release/2017-130).

88. *Katz, Marshall & Banks Client Awarded $2.4 Million by SEC Whistleblower Office for Role in Stopping Manipulation of Mutual Fund Share Prices,* KATZ, MARSHALL & BANKS, LLP, http://www.kmblegal.com/news/katz-marshall-banks-client-awarded-24-million-sec-whistleblower-office-role-stopping (last visited June 9, 2018).

89. Kansas Gas & Electric v. Brock, 780 F.2d 1505 (10th Cir. 1985).

Labor.[90] The issue became whether the act of internal reporting was protected under the whistleblower statute. In another case, the appellate court looked at who and what constitutes a whistleblower under the Dodd-Frank Act.[91] This case involved an employee, Asadi, who witnessed a security law violation while stationed at a plant in Iraq and later was retaliated against for the internal reporting.[92] The court determined that Asadi was not a whistleblower because he only reported internally, and not to the SEC. The court ultimately decided that the language of the statute was ambiguous, and it was not the court's place to rewrite the language written by Congress. Since the language of Dodd-Frank was unclear regarding whether Asadi was a whistleblower, the court was not compelled to make the decision. This case conflicts with the SEC's interpretation of the statute as well as several other lower court decisions. Company employees may now feel exposed and vulnerable. In a subsequent case, where the employee reported the violation both internally and to the SEC, the court broadened the definition of a whistleblower. In *Kramer v. Trans-Lux Corp.,* the court indicated that the narrow statutory interpretation in *Asadi* went against the goal of the Dodd-Frank Act.[93]

Most recently the United States Supreme Court has spoken on the issue of the definition of whistleblower. In *Digital Realty Trust, Inc. v. Somers,* the Court held that Dodd-Frank did not protect an internal whistleblower from retaliation who did not report the information to the SEC.[94] The Court determined that the definition of a whistleblower is one "who provides pertinent information to the Commission."[95] The whistleblower in the case, Paul Somers, alleged that his employment was terminated after he reported securities law violations to senior management of his employer. Somers believed that this was retaliation in violation of Dodd-Frank. The Court disagreed with this argument and made literal interpretations of three clauses in Dodd-Frank to determine "what conduct, when an engaged "whistleblower," is shielded from employment discrimination."[96] A whistleblower with

90. *Id*. at 1508.

91. Asadi v. G.E. Energy, L.L.C., 720 F.3d 620 (5th Cir. 2013).

92. *Id*.

93. Kramer v. Trans-Lux Corp., No. 3:11CV1424 SRU, 2012 WL 4444820 at *1 (D. Conn. Sept. 25, 2012). *See* Jim McQuade, Renee Phillips & Mike Delikat, *Federal Court Decisions Permit Two Dodd-Frank Whistleblower Cases to Proceed*, EMP. L. & LITIG. BLOG (Oct. 11, 2012), http:// www.jdsupra.com/legalnews/federal-court-decisions-permit-two-dodd-58264.

94. Digital Realty Trust, Inc. v. Somers, 138 S.Ct. 767 (2018).

95. *Id*. at 770.

96. *Id*.

conduct that falls outside of this described conduct, "is ineligible to seek redress"[97] under Dodd-Frank.

Whistleblowers do not need to use an internal process before reporting to the SEC. In fact, the U.S. Supreme Court recently ruled that Dodd-Frank whistleblower protections against retaliation only applies to whistleblowers that externally report to the SEC.[98]

In summary, anonymity should always be preserved for as long as possible. However, if a whistleblower wishes to claim a reward available under the law, his or her anonymity will likely be stripped away in favor of confidentiality. Therefore, the compensation needs to be significant to outweigh the professional and personal risks to the whistleblower.

D. *Additional Whistleblower Guidelines*

The International Ombudsman Association is an organization that may provide an avenue of confidentiality when setting up an internal whistleblower plan. The International Ombudsman Association was created in 2005 to "advance the profession of organizational ombudsman and ensure that practitioners are able to work to the highest professional standards.[99] The organization supports internal ombudsmen groups working within businesses, educational institutions, the government, and nonprofit ventures.[100]

A provision in the International Ombudsman Association Standards of Practice concerns the confidentiality of the whistleblower.[101] The provision suggests that the Ombudsman should "take all reasonable steps to safeguard confidentiality,"[102] including "the identity of any individual contacting the Ombudsman office."[103]

III. DEFINING THE PROBLEM

> "Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth." Oscar Wilde[104]

---

97. *Id*. at 770-71.

98. *Id*. at 779.

99. *About Us,* INT'L OMBUDSMAN ASSOC., https://www.ombudsassociation.org/About-Us.aspx (last visited June 9, 2018).

100. *Id*.

101. *IOA Standards of Practice*, INT'L OMBUDSMAN ASSOC., https://www.ombudsassociation.org/IOA_Main/media/SiteFiles/IOA_Standards_of_Practice_Oct09.pdf (last visited Nov. 11, 2018).

102. *Id*.

103. *Id*.

104. OSCAR WILDE, THE CRITIC AS ARTIST (1891).

In this section, we outline key issues that threaten the effectiveness of modern whistleblowing. First, we discuss potential motivations for the identification of whistleblowers. Second, we discuss key differences between anonymity and confidentiality. Third, we discuss different types of identification, along with various methods interested parties might employ to identify anonymous whistleblowers. Lastly, we address some challenges with respect to obtaining evidence to support retaliation claims.

A. *Motivations for Whistleblower Identification*

Before we can take steps to protect a group of individuals, we must first better understand the threats against them. Threat modeling is an approach that attempts to identify the actors and methods employed by those actors to ensure that proper safeguards are in place.[105] This section will describe some of the possible motivations for identifying whistleblowers.

In the context of whistleblowing, there are many actors that might be highly interested in discovering the wrongdoing being reported and/or identifying the individual(s) making the report. Each type of actor is motivated differently. We have classified these actors into the following groups: accused, employer, competitors, government agencies, state-sponsored adversaries, media organizations, criminals, and hacktivists. Examples of what might motivate actors to attack reporting systems include self-preservation, economic benefit, power, and social justice. Therefore, we must ensure that these threats have been considered.

The most common threat against whistleblowers comes in the form of retaliation levied by the individuals that are accused of wrongdoing and/or other members of the organization.[106] These actors have a vested interest in suppressing the reporting of the wrongdoing because they feel that its disclosure will result in negative consequences for them. If the individuals responsible for reporting can be identified, it might be possible to prevent the wrongdoing from being disclosed publicly. It is also important to note that employers regularly monitor employee behavior, which can thwart efforts to expose corruption prior to a report even being made. For example, an employer might be able to detect an individual attempting to gather evidence of a wrongdoing.

