2012

Virtual Whistleblowing

Miriam A. Cherry
Saint Louis University School of Law

Recommended Citation
Cherry, Miriam A., Virtual Whistleblowing. 54 South Texas Law Review 9 (2012); Saint Louis U. Legal Studies Research Paper No. 2013-19.

SOUTH TEXAS LAW REVIEW

VOLUME 54 FALL 2012 NUMBER 1

VIRTUAL WHISTLEBLOWING

MIRIAM A. CHERRY

VIRTUAL WHISTLEBLOWING

MIRIAM A. CHERRY*

I. INTRODUCTION

In approximately 2004, Michael DeKort, a forty-one-year-old Lockheed Martin project manager, became concerned about security flaws in ships his employer was selling to the United States Coast Guard. The new ships were part of a planned $24 billion equipment upgrade that would make the United States Coast Guard a more active part of the war on terror.[1] However, according to DeKort, the

* Professor of Law, Saint Louis University; B.A., 1996, Dartmouth College; J.D., 1999, Harvard Law School. I appreciate the input and comments of Professors Orly Lobel, Marica McCormick, and Paul Secunda. My appreciation to Richard Carlson at the South Texas College of Law for organizing the symposium, as well as my thanks to the other participants. I also wish to thank librarian David Kullman, faculty fellows Ameya Patankar and Myles McCabe, and the editors of the *South Texas Law Review* for their excellent research assistance and hard work.

1. *See* David Axe, *Sunk Costs: Why, After $24 Billion in Upgrades, the Coast Guard Still Deploys a Fleet of Rustbuckets*, WASH. MONTHLY, Nov./Dec. 2008, http://www.washingtonmonthly.com/features/2008/0811.axe.html ("More than a decade ago, the Coast Guard came up with a plan, called Deepwater, to replace aging vessels . . . with new cutters, at a reasonable cost to taxpayers. But in the feverish aftermath of 9/11, with the Bush administration eager to turn all government departments into outposts of the war on terror, the humble Coast Guard attempted a far more ambitious transformation—a $24 billion scheme to transform its boats into an integrated fleet boasting heavy weaponry and futuristic communications systems. When the agency leapt at the opportunity to get its hands on an expanded budget and high-tech ships, however, it

vessels featured security cameras with significant blind spots and communications equipment that was not secure.[2] Further, DeKort alleged that other equipment on board could not operate at the extreme temperatures required by Lockheed's contract with the government.[3] This was an especially serious problem given that the Coast Guard vessels might be deployed anywhere from the heat of the Persian Gulf to the cold of the Antarctic. DeKort claimed that he had alerted the Coast Guard and his supervisors at Lockheed, but that he had been told to keep quiet because the program was behind schedule and over budget.[4] Concerned that critical national security matters were being compromised because of inaction, DeKort uploaded a ten-minute video to the website YouTube in which he catalogued the safety and security problems on the ships.[5]

Reactions to DeKort's video varied. Dina Kaplan, co-founder of Blip.tv, said, "This is an excellent example of the democratization of the media, where everyone has access to the printing press of the 21st century."[6] A spokesman for Lockheed Martin said, "Anybody with a webcam and something to say, regardless of whether it's true or not, can say it on YouTube."[7] Lockheed Martin terminated DeKort's employment just days after the video was released, but claimed the

---

failed to put in place the necessary tools to make sure that such massive contracts would actually deliver what the government ordered. The result has been six years of incompetence and alleged fraud by private contractors and billions of squandered taxpayer money, much of it wasted on flawed boats that have since been scrapped. The Coast Guard, meanwhile, is still attempting to play a growing military role with ships that are old, unreliable, and a hazard to their crews.").

2. Griff Witte, *On YouTube, Charges of Security Flaws*, WASH. POST, Aug. 29, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/08/28/AR2006082801293.html; *see also Coast Guard Delays Cutter over Radios*, WASH. TIMES, Mar. 11, 2008, http://www.washingtontimes.com/news/2008/mar/11/coast-guard-delays-cutter-over-radios/?page=all (documenting concerns about compromise of communications equipment).

3. Witte, *supra* note 2.

4. *Id.*

5. See Michael DeKort, YOUTUBE (Aug. 3, 2006), http://www.youtube.com/watch?v=qd3VV8Za04g, for DeKort's video. When asked by *60 Minutes* reporter Steve Kroft why he had decided to post a video noting the problems with the ships, DeKort responded as follows: "Yes, sir. I—I was trying to be resourceful and keep the issue going." When asked why he did not go to the press, DeKort responded that he had, but that the media did not seem to believe that radios designed for the Coast Guard would not be waterproof. *60 Minutes: The Troubled Waters of "Deepwater"* (CBS television broadcast Aug. 19, 2007), *transcript available at* 2007 WLNR 16167891.

6. Witte, *supra* note 2.

7. *Id.*

move was long planned and not in response to his video.[8] At the date of this Article's publication, DeKort's video has been viewed over 160,000 times. It also attracted the attention of members of Congress, who eventually held a series of hearings seeking explanations and answers.[9]

After being fired by Lockheed Martin, DeKort filed a *qui tam* action under the False Claims Act. DeKort later settled his claims with Lockheed Martin for an unspecified amount. His claims against Integrated Coast Guard Systems continued but were dismissed on summary judgment because the district court ruled that the information provided had already been publicly disclosed through congressional hearings.[10] Although DeKort's decision to whistleblow via YouTube was certainly controversial, in the end, as whistleblowing goes, it could be termed a mixed success. The attention that the video received meant that DeKort's allegations could no longer be ignored, and congressional hearings investigated and substantiated his claims. DeKort apparently received some sort of settlement with Lockheed Martin, and he was recently honored with a public service award presented to him by U.S. Representative Elijah E. Cummings.[11]

In the past, many workers have found themselves in similar situations—confronted with profound ethical, moral, or social dilemmas that pit the citizen's interest against that of his or her employer. Unfortunately, countless employees will find themselves in similar positions in years to come. What makes DeKort's situation novel is the way in which he went about blowing the whistle. By taking his allegations directly to YouTube, he was able to use the Internet to call attention to his claims. And in making those claims public, he was able to establish that the problems he was calling attention to were critical and could not be ignored.

With the advent of YouTube, blogs, social networking, and whistleblower websites such as WikiLeaks, the paradigm of whistleblowing is changing. The new paradigm for "virtual whistleblowing" is increasingly online, networked, and anonymous. While whistleblowing can take place in many contexts, this

8. *See id.*

9. *See, e.g.*, Alicia Mundy, *Coast Guard's Deepwater Program Hits Rough Waters*, SEATTLE TIMES, Mar. 13, 2007, http://seattletimes.com/html/localnews/2003615378_coastguard13m.html.

10. U.S. *ex rel.* DeKort v. Integrated Coast Guard Sys., No. 3:06-CV-1792-O, 2010 WL 4363379, at *5 (N.D. Tex. Oct. 27, 2010), *aff'd*, 475 F. App'x 521 (5th Cir. 2012).

11. *Rep. Cummings Presents Award to Deepwater Whistleblower*, U.S. FED. NEWS, Jan. 28, 2008, at 1, *available at* 2008 WLNR 1654053.

symposium contribution concentrates on the impact of technological changes on employment law whistleblowing. Employee whistleblowing is a particularly important component of whistleblowing overall, as corporations, governments, and other entities can only act by and through their agents.[12] Therefore, agents are an important source of discovering and policing organizational wrongdoing. Further, termination of employment is a common retaliatory gesture, and it is an extremely damaging one, given its impact on a person's psychological and financial well-being. My contention for some time has been that existing regulation has been inadequate to cover existing forms of whistleblowing.[13] Therefore, it is not surprising that existing whistleblowing laws have also failed to keep pace with the changes brought by modern technology. And so, if older laws cannot be made to fit the new paradigm of virtual work, it is necessary to reassess and determine what changes in the law might more appropriately fit these new forms of whistleblowing.

Traditionally, whistleblowing was conceived of as an exception to the employment-at-will rule.[14] Public policy or whistleblowing-type exceptions allowed employees to report illegal activity within an organization or to outside authorities without fear of retaliation.[15] The public policy for protecting whistleblowers, or as Professor Richard Carlson terms them, "citizen employees,"[16] includes protecting the

12. *See* Reid Rd. Mun. Util. Dist. No. 2 v. Speedy Stop Food Stores, Ltd., 337 S.W.3d 846, 853 (Tex. 2011) ("An organization takes action through its agents."); *see generally* RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. (2006) (exploring the general concept of agency and the various types of relationships that may constitute agency relationships).

13. *See* Miriam A. Cherry, *Whistling in the Dark? Corporate Fraud, Whistleblowers, and the Implications of the Sarbanes–Oxley Act for Employment Law*, 79 WASH. L. REV. 1029, 1085 (2004).

14. The at-will rule provides that an employee may be fired for a good reason, a bad reason, or no reason at all. In other words, it provides the employer the discretion to fire without having to explain the reason for letting the employee go. The at-will rule is the law in forty-nine states, with Montana the sole exception. In past decades, there have been increasing incursions to the at-will rule, especially to limit the "bad reasons" that employers may use. Limitations include firing someone for a discriminatory reason or for whistleblowing by reporting wrongdoing. *Id.* at 1042–45.

15. *See id.* at 1042–43.

16. Richard R. Carlson, *Citizen Employees*, 70 LA. L. REV. 237, 237–38 (2009) ("By 'citizen employees,' I mean employees who respond to a sense of public duty even at some cost to their work, professional relations, or their employer's business. Citizen employees are defined by their conduct. They question or resist instructions to commit or assist wrongful activity. When they discover wrongful conduct of fellow employees or managers, they blow the whistle to other responsible managers or outside law enforcement authorities. They serve the public as jurors, witnesses, military reservists, and volunteer emergency responders, despite the competing demands of their employment.").

public from illegal activities that would otherwise occur at work and providing fuller enforcement for the underlying laws against such illegal activity.[17] Despite these important public policies, protection against retaliation has been criticized as both piecemeal and inadequate.[18]

Coverage has been seen as piecemeal because current laws are a patchwork of federal statutes, state statutes, and judicially created exceptions under judicially created public policy exemptions.[19] Some statutes only cover particular types of whistleblowing, and often in ways that are not particularly rational or logical. As I have noted in earlier writing, it is all too easy for an employee's whistleblowing claim to "fall through the cracks."[20] Given that many workers do not understand that their employment is at will, or what the legal consequences of at-will employment are,[21] let alone the nuances and details of what they would need to do in order to claim whistleblower protection, there certainly is a good argument that law reform is needed.

Aside from existing whistleblowing laws' piecemeal nature, others have criticized current law as ineffectual.[22] Studies have shown that whistleblowers often face serious consequences for reporting wrongdoing, even beyond termination of employment (despite the illegality of such actions). Often the whistleblower's decision to report

17. *See, e.g.*, Richard E. Moberly, *Sarbanes–Oxley's Structural Model to Encourage Corporate Whistleblowers*, 2006 BYU L. REV. 1107, 1113, 1117 (2006) (discussing the importance of "rank-and-file" employees disclosing knowledge of wrongdoing within corporation); Carlson, *supra* note 16, at 238.

18. *See* Carlson, *supra* note 16, at 240–41.

19. *See* Cherry, *supra* note 13, at 1085 (advocating a uniform federal and state approach to whistleblower statutes).

20. *Id.*; *see also* Geoffrey Christopher Rapp, *Mutiny by the Bounties? The Attempt to Reform Wall Street by the New Whistleblower Provisions of the Dodd–Frank Act*, 2012 BYU L. REV. 73, 80 (2012) (describing whistleblower protections as "haphazard").

21. *See* Pauline T. Kim, *Bargaining with Imperfect Information: A Study of Worker Perceptions of Legal Protection in an At-Will World*, 83 CORNELL L. REV. 105, 133 (1997) ("The survey data reveal[s] a striking level of misunderstanding among [employee] respondents of the most basic legal rules governing the employment relationship."); Cynthia L. Estlund, *How Wrong Are Employees About Their Rights, and Why Does It Matter?*, 77 N.Y.U. L. REV. 6, 6 (2002) ("Most employees are terminable at will, yet apparently most believe they only can be fired for cause.").

22. *See* Carlson, *supra* note 16, at 243 ("[W]hile the number and variety of laws protecting citizen employees seems impressive, these laws form an incomplete, inconsistent, and unreliable patchwork. There is no master anti-retaliation law of the order of Title VII to fill the gaps, either at the federal level or in any but a few states. A citizen employee's protection against retaliation and interference depends as much on the luck of geography, occupation, and the law the employer violated as on the merits of the employee's conduct or the value of his action to the community.").

results in ruined career expectations, depression, and even the breakdown of personal friendships and other intimate relationships.[23] In the realm of virtual work, whistleblowers facing these potentially harsh consequences may quite sensibly wish to avoid making a complaint through official channels. Instead of engaging in reporting in traditional ways where they might expose themselves to retaliation, in the future whistleblowers may seek alternate forms of communication to spread the word about law-breaking or other improper activity at work. Some of these methods of communication are enabled by new technologies—like YouTube—that have gained in popularity in recent years.

This piece explores virtual whistleblowing in four parts. First, how is work changing? Who are virtual workers, and what types of work are they performing? Why do virtual workers need whistleblowing protections? What special types of protections might virtual workers need specific to their changed working conditions? Second, even workers employed in traditional workplaces may have a need for additional protections, because—just like Michael DeKort used YouTube—traditional workers may want to use online forms of communication in order to blow the whistle. In this section, I discuss "whistleblogging," where employees use blogs to blow the whistle—and often find themselves "dooced," i.e., fired for blogging. In the third section, I examine the controversial website WikiLeaks. Embroiled in controversy, WikiLeaks involves other issues—such as national security—but also involves employment, as employees of private corporations or the government have provided sensitive information to WikiLeaks. Finally, in the last section, I discuss possible legal alternatives for these new forms of online and virtual whistleblowing. In addition, here I take up Professor Richard Carlson's call for a uniform law that would protect citizen employees, so that workers clearly understand their rights when engaging in protected activity.