---

105. ADAM SHOSTACK, THREAT MODELING: DESIGNING FOR SECURITY 3-25, 34-42 (2014).

106. Michael T. Rehg, *Retaliation Against Whistle-Blowers: An Integration and Typology*, 11 J. ACAD. BUS. & ECON. 47, 48 (2011).

However, attempts to compromise the reporting of wrongdoing are not limited to those within the organization. While illegal within the United States, both domestic and foreign competitors have been known to engage in corporate espionage.[107] The mere existence of a reporting system that potentially contains an organization's deepest and darkest secrets presents an attractive target. For example, if a competitor is able to gain access to such a system, it would then be possible for evidence of wrongdoing to be passed along to media organizations or law enforcement to negatively impact public perception and/or reduce market value. On the other hand, government agencies and other state-sponsored adversaries could potentially be interested in obtaining such information to gain leverage over certain individuals in the organization.[108]

Data breaches are a regular headline today and most cyber thieves are equal opportunity criminals willing to attack any system of value. If an organization employs a poorly protected reporting system, one can expect cyber attacks to eventually compromise it. Depending upon the information that is obtained, opportunistic hackers could resell that knowledge on the dark web or exploit it for their own purposes.[109]

In free societies, the media is expected to hold individuals, organizations, and the state accountable for its actions, which makes whistleblowers attractive sources.[110] While proper journalistic practices would not condone unethical methods of obtaining sources or evidence, this is likely untrue for hacktivists. While the two might be similarly motivated, hacktivists commonly feel that the ends justify the means.[111]

B. *Anonymity Versus Confidentiality*

Perhaps the most fundamental issue plaguing existing whistleblowing laws is the lack of specific definitions for confidentiality and anonymity. As a whistleblower wishing to remain anonymous, this

107. Marjorie Chan, *Corporate Espionage and Workplace Trust/Distrust*, 42(1) J. BUS. ETHICS 45, 46 (2003); William M. Fitzpatrick, Samuel A. DiLullo, Donald R. Burke, *Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law*, 12 ADVANCES IN COMPETITIVENESS RES. 57 (2004).

108. Scott Jasper & James Wirtz, *Cyber Security*, *in* THE PALGRAVE HANDBOOK OF SECURITY, RISK & INTELLIGENCE 159-164 (2017).

109. *Id*.

110. JOHNSON, *supra* note 61, at 10; TOM DEVINE & TAREK F. MAASSARANI, THE CORPORATE WHISTLEBLOWER'S SURVIVAL GUIDE 108-10 (2011).

111. Brett Lunceford, *Programs or People? Participation and the Ethics of Hacktivism*, *in* CONTROVERSIES IN DIGITAL ETHICS 82-88 (2016).

distinction becomes crucial. If a whistleblower is identified, it can lead to significant financial losses including the end of a job or worse yet, a career.[112] Despite being central aspects of statutes designed to protect whistleblowers, the ambiguity surrounding these terms has allowed for a wide interpretation of what satisfies the legal requirements, especially with respect to technical aspects of whistleblower reporting systems. This section will contrast confidentiality and anonymity.

According to experts "anonymity is one polar value of a broad dimension of identifiability versus nonidentifiability"[113] along a continuum from "fully anonymous to fully identified".[114] Once a person can be identified along one or more of the seven dimensions of identity, maintaining his or her anonymity is no longer possible.[115] Similarly, individuals often assume that confidentiality also provides anonymity. Confidentiality is employed when a source's identity can be known to at least one authorized person, but he or she promises that the source's identity will not be shared with any unauthorized parties.[116] However, since the source is identified by at least one individual, all expectations of anonymity must be abandoned.[117] Therefore, anonymity can only be achieved if it is impossible for any person to identify the individual in question.

Consequently, it is impossible to achieve anonymity in non-mediated interactions.[118] This might occur when an employee raises a concern to his or her superior as prescribed in an open-door policy. In those situations, confidentiality is a whistleblower's only hope. Since at least one person knows the identity of the source, the whistleblower's safety is dependent upon his or her identity not being shared with someone interested in retaliating against the whistleblower.

C. *Identifying Anonymous Whistleblowers*

> "You know, it's not everyday that a whistleblower is actually willing to be identified." Laura Poitras[119]

---

112. Kathleen Clark & Nancy J. Moore, *Buying Voice: Financial Rewards for Whistleblowing Lawyers,* 56 B.C. L. REV. 1697, 1700 (2015).

113. Gary T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity*, 15 THE INFOR. SOC'Y 99, 100 (1999) (defining the terms anonymity and identifiability).

114. Craig R. Scott, *To Reveal or Not to Reveal—A Theoretical Model of Anonymous Communications*, 8(4) COMM. THEORY 381, 387 (1998).

115. Marx, *supra* note 113, at 100.

116. Scott, *supra* note 114, at 383.

117. Scott, *supra* note 114, at 383.

118. Scott, *supra* note 114, at 382.

119. Laura Poitras & Tom Engelhardt, *Tomgram: Laura Poitras and Tom Engelhardt, The Snowden Reboot,* TOMDISPATCH (Oct. 19, 2014, 5:01 PM), http://www.tomdispatch.com/blog/175909/tomgram%3A_laura_poitras_and_tom_engelhardt,_the_snowden_reboot/.

There are many potential threats to anonymity and failing to account for just one might be the difference in a whistleblower remaining anonymous and potentially the subject of unlawful retaliation. To truly understand how anonymity can be compromised, one must first understand the various ways one might be identified.[120] Marx provides an excellent framework for assessing whether a given system truly delivers anonymity.[121] The seven types of identity knowledge he outlined consist of: "(1) legal name, (2) locatability, (3) pseudonyms that can be linked to legal name and/or locatability (i.e, a form of pseudo-anonymity), (4) pseudonyms that cannot be linked to other forms of identity knowledge, (5) pattern knowledge, (6) social categorization and (7) symbols of eligibility/noneligibility."[122] In this section, we first provide a brief discussion of each type of identity knowledge and then follow with examples to illustrate how a whistleblower might be identified, especially in today's digital world. Note that some techniques apply to multiple types of identity knowledge and thus are only mentioned in the type deemed to be the best fit.

1. Legal Name

If an individual's legal name can be associated with a given action, his or her activity cannot be considered anonymous.[123] This would occur if a source volunteers his or her identity, even if it was done unwittingly. Once a legal name has been attached, all anonymity is immediately and irrevocably lost. For example, let's look at the following hypothetical involving Wendy the whistleblower, Faythe the compliance officer, and Chuck the wrongdoer. If Wendy reports an instance of fraud committed by Chuck to Faythe, some would consider Wendy's anonymity protected by Faythe if she simply never mentions her name to anyone. However, since Faythe knows that Wendy was the source of the report, no anonymity exists between Wendy and Faythe. Instead, Wendy has only truly achieved confidentiality with Faythe, and Wendy's anonymity between her and Faythe is dependent upon Faythe keeping Wendy's identity a secret. If Wendy instead reported the fraud to Mallory, who happened to be an accomplice in Chuck's fraud, Wendy's identity as the whistleblower would be in jeopardy because Mallory would have no interest in protecting Wendy.

120. Marx, *supra* note 113, at 100-02.
121. Marx, *supra* note 113, at 100-02.
122. Marx, *supra* note 113, at 100.
123. Marx, *supra* note 113, at 100.

Unfortunately, one of the most famous cases of whistleblower retaliation occurred in exactly this manner. Four National Security Agency (NSA) executives, Thomas Drake, William Binney, Kirk Wiebe and Ed Loomis, along with Diane Roark, then a staff member of the House of Representatives Permanent Select Committee on Intelligence, attempted to blow the whistle on government surveillance programs.[124] They first raised their concerns directly to senior NSA officials in 2001, then in 2002, filed a complaint with the Inspector General's office of the U.S. Department of Defense, which was responsible for protecting whistleblowers.[125] Under the Whistleblower Protection Act of 1989, they expected their identities to be protected to shield them from retaliation.[126]

However, in November 2005, after Drake witnessed the surveillance program expand rather than see action taken to curb the waste and abuses, he felt that it was necessary to leak information to the press.[127] Drake set up a Hushmail[128] e-mail account and contacted Sibohan Gorman at the *Baltimore Sun* under the pseudonym The Shadow Knows.[129] Drake says that he established three ground rules for his leaks to Gorman: "neither he nor she would reveal his identity; he wouldn't be the sole source for any story; he would not supply her with classified information."[130] Articles critical of the National Security Agency's surveillance activities were published by *The New York Times* in December 2005[131] and the *Baltimore Sun* in May 2006.[132] The *Baltimore Sun* article specifically named the ThinThread program, which was the in-house and privacy-focused alternative to the warrantless wiretap program awarded to private contractors that Drake and his colleagues felt violated the U.S. Constitution.[133]

The Bush administration wanted to identify the sources of both stories,[134] believing that they might have been the same individual.[135] It

124. MARK HERTSGAARD, BRAVEHEARTS: WHISTLE BLOWING IN THE AGE OF SNOWDEN 97-107 (2016).

125. *Id*. at 34.

126. *Id*. at 105.

127. *Id*. at 35.

128. HUSHMAIL, https://www.hushmail.com/ (last visited June 25, 2018).

129. Jane Mayer, *The Secret Sharer*, THE NEW YORKER (May 23, 2011), https://www.newyorker.com/magazine/2011/05/23/the-secret-sharer.

130. *Id*.

131. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

132. HERTSGAARD, *supra* note 124, at 36.

133. Siobhan Gorman, *NSA Killed System That Sifted Phone Data Legally*, THE BALT. SUN (May 18, 2006), https://archive.commondreams.org/scriptfiles/headlines06/0518-07.htm.

134. HERTSGAARD, *supra* note 124, at 111.

is alleged that Henry Shelley, general counsel of the Office of Inspector General, expressed a desire to tell the Federal Bureau of Investigation agents investigating the leak about the NSA whistleblowers, despite his duty to protect them.[136] On July 26, 2007, the homes of Binney, Wiebe, Loomis and Roark were each raided by the FBI.[137] After Drake's home was raided in November 2007, he found himself "stripped of his security clearance, indicted, threatened with life in prison, deprived of his federal pension, blackballed in security circles, and reduced to working as a clerk at an apple store."[138] This example illustrates why any process that only achieves confidentiality by promising to withhold a source's legal name can never be considered anonymous and would not be suitable for protecting whistleblowers.

2. Locatability

Locatability refers to an individual's "reachability" in both the physical sense, as well as digital.[139] In addition to one's physical location, locatability could also be in the form of an email address or telephone number, regardless of whether one's legal name is associated with it. Modern technology has made it even easier to locate individuals, commonly without their knowledge. Despite a whistleblower's best efforts, he or she might be unable to avoid detection. Digital communication devices transmit data that can be used to locate the user. A whistleblower's IP address and telephone number can be traced to the individual's identity, and possibly specific location. To avoid disclosing an identifiable IP address, the user would have to rely on multiple proxies, such as a virtual private network (VPN) or the Tor Anonymity Network.[140] Further jeopardizing a whistleblower's anonymity is the proliferation of Internet-connected and location-enabled devices. Modern cell phones, vehicles, and cameras typically showcase features that can pinpoint an individual's location, such as through the use of the Global Positioning System (GPS). Cellular signals can be triangulated to locate the user of a given cell phone[141]

135. Mayer, *supra* note 129.

136. HERTSGAARD, *supra* note 124, at 111; Charles Clark, *Pentagon Watchdog Officials Now Under Justice Department Probe,* GOV'T EXEC. (Mar. 22, 2016), https://www.govexec.com/defense/2016/03/pentagon-watchdog-officials-now-under-justice-department-probe/126859/.

137. HERTSGAARD, *supra* note 124, at 112.

138. HERTSGAARD, *supra* note 124, at 98.

139. Marx, *supra* note 113, at 101.

140. Roger Dingledine, Nick Mathewson & Paul Syverson, *Tor: The second-generation Onion Router* (2004), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA465464 (last visited June 25, 2018).

141. Malte Spitz, *Your Phone Company is Watching* (2012), https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching (last visited June 25, 2018); Von Kai Biermann, *Be-*

while Internet Protocol (IP) addresses can locate a user connected to the Internet, especially when correlated with other geolocation methods.[142] Even retail stores regularly track consumer movements by monitoring Bluetooth and Wifi identifiers unique to mobile devices.[143]

It was the tracing of emails and phone calls between former Central Intelligence Agency case officer Jeffrey Alexander Sterling and reporter James Risen that led to Sterling being charged and convicted of espionage.[144] To illustrate this further, a potential whistleblower wanted to use email as the method of sending information about an internal safety issue but feared identification. The potential whistleblower used Reddit[145] to inquire about the best way to stay anonymous with the post below:

> I have a situation where I need to send a whistleblower email. It needs to be anonymous. As this is concerning a safety issue and an ongoing lawsuit theres [*sic*] a good chance someone may spend a good deal of time trying to determine the source of the email. My plan was to use my paid VPN at a public wifi hotspot along with a temporary mailbox such as mailinator or 10minutemail (I only need to send a single message, not receive). Will this be enough? Do i [*sic*] need to worry about my MAC address or host name? I don't have the time or technical know-how to even think about going down the TOR route. Any advice is greatly appreciated[146]

This particular Reddit user wisely took steps to disassociate him or herself from post. First, we can see that the user created a unique account for the sole purpose of asking for help with this issue. The username of "76df43" is seemingly random and no other posts are made outside of this thread. Second, the user is clearly aware of how a virtual private network (VPN) can shield the IP address from most adversaries. However, the user could potentially be identified if the VPN provider maintains logs of account activity and the user created

---

trayed by our own data, ZEIT ONLINE (Mar. 10, 2011), https://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz; *Telephone*, ZEIT ONLINE, https://www.zeit.de/datenschutz/malte-spitz-data-retention (last visited June 25, 2018).