23. *See* Cherry, *supra* note 13, at 1053 ("According to a study of eighty-four whistleblowers conducted in the early 1990s, '82% experienced harassment after blowing the whistle, 60% were fired, 17% lost their homes, and 10% admitted to attempted suicide.' Due to the extreme stress, many whistleblowers develop serious mental illness, such as depression, which can lead to other problems, such as alcohol or drug abuse." (quoting David Culp, *Whistleblowers: Corporate Anarchists or Heroes? Towards a Judicial Perspective*, 13 HOFSTRA LAB. & EMP. L.J. 109, 113 (1995))).

II. THE CHANGING PARADIGM: VIRTUAL WORK AND VIRTUAL WORKERS

In my earlier writing, I have noted that there are currently thousands of workers who spend the bulk of their days working in cyberspace in one form or another.[24] These workers have sometimes been referred to as "clickworkers," "cyberworkers," or "cloudworkers,"[25] although I have used "virtual workers" as a more general term. While virtual workers have different skills and labor under different conditions, their commonality is that their "workplaces" exist only in the ether. As more work enters cyberspace and virtual worlds, this will have a profound impact on the nature of work itself, not to mention the legal doctrines of labor and employment law. Today, millions of people worldwide entertain themselves or supplement their incomes—or both—by working within virtual worlds such as Second Life or casually "clicking" to make a few dollars for simple tasks on websites like Amazon.com's Mechanical Turk.[26] From telecommuting "work at home" arrangements,[27] to virtual meetings where employees from five different countries "gather" through avatars in Second Life, to workers answering calls directed to them on their cellphones as part of a crowdsourcing effort,[28] "virtual work" is becoming increasingly commonplace.[29]

There are new forms of work in virtual worlds, including "custom avatar designers, party and wedding planners, casino operators, nightclub owner[s], car manufacturers, fashion designers, freelance scripters, [and] game developers."[30] While these forms of work are

24. Miriam A. Cherry, *A Taxonomy of Virtual Work*, 45 GA. L. REV. 951, 954 (2011).

25. Other terms that have appeared in the news media include "labor as a service" and "human computing."

26. *See* Gabrielle Monaghan, *A Virtual Way to Find Real Talent*, SUNDAY TIMES (London), Mar. 16, 2008, at 19 (discussing the increase in virtual hiring amongst companies worldwide); *see also* EDWARD CASTRONOVA, SYNTHETIC WORLDS: THE BUSINESS AND CULTURE OF ONLINE GAMES 2 (2005) (discussing the amount of people who could be said to "live" in online gaming worlds).

27. *See* Kevin Courtney, *Con Text M-Worker*, IRISH TIMES, Apr. 1, 2008, at 17, *available at* 2008 WLNR 6100967.

28. *See* LIVEOPS, www.liveops.com (last visited Oct. 30, 2012) (example of crowdsourcing technology).

29. *See* Steve Lohr, *Hello India? I Need Help With My Math*, N.Y. TIMES, Oct. 31, 2007, http://www.nytimes.com/2007/10/31/business/worldbusiness/31butler.html?pagewanted=all (discussing the increase in virtual personal services companies).

30. Cherry, *supra* note 24, at 965 (quoting Monaghan, *supra* note 26, at 19); *see also* Cory Ondrejka, *Escaping the Gilded Cage: User Created Content and Building the*

new, other more "traditional" forms of work can also be conducted in a virtual setting. These include traditional service or counseling work, which are essentially equivalent to those positions in the real world. For example, during tax season, one can receive tax advice in the virtual world in the same way as if one were to use a traditional medium, such as visiting an accountant or tax preparer's office or talking to a tax professional on the telephone.[31] The only difference is that the consultation and "meeting" occurs in the virtual environment. Attorneys are beginning to establish virtual offices in Second Life, but so far the model seems to be to use Second Life to meet clients and then to take the clients into the "real world."[32] It is not so much that Second Life specifically changes these "old economy" service occupations. Rather, it may just make the work more efficient, obviate the need for in-person consultations or conferences, and provide an additional way to stay connected, especially if clients are geographically far from service providers.

While crowdsourcing does not take place in a virtual world, it is a new form of work that utilizes Web 2.0 technology and is rapidly growing in importance.[33] In crowdsourcing, computers automate and break down tasks and then the work for which humans are needed is sourced out to them. The work is matched with thousands of computer workers who perform tasks. After each worker performs a small piece of work, that bit of work is then integrated back into a larger project. Since I began writing about this topic several years ago, the number of crowdsourcing websites has multiplied.[34]

Metaverse, 49 N.Y. L. SCH. L. REV. 81, 94 (2004) (explaining that Second Life users "have become entrepreneurs, [are] opening stores, bars, and strip clubs, and searching out creators to provide goods and services for them"); Shannon L. Thompson, *Securities Regulation in a Virtual World*, 16 UCLA ENT. L. REV. 89, 93-94 (2009) (noting careers such as "resort owner, detective, and virtual furniture store owner").

31. Indeed, the author visited Second Life during tax season and found that tax preparation services were available there, just as they would be in the real world.

32. *See, e.g.*, Monaghan, *supra* note 26, at 19 (describing an attorney who used Second Life to find clients and within two weeks had made $7,000); Attila Berry, *Lawyers Find Real Revenue in Virtual World*, LAW TECH. NEWS (July 31, 2007), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=900005487405&slreturn=20120931170101 (describing a law firm that brought in $20,000 in revenue in its first year from its Second Life office).

33. Randall Stross, *When the Assembly Line Moves Online*, N.Y. TIMES, Oct. 30, 2010, http://www.nytimes.com/2010/10/31/business/31digi.html; *see also* Jonathan Zittrain, *Ubiquitous Human Computing* 2 (Univ. of Oxford Legal Research Paper Series, Paper No. 32, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1140445.