142. *Geolocation API Specification 2nd Edition*, WORLD WIDE WEB CONSORTIUM (W3C) (2016), https://www.w3.org/TR/geolocation-API / (last visited June 26, 2018).

143. Dieter Oosterlinck, Dries Benoit, Philippe Baecke & Nico Van de Weghe, *Bluetooth Tracking of Humans in an Indoor Environment: An Application to Shopping Mall Visits*, 78 APPLIED GEO. 55, 56 (2017); Jessica Gallinaro, *Meet Your New Big Brother: Weighing the Privacy Implications of Physical Retail Stores Using Tracking Technology*, 22 GEO. MASON L. REV. 473, 474 (2015).

144. United States v. Sterling, 818 F.Supp. 2d 945, 947 (E.D. Va. 2011), *rev'd*, 724 F.3d 482 (4th Cir. 2013).

145. REDDIT, www.reddit.com (last visited June 25, 2018).

146. 76df43, REDDIT (Feb. 4, 2015), https://www.reddit.com/r/privacy/comments/2upzw6/how_to_send_an_anonymous_whistleblower_email/ (last visited June 11, 2018).

the VPN account using his or her true identity or a traceable payment method.[147]

Of course, the rapid adoption of cameras for surveillance purposes can also jeopardize the whistleblower. For example, China has invested heavily in surveillance technology which, as was demonstrated to British Broadcasting Corporation correspondent John Sudworth, is capable of locating targets using facial recognition and result in their apprehension in just seven minutes.[148] Further, once located, the prior movements of an individual can be retraced up to a week.[149] While the current timeframe is troubling, additional data storage could essentially allow for location history to be stored indefinitely. The wide-scale adoption of surveillance technology has made it even more difficult for whistleblowers to ensure that their whereabouts remain unknown to interested parties. Footage could place an individual at locations known to be visited by the whistleblower to report the wrongdoing or the very location where the whistleblower witnessed the wrongdoing itself. Given these capabilities, even dropping an unsigned letter into a public mailbox would not ensure that the sender remains anonymous, especially from government actors. Therefore, to remain anonymous, all threats to identification through locatability must be accounted for.

3. Linkable Pseudonyms

Some processes and systems that claim to offer anonymity protections simply replace any references to an individual's legal name with an associated pseudonym.[150] While this might appear to provide anonymity at first glance, it fails to do so since it does not actually sever the link between the pseudonym and identity. One example of this type of identification would be when responses are solicited from known individuals and instead of associating the person's name with the response, a placeholder value, such as an employee ID number, is used instead. Since the number can be traced back to the employee's identity, no anonymity is truly provided. Instead, the user is again dependent upon confidentiality to protect them from retaliation, which is not reliable.

---

147. Charles Arthur, *Second LulzSec Hacker 'Neuron' Could be Tracked Down via UK VPN*, THE GUARDIAN (Sept. 26, 2011), https://www.theguardian.com/technology/2011/sep/26/lulzsec-second-hacker.

148. BBC News, *China: "the world's biggest camera surveillance network" – BBC News*, YOUTUBE (Dec. 25, 2017), https://www.youtube.com/watch?v=pNf4-d6fDoY.

149. *Id*.

150. Marx, *supra* note 113, at 101.

Further, even if a whistleblower feels that reporting wrongdoing would be safer by mailing a physical document, it would be extremely difficult to ensure that all fingerprints and DNA have been removed and that no record of their actions has been collected. Therefore, these characteristics could allow a well-funded and highly motivated actor to potentially identify the individual. Some reporting systems allow for the whistleblower to remain engaged in conversation with an investigator by establishing a unique username or password upon submission. Unfortunately, many of these systems also allow the user to select their own credentials, rather than supplying them with a randomly generated passphrase. Because most people reuse their usernames and passwords for multiple accounts, this could result in the individual being identified by an adversary that has access to such information.

4. Unlinkable Pseudonyms

Unique pseudonyms that have never been linked to a name or location provide the highest degree of anonymity when it is desirable for multiple actions to be associated with the same pseudonym.[151] This is especially useful in the context of whistleblowing since investigators would prefer to maintain contact with the source. To maintain contact, the whistleblower must be able to provide the investigator with some way to associate each contact with the single source. Some systems allow whistleblowers to create their own secret credential that they will use whenever interacting with the system. However, if the user naively selects something that can be linked to his or her identity, any anonymity the system claimed to provide would be compromised. Instead, it would be best for the system to randomly generate a credential for the whistleblower to ensure that users do not accidentally jeopardize their own anonymity.

5. Pattern Knowledge

Further, it is important to note that simply using a random pseudonym does not prevent other actions from betraying the whistleblower's identity. Individuals can also be identified due to recognizable patterns in their behavior, regardless of whether their identity is known.[152] For example, researchers have shown that even if credit card or social media data is stripped of all personally identifying information, individuals can still be identified by correlating seem-

151. Marx, *supra* note 113, at 101.

152. Chris Y.T. Ma, David K.Y. Yau & Nung Kwan Yip, *Privacy Vulnerability of Published Anonymous Mobility Traces*, 21 IEEE/ACM TRANSACTIONS ON NETWORKING 721 (2013).

ingly disparate datasets.[153] As Marx also points out, one might recognize and be able to identify an individual who rides the same subway to work each day, even without knowing his or her legal name.[154] The very details shared in a report could also compromise the source by placing someone at a specific time and place. If a complete list of individuals known to be present at that time can be obtained, all potential witnesses can be combed for additional clues that might point to the source's identity.

A whistleblower can also be identified by technical characteristics. One major challenge in protecting whistleblowers from these types of vulnerabilities is that organizations are rightfully motivated in deterring legitimate insider threats.[155] However, the same measures used to detect malicious activity can jeopardize the anonymity of pro-social whistleblowers.[156]If a whistleblower's digital activity appears similar to malicious insider behavior, it could result in the whistleblower being accused of wrongdoing before they can even blow the whistle.

For example, system logs and digital fingerprints embedded in documents can provide a clear timeline of who accessed a file relevant to the alleged wrongdoing. Wikileaks published documents exposing efforts by the Central Intelligence Agency to identify whistleblowers through digital watermarking with a tool codenamed Scribbles.[157] These techniques are not limited to government agencies. Any individual can employ similar methods using a free online tool called Canarytokens, which was primarily developed to identify data breaches by "phoning home" to the token creator any time a particular resource is accessed.[158] Canarytokens can be generated for particular websites, hostnames, email addresses, images, Microsoft Word or PDF

153. Yves-Alexandre De Montjoye, Laura Radaelli & Vivek Kumar Singh, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata, in* SCI. MAG 347, 536 (2015); and Christopher Riederer, Yunsung Kim, Augustin Chaintreau, Nitish Korula & Silvio Lattanzi, *Linking Users Across Domains with Location Data: Theory and Validation*, *in* PROCEEDINGS OF THE 25TH INT'L CONFERENCE ON WORLD WIDE WEB 708 (2016).

154. Marx, *supra* note 113, at 101.

155. GEORGE SILOWASH, DAWN CAPPELLI, ANDREW MOORE, RANDALL TRZECIAK, TIMOTHY J. SHIMEALL, & LORI FLYNN, COMMON SENSE GUIDE TO MITIGATING INSIDER THREATS 4-5, 56-59, 82-85 (4th ed. 2012).

156. MARISA REDDY RANDAZZO, MICHELLE KEENEY, EILEEN KOWALSKI, DAWN M. CAPPELLI & ANDREW P. MOORE, INSIDER THREAT STUDY: ILLICIT CYBER ACTIVITY IN THE BANKING AND FINANCE SECTOR 16 (2005).

157. *Scribbles User's Guide*, WIKILEAKS, https://wikileaks.org/vault7/document/Scribbles_v1_0_RC1-User_Guide/Scribbles_v1_0_RC1-User_Guide.pdf (last visited June 13, 2018).

158. CANARYTOKENS, http://canarytokens.org/ (last visited June 25, 2018); *Canarytokens Introduction*, THINKST, http://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html (last visited June 13, 2018).

documents.[159] A Canarytoken can even be planted within file folders to receive alerts when users access it.[160] Thus, investigators with ill-intent could send files or links with embedded Canarytokens to anonymous whistleblowers. If a whistleblower does not know how to block such techniques from being able to transmit back to the token creator, his or her identity would be immediately exposed as soon as the resource is opened, all without the whistleblower's knowledge.

Even if a whistleblower printed documents to use as evidence, the exact printer used can be identified by examining unique microscopic tracking dots that are added to each document as an invisible watermark.[161] This type of document fingerprinting was originally intended to prevent forgery, but it was reportedly used as a key piece of evidence in building a case against Reality Leigh Winner.[162] Ms. Winner, a former Air Force linguist, accepted a job as a contractor for the National Security Agency.[163] While assigned to an eavesdropping facility in Georgia, Ms. Winner printed out a top-secret intelligence report and physically removed it from the facility with the intent of mailing it to a reporter at *The Intercept*.[164] The government was notified of the impending publication on May 30, 2017.[165] Ms. Winner was not aware that printing the document could be traced to her through system logs and document watermarking. These clues resulted in Ms. Winner being identified and arrested prior to the story being published on June 5, 2017, less than a week after the government was notified of the forthcoming story.[166]

Simply browsing to the webpage for reporting wrongdoing can also reveal several key pieces of information that could be used to identify

159. *Canarytokens Introduction*, THINKST, http://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html (last visited June 13, 2018).

160. *Id*.

161. Jason Tuohey, *Government Uses Color Laser Printer Technology to Track Documents*, PCWORLD (Nov. 22 2004), https://www.pcworld.com/article/118664/article.html.

162. Charlie Savage, Scott Shane & Alan Blinder, *Reality Winner, N.S.A. Contractor Accused of Leak, Was Undone by Trail of Clues*, N.Y TIMES (June 6, 2017), https://www.nytimes.com/2017/06/06/us/politics/reality-leigh-winner-leak-nsa.html (stating that "color printers leave barely visible microdots identifying the serial number of the printer, the date and time of the printing" which NSA used to identify the printer used by Winner).

163. *Id*.

164. *Id*.

165. Affidavit in Support of Application for Arrest Warrant, United States v. Reality Leigh Winner (S.D. Ga. 2017) (No. MJ 117-024) (evidentiary decisions were recently determined against the defendant).

166. *Id*. All court filings can be viewed at https://cryptome.org/2017/06/winner-nsa-court-files.pdf (last visited June 19, 2018)).

the individual.[167] Most websites today gather and analyze information about its users, such as IP address, web browser, screen resolution, and operating system.[168] These characteristics are typically used in improving website usability, but they can just as easily be used to identify the individual. Many websites also track behavior across multiple websites with browser cookies.[169] For example, if a whistleblower happened to be logged into one website while simultaneously reporting wrongdoing on another, it is possible for a browser cookie to tie the actions on both websites to the same user. Accepting default settings on standard Internet browsers can also leak identifiable data about the user and his or her actions, such as location, browsing history, information that is copied from the website, and the status of the device's webcam, microphone, and battery.[170]

6. Social Categorization

A whistleblower could also be identified through social categorization, such as gender, ethnicity, religion, age, health status, or leisure activities.[171] For example, a whistleblower's voice could be analyzed if they call a telephone hotline.[172] A person's handwriting, or even writing style, especially with the advancement of text analytics, can also be reliably compared to writing attributable to known individuals.[173] For example, the use of proper grammar could reveal the individual's likely education level. Many reporting systems in use today also seek a tremendous amount of contextual information regarding the wrongdoing in question. Unfortunately, by prompting the user to submit this information, a naïve whistleblower is likely to comply, which could potentially jeopardize his or her anonymity. For example, asking a whistleblower to provide information regarding the time, location, or individuals involved could allow for those interested in

167. COMPLETE GUIDE TO INTERNET PRIVACY, ANONYMITY & SECURITY 15-21 (2d ed. Nerel Online, 2015).

168. Peter Eckersley, *How Unique Is Your Web Browser? in* PRIVACY ENHANCING TECHNOLOGIES 1–18 (Mikhail J. Atallah & Nicholas J. Hopper eds., 2010).

169. *Id*.

170. MICHAEL BAZZELL, HIDING FROM THE INTERNET, 61-63 (4th ed. 2018).

171. *Id*.