34. Cherry, *supra* note 24, app. A (providing appendix listing websites for crowdsourcing).

In a previous article, I described an effort to go undercover in Second Life in order to find a "virtual job" and in the process to discover more about the work opportunities offered on Second Life.[35] At that time, I noted that the difficulties a job seeker encounters in Second Life mirrored those in the real world but were compounded by the need to orient oneself to the new virtual environment.[36] The ubiquitous evils of the Internet—spam and pornography—made finding work even more difficult.[37] In that same article, I documented how my efforts as well as those of my research assistant to earn minimum wage on crowdsourcing websites were met with failure. Try as we could, we were unable to complete enough piecework to make the hourly federal minimum wage.[38] I ended that article with some thoughts about how to handle virtual piecework, the distinctions between work and leisure, and the importance of a living wage for virtual workers.[39]

In fact, virtual workers may find themselves in possession of the same kind of information that causes employees at "brick-and-mortar" workplaces to blow the whistle—proof of financial fraud or other illegal activity, for example. But virtual workers may also face their own set of unique issues that arise from the particularized circumstances of their own online employment environment. So, for example, virtual workers may have more reason to report violations of wage and hour laws. Perhaps, because of the prevalence of pornography on the Internet and the potential for interaction with random strangers, there could also be more reason for workers to report sexual harassment. Our existing employment laws may benefit from a revision to reflect the changing online environment and new forms of virtual work. But, virtual whistleblowing is not just a concept for the virtual worker; another facet encompasses workers in traditional industries and workplaces who use technology to accomplish their whistleblowing.

35. Miriam A. Cherry, *Working for (Virtually) Minimum Wage: Applying the Fair Labor Standards Act in Cyberspace*, 60 ALA. L. REV. 1077, 1085–88 (2009); *see also* Interview with Joshua Smith, Research Assistant, in Sacramento, Cal. (July 24, 2008) (on file with author).

36. Cherry, *supra* note 35, at 1086 (describing the challenges of learning to use Second Life).

37. *Id.* at 1086–87.

38. *See id.* at 1086–88.

39. *Id.* at 1109–10.

III. ONLINE WHISTLEBLOWING

As noted in discussing Michael DeKort's case, whistleblowing is changing even for those workers who are employed in traditional brick-and-mortar workplaces. Even those in traditional occupations are using new methods of communicating information, some of which could also be new methods for blowing the whistle. The number of people who use online weblogs ("blogs") is constantly growing. In 2007, by one estimate, 22.6 million Americans maintained a personal blog,[40] and 5% of American workers maintained a personal blog.[41] The rapid expansion of blogging means that an individual can easily and rapidly communicate their thoughts into the blogosphere. There is currently a thriving discussion about the propriety of employees blogging[42] and more specifically, about employees blogging about work.[43] Some of this discussion is quite controversial.

Whistleblowing, blogging, and the intersection of the two—what has become known on the Internet as "whistleblogging"—have created legal issues that are difficult to address under the existing legal framework. There are a number of bloggers who have been fired because of commentary on blogs that they hosted and wrote during their free time.[44] Some of this commentary involved negative statements about supervisors or coworkers at work that could be considered insubordinate or otherwise disruptive. However, other times, the blogs in question were more concerned with personal topics that seemingly had little to do with work.[45] In fact, being fired for blogging has even been given its own unique name, "dooced."[46] Other

---

40. Paul M. Secunda, *Blogging While (Publicly) Employed: Some First Amendment Implications*, 47 U. LOUISVILLE L. REV. 679, 681 n.12 (2009).

41. Robert Sprague, *Fired for Blogging: Are There Legal Protections for Employees Who Blog?*, 9 U. PA. J. LAB. & EMP. L. 355, 356 (2007).

42. "Blog" is short for "web log." A blog is like a digitally maintained newspaper, except that it is more dynamic because readers can leave comments for the authors, and most authors of blogs welcome the opportunity for feedback from their audience. *See, e.g.*, Paul S. Gutman, Note, *Say What?: Blogging and Employment Law in Conflict*, 27 COLUM. J.L. & ARTS 145, 145–47 (2003) (discussing the basics of blogging).

43. *See, e.g.*, *Blogging About Work*, WORKPLACE PROF BLOG (May 19, 2005), http://lawprofessors.typepad.com/laborprof_blog/2005/05/blogging_about_.html (discussing a Los Alamos National Lab employee who was reprimanded for blogging about his job).

44. *See* Sprague, *supra* note 41, at 355, 385–87 (concluding that although bloggers may have some legal protections, the at-will doctrine, combined with statutory and constitutional limitations on potential causes of action, means that employees should blog with caution).

45. *See id.* at 356–59.

46. The term *dooced* comes from one worker's experience: Heather B. Armstrong used the term to describe being fired from her job as a web designer due to comments she

workers have blogged about their experiences after quitting their jobs or being fired. For example, twenty-two former employees of a trendy restaurant in Brooklyn, New York, took to blogging in order to publicize the sexual harassment they claimed they had suffered by the chef–owner.[47] Only some state whistleblower laws protect employees who approach the media with their claims,[48] and no state whistleblower laws protect bloggers (yet). What protections these whistlebloggers enjoy under other laws is the subject of much debate.

In two recent articles, Professors Robert Sprague and Paul Secunda discussed this phenomenon of "fired while blogging" or being dooced. Professor Sprague concentrates on the private sector while Professor Secunda turns his analysis to the public sector. Employers are concerned, and I think rightly, that employee bloggers may reveal confidential information, threaten, harass or intimidate coworkers, or otherwise engage in disloyal or insubordinate expression.[49] Despite the seriousness of the employer interests at stake, a recent estimate was that only eight percent of companies have a written policy supplying guidelines on what workplace material is acceptable for an employee to write about in a personal blog.[50] In my experiences working at three different law schools and blogging, there have not been any blogging policies in place.[51] Ambiguities and lack of clear guidance regarding employee blogging have divided jurisdictions and led to differing liabilities between groups.

As of this writing, research revealed no states that specifically provide for protections for weblogs or employee bloggers. As blogging becomes more commonplace and accepted, it is possible that the Internet will become a preferred venue for whistleblowing. With particularly sensitive information, some authors may choose

---

wrote about her work on her weblog. *Dooce* was the name of Armstrong's blog, and comes from her misspelling of the word *dude*. *FAQ*, DOOCE, http://www.dooce.com/faq (last visited Nov. 1, 2012).

47. See *The Full Story*, JUVENTINO INQUIRIES, http://juventinodisclosed.wordpress.com/the-full-story (last visited Nov. 1, 2012), for the former employees' blog and story.

48. *See* Cherry, *supra* note 13, apps. A & B (containing a survey of coverage of various state and federal whistleblower protections).

49. *See* Secunda, *supra* note 40, at 682 n.13.

50. Amy Joyce, *Blogged Out of a Job*, WASH. POST, Feb. 19, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/02/18/AR2006021800131.html (citing a July 2006 survey of the Society for Human Resource Management).

51. See generally Christine Hurt & Tung Yin, *Blogging While Untenured and Other Extreme Sports*, 84 WASH. U. L. REV. 1235 (2006), for a discussion about the risks and benefits of blogging as a pretenured professor.

anonymity.[52] Others may want to be more public with their whistleblowing, hoping that the open nature of the Internet will protect them from retaliation rather than relying on legal doctrines to provide that safety net. Whether such activity is protected whistleblowing activity depends on applicable state law.[53] Some states require whistleblowers to exhaust remedies within their companies before reporting the wrongdoing to external sources.[54] Other states have no such obligations, and whistleblowers effectively can gain the protection of the statute by approaching the press directly.[55] Although blogging is not the traditional form of "the media," one assumes that posting the information on the Internet would be treated the same way for purposes of whistleblowing statutes.

Other more-general public policies or statutes may come to bear. However, their roles are somewhat complicated by whether the activity in question is protected by an off-duty conduct statute, whether it is subject to federal laws (like the Stored Communications Act), whether the blogger is the original source of the information, and whether the blogger is a public sector employee.[56] Professor Sprague notes that many states have passed laws protecting activity that an employee conducts during his or her off-duty hours.[57] California Labor Code § 96(k) prohibits adverse employment action for any lawful conduct occurring during nonworking hours away from the employer's premises.[58] According to Professor Sprague, other such "off-duty" statutes may protect employee bloggers.[59] Professor Michael Selmi has made similar points about the need to protect off-

52. *See* Sunny Woan, *The Blogosphere: Past, Present and Future. Preserving the Unfettered Development of Alternative Journalism*, 44 CAL. W. L. REV. 477, 493–95, 502–03 (2008); *see also* Henry Hoang Pham, Note, *Bloggers and the Workplace: The Search for a Legal Solution to the Conflict Between Employee Blogging and Employers*, 26 LOY. L.A. ENT. L. REV. 207, 214, 219–20 (2005) (discussing blogger right to anonymity).

53. *See* Cherry, *supra* note 13, at 1046–47 & app. A ("The state whistleblowing statutes also differ in the type of disclosure they protect, the manner of disclosure they require, and the remedies they provide.").

54. *Id.*

55. *Id.*

56. For example, Connecticut codified protection for employees against wrongful discharge relating to their exercise of First Amendment free speech rights. Sprague, *supra* note 41, at 378 (citing CONN. GEN. STAT. ANN. § 31-51q (West 2003)).

57. *Id.* at 376.

58. *See* CAL. LAB. CODE § 96(k) (West 2011). Colorado, New York, and North Dakota have similar statutes. *See* COLO. REV. STAT. ANN. § 24-34-402.5(1) (West 2008); N.Y. LAB. LAW § 201-d(2) (McKinney 2009); N.D. CENT. CODE § 14-02.4-03 (2009).

59. Sprague, *supra* note 41, at 376.

duty employee conduct and expression.[60] If employee blog posts relate to unionization or the mutual aid of other employees, such communication could gain protection under the federal labor laws.[61] However, some courts have ruled that if an employee uses their employer's equipment to communicate, they forgo any expectation of privacy in their communications.[62]

There are additional limitations on employers. Some blogs are configured so only those who have been granted specific access are allowed to read the blog. As noted by Professor Sprague, employers may "face liability for violation of the federal Stored Communications Act ('SCA') for improperly accessing a private blog."[63] For example, in *Konop v. Hawaiian Airlines, Inc.*, an airline employee's private blog was accessed by his employer, who obtained the password from another employee.[64] The Ninth Circuit held that a non-"user" manager accessing a restricted employee blog violates the SCA.[65] Alternatively, if an authorized user accesses the blog and forwards the contents to the employer, the blogger will have no protection.[66]

Another challenge facing virtual whistleblowers is establishing that they were the original source of the information that resulted in

60. Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035, 1037 (2006) ("Not only has the power of employers expanded but the reach of the workplace has likewise been extended into what used to be considered private domains. Although many recoiled at the notion (and still do so today), at one time, the slogan 'work is for working' reasonably captured the essence of the employment relationship. When one was at work, she worked, but after work was, well, after work. Today, that is no longer true as what is sometimes called the boundaryless workplace now entraps employees far from the confines of the workplace and with virtually no compensating benefits."); *see generally* Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship*, 50 U. LOUISVILLE L. REV. 1 (2011); Marisa Anne Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625 (2004).

61. *See* NLRB v. Unbelievable, Inc., 71 F.3d 1434, 1438 (9th Cir. 1995) (upholding a finding of unfair labor practices when an employer eavesdropped on a private conversation between employees and a union representative and subsequently expelled the representative).

62. *Legal Guide for Bloggers*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/bloggers/legal/labor (last visited Oct. 16, 2012) (citing Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

63. Sprague, *supra* note 41, at 363 (footnote omitted).

64. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872–73 (9th Cir. 2002).

65. *Id.* at 879–80.

66. *Id.* at 880. But in an analogous case to the *Konop* scenario, the New Hampshire Supreme Court allowed a plaintiff employee's claims for wiretapping, eavesdropping, and wrongful discharge where the plaintiff's constructive termination resulted from an intercepted private phone conversation that was reported to the plaintiff's employer. *See* Karch v. Baybank FSB, 794 A.2d 763, 768–73, 776 (N.H. 2002).

their termination. Michelle Sherman writes that the Internet makes it more difficult for anyone to be the "first" source of information, which is critical to establishing a whistleblower defense.[67] Thus, employers "should exhaustively search the Internet for evidence" of prior information when defending against whistleblower claims.[68] In the aftermath of the financial crisis, the Dodd–Frank Act (DFA) established additional bounties for those blowing the whistle on accounting fraud at publicly traded companies.[69] Additionally, since the DFA's bounty provision also requires information to be "original,"[70] it is possible that dissemination on Internet blogs might void the information's claim to originality. The issue is presently unlitigated.

Public employees, Professor Secunda notes, have a stronger case because any adverse employment decision involves state action; public employees receive First Amendment protections.[71] To prevail in a First Amendment claim against a public employer, employees must prove that 1) they spoke as a citizen on a matter of public concern, 2) their interest in speaking outweighs their employer's interest in the efficient provision of government services,[72] and 3) their speech was a substantial or motivating factor in their dismissal.[73] That said, the personal nature of many blog posts means they will not qualify as speech as a matter of public concern.[74] Further, if employees are speaking as part of their official duties, they enjoy no First Amendment protection.[75] For example, in *Richerson v. Beckon*,[76] a public employee blogged criticisms about trainees under her supervision and called her union's chief negotiator a "Nazi."[77] The court upheld the employer's decision to transfer the

67. Michelle Sherman, *Using the Internet to Your Company's Advantage in Defending Against a Whistleblower Action*, 15 NO. 8 J. INTERNET L. 3, 3 (2012).

68. *Id.*

69. *See, e.g.*, Rapp, *supra* note 20, at 74–75.

70. Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, 1740–41 (2010).

71. *See* Secunda, *supra* note 40, at 683 (discussing limited First Amendment protection for private employees).

72. *Id.* at 686, 688.

73. *Id.* at 692.

74. *Id.* at 690–91.

75. Garcetti v. Ceballos, 547 U.S. 410, 426 (2006) ("We reject, however, the notion that the First Amendment shields from discipline the expressions employees make pursuant to their professional duties.").