172. Harry F. Hollien, *Voice and Forensics*, *in* VOICE SCIENCE 231–265 (2005); JOHN OLSSON & JUNE LUCHJENBROERS, FORENSIC LINGUISTICS (3d ed. 2014); John H. L. Hansen & Taufiq Hasan, *Speaker Recognition by Machines and Humans: A tutorial review,* 32(6) IEEE SIGNAL PROCESSING MAG. 74–99 (2015).

173. Sadia Afroz, Avlin Caliskan-Islam, Ariel Stolerman, Rachel Greenstadt & Damon McCoy, *Doppelgänger Finder: Taking Stylometry to the Underground*, *in* IEEE SYMP. SECURITY & PRIVACY 212 (2014); Moshe Koppel & Yaron Winter, *Determining if Two Documents are Written by the Same Author*, 65 J. ASSOC. FOR INFORM. SCI. & TECH. 178 (2013).

retaliation to quickly pinpoint the whistleblower. These types of context clues can vary depending upon the type of wrongdoing being alleged, but every piece of information shared only further reduces the pool of possible whistleblowers.[174]

7. Symbols of Eligibility/Noneligbility

Symbols of eligibility/noneligibility are used for all kinds of activities in modern society.[175] Employee badges, event tickets and toll passes can identify whether an individual has been granted access. However, these symbols are not limited to physical objects. For example, reporting systems can allow for two-way communication with whistleblowers. When a whistleblower wishes to further discuss a prior report, he or she can access the system using a secret passphrase associated with the report for authentication purposes. However, it is important to point out that the security of these symbols is critical to their reliability. If a symbol is compromised, the user will be misidentified. Further, unique lingo or jargon specific to an industry or job role could reveal clues regarding past or present work experience, which might increase credibility, yet also reveal too much about the whistleblower's background. Although not tied to one's legal name directly, this type of information could be correlated to identify the likely source.

D. *Lack of Retaliation Case Law Regarding Anonymous Whistleblowers*

Despite these capabilities, there is little case law that adequately describes the use of these techniques to identify anonymous whistleblowers. We believe that this is likely for a few reasons. First, the Ethics Resource Center reports that 92% of whistleblowers reported their concerns to someone internal to the organization, with 82% reporting to their supervisor at some point in the process.[176] Therefore, the capabilities outlined in this paper are largely unnecessary to identify most whistleblowers because they were likely never anonymous in the first place.

Second, due to continuous log generation and limited storage capacity, system logs might not be stored long enough for whistleblowers to obtain during discovery. While some laws (e.g., Stored

174. STEPHEN M. KOHN, THE NEW WHISTLEBLOWER'S HANDBOOK: A STEP-BY-STEP GUIDE TO DOING WHAT'S RIGHT AND PROTECTING YOURSELF 216 (2013).

175. *Id.*

176. NATIONAL BUSINESS ETHICS SURVEY OF THE U.S. WORKFORCE, ETHICS RESOURCE CENTER 29 (2013).

Communications Act[177] and Sarbanes-Oxley[178]) and industry standards (e.g., Payment Card Industry Data Security Standard (PCI-DSS)[179]) mandate a minimum data retention period for certain data, the retention policies can vary significantly among organizations. If the time between whistleblower identification and the filing of a complaint is greater than the organization's data retention period for the logs sought in discovery, it is unlikely that meaningful evidence will be obtainable. For example, unless other evidence can be uncovered that proves a premeditated and coordinated effort was made to identify the whistleblower, an organization could theoretically identify an anonymous whistleblower and allow the logs to be overwritten by the time a whistleblower ever files a lawsuit for retaliation. Unfortunately, the inability to prove that the whistleblower could have been identified by the organization forces retaliation complaints to be based upon witness testimony and a loose sequence of events without hard proof that the organization targeted the plaintiff in response to efforts to blow the whistle. Therefore, attorneys are unlikely to make timely requests for discovery to uncover the necessary evidence to build such a case.

Third, most whistleblowers are unlikely to be adequately prepared to navigate the technical and legal minefield without accidentally affording the organization a reasonable defense against retaliation. If the organization successfully avoids generating proof of deliberate retaliation and can instead justify its actions based upon sound legal reasoning, the whistleblower is left with little recourse. Therefore, we argue against the advocacy of all types of identified reporting in order to preserve the anonymity protections that whistleblowers deserve. If employees and legislators remain ignorant of these pitfalls, retaliation against whistleblowers will likely continue unabated.

IV. LET'S IMPROVE EXISTING LAWS BY CREATING A NEW, STRONGER LAW

> "In many cases, the best protection against retaliation is to report possible securities violations anonymously." Labaton Sucharow, L.L.P.

Current whistleblower laws in the U.S. do not adequately protect whistleblowers. "U.S. whistleblower policy remains fractured: a

177. Stored Communications Act, 18 U.S.C § 2703(a) (2018).

178. Sarbanes-Oxley Act, 15 U.S.C. § 7213 (a)(2)(A)(i) (2012).

179. PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD (version 3.2.1 2018) (available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss).

patchwork of statutes and case law has led to inconsistent outcomes and incentives, even as the power of whistleblowing in protecting public interest by revealing malfeasance has become clear."[180] It is viewed that the piecemeal approach to the protection of whistleblowers has led to confusion and lack of protection for whistleblowers.[181] We propose a single new federal law in order to strengthen whistleblower protections. This law would not be industry specific and would apply to all sectors, including nonprofits, for-profits, and the government. In this section, we provide recommendations that must be considered during the construction of future federal whistleblower legislation.

A. *Definitions of Anonymity vs. Confidentiality*

To illustrate a critical shortcoming of existing federal whistleblower laws, Table 1 illustrates major federal whistleblower legislation and the lack of definitions for both anonymity and confidentiality. We believe that a new comprehensive federal law should include definitions of both anonymity and confidentiality so that both potential whistleblowers and employers understand the difference between the two terms.

TABLE 1 – ANONYMITY AND CONFIDENTIALITY IN CURRENT WHISTLEBLOWER LAWS

Law	**Adequately Defines**		**Promises Whistleblowers**	
	Anonymity	**Confidentiality**	**Anonymity**	**Confidentiality**
FCA	No	No	No	No
WPA	No	No	No	Yes
WPEA	No	No	No	Yes
LLA	No	No	No	No
FOIA	No	No	No	No
CSRA	No	No	No	Yes
OSHA	No	No	No	Yes
SOX	No	No	Yes	Yes
Dodd-Frank	No	No	Yes	Yes

Laws must ensure that clear definitions are provided for all critical terms. Any ambiguity can result in unintended consequences. There-

180. Bishara, *supra* note 31, at 43.
181. Bishara, *supra* note 31, at 65.

fore, the law, as well as business policies and procedures, should clearly define both terms. The suggested definition for confidentiality is as follows:

> Confidentiality: the identity of the whistleblower will be known by at least one individual as a result of reporting wrongdoing.