76. Richerson v. Beckon, 337 F. App'x 637, 638 (9th Cir. 2009); Secunda, *supra* note 40, at 690.

77. *Richerson*, 337 F. App'x at 638.

employee involuntarily because her speech caused a substantial disruption of the workplace environment.[78] However, in some situations, public employees may not have the right to access blogs at work. For example, in *Nickolas v. Fletcher*,[79] the state of Kentucky prohibited employees from accessing blogs on state-owned computers.[80] A district court ruled against the employees because the ban was viewpoint-neutral, and there was objective evidence that state employees were wasting time on Internet blogs.[81]

If this situation were not complicated enough, other legal issues have arisen around aspects of liability for anonymous blogging and for hosting services. If a blogger writes anonymously, the employer or aggrieved party is not without recourse. The aggrieved party may file a "Doe" lawsuit with an unnamed defendant or defendants.[82] Then, the plaintiff serves the defendant's Internet service provider (ISP) with a subpoena to obtain the poster's identity.[83] The defendant is typically alerted by the ISP and is then able to file an action or motion to quash the subpoena without revealing their identity.[84] When and if the identity is obtained, the plaintiff can amend the pleadings to name the disclosed defendant.[85] When an employer's confidential information is posted online, the website hosting the blog (such as Google or Wordpress) will not generally face liability. The Communications Decency Act[86] provides that "[n]o provider or user of an interactive computer service shall be treated as [a] publisher or speaker of any information provided by another information content provider."[87] Thus, content posted on a website, even if reposted, is "information provided by another information content provider" and the host website will have no liability.[88]

78. *Id.* at 638–39; *see also* Secunda, *supra* note 40, at 689–90.
79. Nickolas v. Fletcher, No. 3:06-CV-00043, 2007 WL 1035012, at *1 (E.D. Ky. Mar. 30, 2007).
80. *Id.*; Secunda, *supra* note 40, at 693.
81. *Nickolas*, 2007 WL 1035012 at *9; Secunda, *supra* note 40, at 694–95.
82. Robert D. Brownstone, *Identified Plaintiff Seeking Disclosure of Anonymous Defendant—Various Contexts*, *in* 1 DATA SECURITY & PRIVACY LAW § 9:132 (Ronald N. Weikers ed., 2012).
83. *Id.*
84. *Id.*
85. *Id.*
86. 47 U.S.C. § 230 (2006).
87. Shiamili v. Real Estate Group of N.Y., Inc., 952 N.E.2d 1011, 1015 (N.Y. 2011) (first alteration in original) (quoting 47 U.S.C. § 230(c)(1)).
88. *See id.* at 1020.

IV. THE STORY OF WIKILEAKS

To this point, this Article has discussed situations where employees might whistleblog, but publication on a personal blog is not the only way to publicize wrongdoing. Employees might also choose to provide information to a third party and then have that information publicized while remaining anonymous. Traditionally, journalists and print publications took information from anonymous sources, gave it to editors for review, and then printed the information.[89] As the process of whistleblowing becomes virtual, no organization is more notorious or controversial than the website WikiLeaks.[90] We have now moved from a paradigm where Daniel Ellsberg distributes photocopies of the Pentagon Papers to major national media outlets to one in which Julian Assange[91] posts thousands of pages of raw intelligence reports on his WikiLeaks website, doing an end-run around the mainstream press.[92] In both situations, the "conflict between providing truthful, but damaging, information about the government and its military operations, and providing the [public] with the information necessary to hold government accountable" remains identical.[93]

---

89. *See* Mary-Rose Papandrea, *The Publication of National Security Information in the Digital Age*, 5 J. NAT'L SECURITY L. & POL'Y 119, 121 (2011); *see also* Mary-Rose Papandrea, *Laptops, Watchdogs, and Scapegoats: The Press and National Security Information*, 83 IND. L. J. 233, 258–62 (2008) (describing the history of the relationship between leakers of national security information and mainstream press).

90. *See, e.g.*, Geoffrey R. Stone, *WikiLeaks, the Proposed SHIELD Act, and the First Amendment*, 5 J. NAT'L SECURITY L. & POL'Y 105, 105 (2011) (describing furor in U.S. Congress over the WikiLeaks website).

91. Julian Assange founded WikiLeaks, and he still leads the site today amongst a great deal of controversy. Assange has been under house-arrest in the UK, pending extradition to Sweden to face sexual assault allegations. On June 20, 2012, he fled to the Ecuadorian embassy in London and requested political asylum in Ecuador. Paul Sonne & Alice Speri, *Police Say Assange Has Violated Bail*, WALL ST. J., June 20, 2012, http://online.wsj.com/article/SB10001424052702304898704577478050655723724.html; *see also* John F. Burns & Ravi Somaiya, *WikiLeaks Founder on the Run, Trailed by Notoriety*, N.Y. TIMES, Oct. 23, 2010, http://www.nytimes.com/2010/10/24/world/24assange.html?pagewanted=all.

92. For more on the comparison between WikiLeaks and the Pentagon Papers case, see generally Jerome A. Barron, *The* Pentagon Papers *Case and the WikiLeaks Controversy: National Security and the First Amendment*, 1 WAKE FOREST J. L. & POL'Y 49 (2011); Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448 (2012); and Heidi Kitrosser, *What if Daniel Ellsberg Hadn't Bothered?*, 45 IND. L. REV. 89, 116-17 (2011).

93. Ronald J. Krotoszynski, Jr., Cyberspace and the First Amendment: Avoiding the Pitfalls Associated with the "Law of the Horse" 7 (July 28, 2012) (unpublished draft) (on file with author); *see also* Sandra Davidson, *Leaks, Leakers, and Journalists: Adding Historical Context to the Age of WikiLeaks*, 34 HASTINGS COMM. & ENT. L.J. 27 (2011)

According to its website, WikiLeaks is a nonprofit media organization.[94] The website's goal is to bring important news to the public by providing "innovative, secure, and anonymous" ways for sources to leak information electronically.[95] The leaked information is then published in its entirety after being verified.[96] Since its first leak in 2006, WikiLeaks claims to have "released more classified intelligence documents than the rest of the world press combined."[97] Those leaks have made WikiLeaks powerful enemies. A U.S. Army report[98] determined that WikiLeaks represented "a potential force protection [and] counterintelligence . . . threat to the U.S. Army."[99] WikiLeaks has released classified U.S. Army documents detailing procedures at Guantanamo Bay, information on military equipment, units, operations, and "nearly the entire order of battle" for American forces in Iraq and Afghanistan.[100] True to its mission, only two of WikiLeaks's sources have ever been publicly identified. Because both sources leaked information obtained during the course of their employment, I discuss these two situations briefly to provide a flavor of this type of virtual whistleblowing.

A. WikiLeaks and Tax Evasion

Rudolf Elmer was an accountant and former Senior Vice-President of the Cayman Islands operations of Julius Baer, a Swiss bank.[101] In that capacity, Elmer claims he witnessed rampant bank-assisted tax evasion by Julius Baer clients.[102] Elmer alleged that billions of dollars in taxes were evaded by routing money through

(exploring the question of weighing the value of openness against government claims of national security).