However, even if confidentiality is promised to the whistleblower, the identity of the whistleblower can become known to the government, their attorney, a person at work or a third-party reporting company. Given the sensitive nature of whistleblowing and the likelihood of retaliation, we contend that confidentiality is not enough to adequately protect whistleblowers.

We argue that because confidentiality is not sufficient, the law should mandate anonymity. The definition of anonymity must focus on whether the individual can be identified in any way, rather than simply focus on whether he or she provided a name at the time of reporting. As previously discussed, whistleblower anonymity can be compromised in several different ways, leaving them vulnerable to retaliation. Consequently, we argue that true anonymity can only be achieved if absolutely no one can identify the source of the report of wrongdoing. The sender anonymity set is "a subset of all subjects worldwide who may send messages."[182] Therefore, the suggested definition for whistleblower anonymity is as follows:

> Anonymity: the state of being not identifiable within a set of potential whistleblowers, known as the anonymity set.[183]

A whistleblower is only anonymous if he or she cannot be identified in any way as a result of blowing the whistle, including actions taken to acquire evidence of wrongdoing, report concerns internally or externally, as well as any subsequent investigations or legal proceedings. If anonymous reporting cannot be provided, organizations must make it clear that anonymity protections are not available and that any information shared, including one's identity, can only be kept confidential, which offers less protection than anonymity.

B. *Corporate Policies and Procedures*

The proposed law should mandate organizational policies and procedures. These mandated policies and procedures should ensure that all potential whistleblowers are properly notified of their options, are

182. Andreas Pfitzmann & Marit Köhntopp, *Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology*, *in* DESIGNING PRIVACY ENHANCING TECHNOLOGIES 2 (H. Federrath Ed. 2001).

183. *Id*.

assured that the choice to continue or withdraw a report will be respected and that any action taken by the whistleblower will not lead to retaliation. These policies and procedures should provide a mechanism for whistleblowers to report any retaliation. Notice of the requirement of anonymity should also be part of the notification to all employees whom someday may be a whistleblower.

1. Awareness/Notice

It is critical that whistleblowers clearly understand and accept all risks prior to making their report. Regardless of the capabilities of the reporting system, all potential whistleblowers should be provided with definitions of anonymity and confidentiality to reduce the ambiguity surrounding each term. Organizational policies and procedures would be a good starting point for this notice to be located. In addition to being informed of the safest methods to report wrongdoing, potential whistleblowers must also be provided clear explanations of how their identity will be protected.

Instructions should include statements that discourage the sharing of any information that could be used to identify the whistleblower. Similarly, whistleblowers must not be prompted for any specific information. The inclusion of multiple form fields might result in a whistleblower offering too much information without adequately knowing how it might jeopardize anonymity. Instead, a single, open response form should be provided to allow the whistleblower to craft their report however they see fit. Subsequent communication can allow for investigators to obtain additional information, if necessary.

Further, information on how to raise concerns should be distributed in such a way that it protects those who might report by increasing the size of the anonymity set. For example, rather than only providing reporting instructions and a link to the reporting system on a single page of the company website, the instructions can be embedded on each page. This, in effect, makes all visitors to any page of the website potential whistleblowers. For the same reason, all employees should receive physical copies of the whistleblowing policy and procedure. Additionally, regular training on how to report wrongdoing without compromising their safety should be provided. Due to conflict of interest, we recommend that this training be provided by outside information security experts rather than by the employer. All of these actions increase the number of people who have seen the instructions, which expands the anonymity set.

2. Choice/Consent

Whistleblowers must be trusted to choose the most appropriate outlet to raise their concern. Laws intended to protect whistleblowers should not restrict whistleblowers from reporting wrongdoing to whomever they deem will provide the best protection. While organizations would certainly prefer that all whistleblowers raise their concerns internally, this desire is counter to the true goal of correcting wrongdoing. Rather than view external whistleblowers as disloyal members and threats to the organization, potential whistleblowers should be provided reassurance that their safety is paramount and that external outlets are acceptable if a whistleblower perceives internal conditions threaten his or her safety. We propose a single federal agency to which whistleblowers would report wrongdoings and retaliation.

Whistleblowers must always have the option of discontinuing their report. Should a whistleblower's anonymity be compromised in any way in the course of reporting or investigating alleged wrongdoing, the whistleblower must be informed immediately and given the option of withdrawing their report. Failing to properly inform whistleblowers or forcing them to accept what they deem to be undesirable risks would be unethical and negatively impact the perception of the reporting channel for future whistleblowers.

3. Access/Participation

The proposed federal law should ensure that it is mandatory that whistleblowers be allowed reasonable access to the status of any investigation into the alleged wrongdoing. The manner in which access is provided must not compromise the whistleblower's anonymity. This can be achieved by providing whistleblowers with a randomly generated passphrase at the time of the initial report. The passphrase will allow the whistleblower to access the reporting system and maintain communication with investigators throughout the process.

C. *Technical Requirements*

Most of the online reporting channels still in use today were originally developed over 15 years ago in response to the passage of the Sarbanes-Oxley Act. These channels solicit reports via telephone hotlines or standard online forms. Unfortunately, due to poor design and implementation, most channels available today fail to provide any level of reliable anonymity protection without the whistleblower proactively taking steps to protect their own identity. As more infor-

mation is known, the easier it is to narrow down the likely source of a report of wrongdoing. Consequently, a naïve whistleblower could still unintentionally reveal his or her identity simply out of ignorance. Therefore, the proposed law must require that organizations only solicit anonymous reports in a way that minimizes the collection of any information that could be used to identify the whistleblower. Three key improvements to the law can be made with respect to the technical requirements of reporting systems.

First, laws should state the requirement that the "best available technology and reporting methods" should be used by both government and business organizations to ensure the anonymity of all whistleblowers. Although whistleblowing has received considerable attention in the media and academic literature over the past 30 years,[184] there has been limited research focused on an overlooked element of modern whistleblowing; that is, the reporting system itself. This leaves those who attempt to seek protection under the law worse off as the mere existence of well-intended statutes might lead some to gain a false sense of security in believing that their actions are anonymous. Despite its use in practice and a recognized need for such systems in information systems research,[185] little attention has been given to the technical requirements necessary to maintain anonymity in the context of whistleblowing, nor has practice benefited from a proposed design of an effective whistleblowing system. While constructing legislation involving technology is extremely difficult, especially when such systems suffer from inadequate development, it is imperative that laws intended to protect those who reveal wrongdoing must be future-proof by requiring indicate that the best available technology should be used in order to protect the identities of whistleblowers. We also suggest that information systems researchers concentrate on