94. *What Is Wikileaks?*, WIKILEAKS, http://wikileaks.org/About.html (last visited Jun. 21, 2012).

95. *Id.*

96. *Id.*

97. *Id.*

98. Ironically, the U.S. Army report was leaked to WikiLeaks and published.

99. Stephanie Strom, *Pentagon Sees a Threat from Online Muckrakers*, N.Y. TIMES, Mar. 17, 2010, http://www.nytimes.com/2010/03/18/us/18wiki.html (quoting U.S. Army report).

100. *Id.* (noting the U.S. Army report speculated WikiLeaks may be funded by the Central Intelligence Agency).

101. Ralph Pöhner, *Die Stimmen Von Innen [The Voices from Within]*, ZEIT ONLINE (Aug. 1, 2010), http://www.zeit.de/2010/02/CH-Banken/seite-1 (Ger.).

102. *See* Lynnley Browning, *Swiss Banker Blows Whistle on Tax Evasion*, N.Y. TIMES, Jan. 18, 2010, http://www.nytimes.com/2010/01/19/business/19whistle.html?_r=1 ("Mr. Elmer . . . moved to Mauritius in the Indian Ocean and began parceling out to global tax authorities what he said were the secrets of his former employer.").

offshore havens in the Caribbean.[103] Julius Baer dismissed Elmer in December 2002 for "doubts as to his discretion" after taking a lie detector test at his employer's request.[104] After his termination, Elmer copied numerous bank documents and began pressuring Julius Baer to investigate his allegations of tax evasion. In 2005, Elmer was arrested and detained for thirty days for allegedly violating Swiss bank secrecy laws, falsifying documents, and threatening Julius Baer employees.[105]

In 2008, feeling that his internal complaints as well as his complaints to the Swiss government were being ignored,[106] Elmer gave WikiLeaks a list of fifteen Julius Baer clients and at least some of their banking information.[107] After the client list's appearance on WikiLeaks, the leak attracted the attention of the IRS, and in 2009, Elmer gave U.S. authorities thousands of pages detailing names and transactions of hundreds of companies, individuals, and trusts in accounts located in the Cayman Islands.[108] The documents allegedly included "legal tax avoidance structures [and] [o]ther files . . . alleged to point to potential illegal tax evasion by individuals around the globe."[109] Julius Baer denies Elmer's accusations and maintains that after being passed over for a promotion in 2002, Elmer stole internal documents.[110] Julius Baer claims Elmer used altered and forged documents to engage in a campaign to threaten and discredit the bank and its clients after they refused to provide him with a financial settlement.[111]

In January 2011, Elmer flew to London and held a press conference in which he gave WikiLeaks founder Julian Assange two

---

103. *Id.*

104. *See* Pöhner, *supra* note 101.

105. Ashley Fantz, *Who Is Rudolf Elmer, WikiLeaks' Newest Leaker?*, CNN: THIS JUST IN (Jan. 17, 2011, 11:19 AM), http://news.blogs.cnn.com/2011/01/17/who-is-rudolf-elmer-WikiLeaks-newest-leaker/.

106. *See id.*

107. Ed Vulliamy, *Swiss Whistleblower Rudolf Elmer Plans to Hand over Offshore Banking Secrets of the Rich and Famous to WikiLeaks*, GUARDIAN, Jan. 15, 2011, http://www.guardian.co.uk/media/2011/jan/16/swiss-whistleblower-rudolf-elmer-banks.

108. *Isles of Plenty*, GUARDIAN, Feb. 12, 2009, http://www.guardian.co.uk/business/2009/feb/13/tax-gap-cayman-islands ("The whistleblower's documents have been seen by the Guardian. They record the names and transactions of hundreds of companies, trusts, funds and wealthy individuals.").

109. *Id.*

110. *See Former Swiss Banker Is Arrested in WikiLeaks Case, After a Conviction*, N.Y. TIMES, Jan. 20, 2011, http://www.nytimes.com/2011/01/20/business/global/20baer.html.

111. *See Isles of Plenty*, *supra* note 108 (discussing forged documents); *see also Former Swiss Banker is Arrested in WikiLeaks Case, After a Conviction*, *supra* note 110.

discs containing the names of individuals and companies allegedly involved in tax evasion.[112] It is unclear whether this is the same data turned over to U.S. authorities or new data. A few days later—only hours after being convicted by a Swiss court of violating bank secrecy laws—Elmer was rearrested for violating those same laws with his latest leak.[113]

B. WikiLeaks and National Security

The other known "wikileaker" is U.S. Army intelligence analyst Bradley Manning.[114] Transition to Army life was difficult for Manning, and in August 2009, he was referred to mental health counseling by his supervisor.[115] After deploying to Baghdad, Iraq, in late 2009, Manning confided to a friend that he had received sensitive information that he was considering passing along to WikiLeaks.[116] In February 2010, WikiLeaks began posting leaks from inside the U.S. government.[117] In April 2010, WikiLeaks published a 2007 video shot from a U.S. helicopter over Baghdad.[118] According to the Washington Post:

> The action is viewed through the crosshairs of an Apache gunship, as unseen shooters take aim at suspected insurgents, saying, "Light 'em all up. Come on, fire!" The gunfire killed about a dozen people, including two Reuters employees—a driver and a photographer, whose lens had been mistaken for a weapon.[119]

In May 2010, an Army psychiatrist recommended Manning's discharge for psychological reasons.[120] Shortly thereafter, Manning allegedly contacted Adrian Lamo, a well-known hacker from

---

112. *See Business This Week*, ECONOMIST, Jan. 28, 2011, at 98, *available at* 2011 WLNR 1306399.

113. *Swiss Banker Elmer Re-Arrested over WikiLeaks Charges*, BBC NEWS (Jan. 19, 2011), http://www.bbc.co.uk/news/business-12234139.

114. *See, e.g.*, Wendy J. Keefer, *Protection of Information to Preserve National Security: Is WikiLeaks Really the Issue?*, 5 CHARLESTON L. REV. 457, 458 (2011); Ellen Nakashima, *Bradley Manning Is at the Center of the WikiLeaks Controversy. But Who Is He?*, WASH. POST, May 4, 2011, http://www.washingtonpost.com/lifestyle/magazine/who-is-wikileaks-suspect-bradley-manning/2011/04/16/AFMwBmrF_story.html.

115. Nakashima, *supra* note 114.

116. *Id.*

117. *Id.*

118. Jesselyn Radack & Kathleen McClellan, *The Criminalization of Whistleblowing*, 2 AM. U. LAB. & EMP. L.F. 57, 68 (2011).