184. *See* JANET P. NEAR & MARCIA P. MICELI, STANDING UP OR STANDING BY: WHAT PREDICTS BLOWING THE WHISTLE ON ORGANIZATIONAL WRONGDOING?, RES. IN PERSONNEL & HUM. RESOURCES MGMT. 95 (Joseph J. Martocchio ed., 2005); Jessica R. Mesmer-Magnus & Chockalingam Viswesvaran, *Whistleblowing in Organizations: An Examination of Correlates of Whistleblowing Intentions, Actions, and Retaliation*, 62(3) J. BUS. ETHICS 277 (2005); Rafik Elias, *Auditing Students' Professional Commitment and Anticipatory Socialization and Their Relationship to Whistleblowing*, 23 MANAGERIAL AUDITING J. 283 (2008); A. J. BROWN, DAVID LEWIS, RICHARD E. MOBERLY & WIM VANDEKERCKHOVE, INT'L HANDBOOK ON WHISTLEBLOWING RESEARCH (2014); Janet P. Near & Marcia P. Miceli, *Whistle-blowing: Myth and Reality*, 22 J. MGMT. 507 (1996).

185. *See* Paul B. Lowry et al., *The Drivers in the Use of Online Whistle-Blowing Reporting Systems*, 30 J. MGMT. INFORM. SYS. 154 (2013); ChongWoo Park et al., *Overcoming the Mum Effect in IT Project Reporting: Impacts of Fault Responsibility and Time Urgency*, 9 J. ASSOC. INFORM. SYS. 409 (2008); ChongWoo Park & Mark Keil, *Organizational Silence and Whistle-Blowing on IT Projects: An Integrated Model*, 40 DECISION SCI. 901 (2009).

the design of reporting systems with a focus on maintaining whistleblower anonymity.

Second, legislation should require that organizations only employ open-source systems. The ability for interested parties to audit the source code of any system provides the user with reassurances that the system behaves as described. Proprietary, or closed-source, systems do not allow outside parties to inspect the true behavior of the system, which could allow organizations to include methods to identify whistleblowers rather measures to protect them.

Third, in addition to open review of source code, any reporting system being used by an organization must also be required to undergo regular, independent audits that focus on assessing both security and anonymity protections. A 2006 review of internal reporting procedures advocated for the testing of whistleblowing, policies, procedures and systems, yet failed to consider whether the whistleblower's anonymity was properly protected.[186] These audits should also extend to the organization's policies and procedures regarding whistleblowing. Doing so will ensure that the anonymity of whistleblowers is protected by confirming that the process adequately protects whistleblowers from current threats. Including these last two measures will future-proof the law with respect to advances in technology.

D. *Corporate Motivation to Comply with the Law*

Questions could be raised as to whether firms are truly interested in protecting whistleblowers. Given the prevalence of retaliation, it is possible that some organizations are successfully exploiting weaknesses in the law by meeting the minimum standard for compliance while intentionally employing inadequate systems to identify whistleblowers. To combat this issue, legislation must ensure that the requirements for compliance are clearly stated, but in such a way that protections can evolve with technological advances.

If whistleblower laws were to clearly define the differences between anonymous and confidential reporting, any organization that fails to provide a truly anonymous reporting channel would expose itself to increased liability. Employees could take advantage of the organization's poor internal whistleblowing system by submitting an allegation of wrongdoing that they know will identify them to hold the organization hostage. If the organization later attempted to terminate the employee or some other adverse employment action, the employee could

186. Steven E. Kaplan & Joseph J. Schultz, *The Role of Internal Audit in Sensitive Communications*, J. MGMT. STUD. 10, 25 (2006).

point to the organization's ability to identify his or her complaint and claim that the subsequent termination is a form of retaliation. Therefore, the assurance of anonymity not only protects the whistleblower, but also protects the organization.

Further, media organizations such as Wikileaks are aggressively developing their own anonymous reporting channels for the purposes of soliciting tips from the public. For example, the Freedom of the Press Foundation manages the development of SecureDrop[187], an open-source whistleblower submission system. Such systems provide significantly better anonymity protections when compared to what most firms are currently using, which only encourages whistleblowers to disclose their concerns to external outlets. If organizations fail to implement systems with adequate protections, they run the risk of damaging information being aired out publicly.

E. *Punitive Damages*

Existing laws require organizations to defend their statutorily mandated compliance programs. However, whistleblowers rarely obtain favorable decisions unless a clear fact pattern, backed by direct evidence, proves intentional retaliation. Therefore, we suggest that punitive damages be introduced into new laws that allows for a plaintiff to receive funds if an organization implements policies, procedures or systems that can be shown to likely jeopardize whistleblower's anonymity and are reported by the plaintiff. The new federal law should name a government entity such as the SEC or Department of Labor as the administrative agency in charge of compliance. Potential plaintiffs could first bring the organizational whistleblower deficiencies to this agency, and if found not in compliance, then the punitive damages provision would be applicable as punishment to the organization and a reward for the "whistleblower" of the deficiencies. Of course, the deficiencies would need to be remedied.

An organization's failure to maintain adequate internal controls might violate the bookkeeping and accounting provisions of the Foreign Corrupt Practices, Dodd-Frank, and Sarbanes-OxleyActs.[188] While some whistleblowers can blow the whistle on the lack of internal controls under these laws, we argue that comprehensive legislation should encourage and protect this behavior for all whistleblowers.

187. SECUREDROP, https://securedrop.org/ (last visited June 25, 2018).

188. KOHN, *supra* note 22, at 217.

F. *Whistleblower Protection Agency*

Due to the complex patchwork of existing laws providing varying degrees of whistleblower protections, we advocate for the creation of a single, independent agency that would be solely responsible for overseeing compliance with whistleblowing issues for all organizations. All of the agencies and offices currently responsible for receiving or investigating reports of wrongdoing would be managed by the newly formed agency. Doing so would ensure that those facilitating the whistleblowing process are adhering to best practices and provide potential whistleblowers with a simplified structure to assist in navigating the legal minefield.

V. CONCLUSION

While federal and state whistleblower laws exist, they fall short in protecting the whistleblower. This leaves those who attempt to seek protection under the law worse off as the mere existence of well-intended statutes often lead to a false sense of security in believing that their actions are anonymous. New federal legislation should address these shortcomings by including clear definitions of confidentiality and anonymity, requiring the use of the best available technological protections to facilitate anonymous reporting, increasing financial liabilities for noncompliance by businesses, promoting better corporate policies, and enhancing the availability of punitive damages for whistleblowers suing businesses for both retaliation and for noncompliance with the law for not having anonymous reporting methods available to their employees. It is imperative that laws intended to protect those who reveal wrongdoing be future proof and truly provide meaningful legal protections.