119. Nakashima, *supra* note 114.

120. *Id.*

California.[121] Through a combination of his own technical expertise and the government's sloppy security procedures, Manning allegedly gained access to much of the field network.[122] He allegedly revealed that upon learning fifteen Iraqi dissidents had been arrested on trumped-up charges, he notified his commander and was told to "shut up" and to assist Iraqi police in finding more detainees.[123] Shortly thereafter, Lamo notified authorities and turned Manning in.[124] Manning was arrested on May 29, 2010, and was transferred back to the United States.[125] While in prison, the U.N. special rapporteur on torture asked on several occasions to see Manning without being monitored, but those requests were denied.[126] Manning has been declared competent for court-martial, but has not entered a plea.[127] He is accused of giving WikiLeaks hundreds of thousands of classified State Department cables, daily field reports from Iraq and Afghanistan, and other classified material.[128] He faces twenty-two charges and could be sentenced to life in prison.[129]

One of the questions that I believe it is important to ask is whether Manning would be facing the same charges had he leaked the documents to the New York Times instead of WikiLeaks. Will the proceedings really be proceedings against Manning, or will they in reality be a trial against WikiLeaks itself?

These two examples from WikiLeaks may seem extreme, but a whistleblowing case may involve sensitive situations. The WikiLeaks examples force us to confront the difficult and sensitive issues surrounding virtual whistleblowing. If whistleblogging and WikiLeaks are creating new legal issues, where might future legal issues arise? And might other websites, instead of creating legal issues, use technology to help solve them?

---

121. Elisabeth Bumiller, *Army Leak Suspect Is Turned In, by Ex-Hacker*, N.Y. TIMES, June 7, 2010, http://www.nytimes.com/2010/06/08/world/08leaks.html.

122. *See* Nakashima, *supra* note 114.

123. *Id.*

124. Bumiller, *supra* note 121.

125. Nakashima, *supra* note 114.

126. Ed Pilkington, *Bradley Manning's Treatment Was Cruel and Inhuman, UN Torture Chief Rules*, GUARDIAN, Mar. 12, 2012, http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un.

127. Nakashima, *supra* note 114; Julie Tate, *Bradley Manning Declines to Enter Plea at Court-Martial*, WASH. POST, Feb. 23, 2012, http://www.washingtonpost.com/world/national-security/bradley-manning-declines-to-enter-plea-at-court-martial/2012/02/23/gIQAhLF6VR_story.html.

128. Tate, *supra* note 127.

129. *Id.*

V. SOLUTIONS

A. *Technological Solutions: Glass Door*

Just as the landscape of whistleblowing doctrine must change in response to technology, so too must the tools for sorting, assessing, and remedying any such claims of wrongdoing. If so much information is being published on the Internet—in many cases anonymously—there is certainly the possibility for false claims. Disgruntled or unhappy employees with an ax to grind against a former employer may provide wildly inaccurate information. Business competitors could even jump on the bandwagon, hoping to denigrate a brand's reputation, manipulate stock, or otherwise wreak havoc against those perceived to be a threat.[130] As with all whistleblowing claims, the problem is one of separating the wheat from the chaff. How does one take notice of wrongdoing, stop it in time, and protect those that report on it without encouraging false or, at the very least, burdensome claims that interfere with the organization's mission? Perhaps it is possible that technology can provide some sort of solution for sorting out these claims in the new world of virtual work.

A new website, Glassdoor,[131] asks for anonymous users to provide information about their companies and the salaries they receive, and asks them to share information about the CEOs and other top management at various companies. While this information is perhaps basic, how long will it be before Glassdoor, or its analogues and future competitors, begins asking for other types of information and is able to provide an accurate snapshot of what it is truly like to work at a company? Along with other measures, such as surveys, these types of tools may help users discern information about a company before they join as employees.

Of course, that brings out the possibility that there will be some users who will write undeserved negative comments. Perhaps the users will not just be acting irascibly but will be trying to interfere deliberately with the information. In that case, these "trolls" will pose a real danger to the success of the endeavor, unless of course the computer algorithm is programmed to deal with this eventuality. In which case (perhaps by using a type of program similar to that which

130. *See* Andrew Martin, *Union of Whole Foods and Wild Oats Is Put in Doubt*, N.Y. TIMES, July 30, 2008, www.nytimes.com/2008/07/30/business/30food.html (describing CEO's use of electronic messaging board in the midst of negotiations to purchase grocery chain Wild Oats).

131. GLASSDOOR, http://www.glassdoor.com (last visited Oct. 12, 2012).

allows iTunes or Amazon to make recommendations based on items that each user likes) the website will be able to—at least in a crude way—sort the trolls from the workers providing objective information that would help prevent wrongdoing or provide advice to jobseekers. While technology may provide some creative solutions that may help whistleblowers to communicate information and may also be of use for others seeking information, what are some of the other solutions that might help virtual whistleblowers?

B. Citizen Employees or Citizen Journalists?

The line between professional journalists and bloggers has blurred. In recent years, courts have struggled to delineate between legitimate journalists and those who would declare themselves journalists to obtain the privileges afforded to professional journalists.[132] Journalists often obtain information from confidential sources and in some cases have even been jailed for refusing to disclose their sources. The Supreme Court has recognized that in some circumstances, requiring a journalist to reveal their sources is detrimental to the free flow of information.[133] While some states have passed "shield laws" to protect journalists who refuse to reveal their sources, it is unclear whether those laws apply to bloggers.

In *Branzburg v. Hayes*,[134] the Supreme Court heard from a journalist who argued that "journalists should have a qualified privilege not to testify before the grand jury if the outcome is to reveal a confidential source."[135] The Court declined to extend such privilege, reasoning that defining a class of people as "journalists" and granting them special legal status would be difficult and "constitutionally suspect."[136] The Court also noted that "[f]reedom of the press is 'a "fundamental personal right" which is not confined to newspapers and periodicals.'"[137] In the wake of *Branzburg*, many state legislatures have passed shield laws, which exempt journalists from revealing their

132. *See generally* Lili Levi, *Social Media and the Press*, 90 N.C. L. REV. 1531 (2012) (discussing the impact that the Internet has had on journalism and judicial interpretation of journalistic privilege).

133. *See, e.g.*, Tracie Watson & Elisabeth Piro, Note, *Bloggers Beware: A Cautionary Tale of Blogging and the Doctrine of At-Will Employment*, 24 HOFSTRA LAB. & EMP. L.J. 333, 343 (2007) (citing Branzburg v. Hayes, 408 U.S. 665, 725, 737–38 (1972) (Stewart, J., dissenting)).

134. 408 U.S. 665.

135. Watson & Piro, *supra* note 133, at 343.

136. *Id.* at 343–44.

137. *Id.* (quoting *Branzburg*, 408 U.S. at 704).

confidential sources before a grand jury.[138] During oral arguments of *In re Grand Jury Subpoena, Judith Miller*, Floyd Abrams, a prominent First Amendment attorney, conceded that web bloggers should have a constitutional privilege to refuse to disclose confidential sources.[139] The special prosecutor, Patrick Fitzgerald, responded by noting that "[j]ournalists are not entitled to promise complete confidentiality—no one in America is."[140] The debate is important, as ambiguity in the application of shield laws might discourage potential sources and whistleblowers from coming forward on blogs or in print.[141]

In *O'Grady v. Superior Court*, a California appellate court allowed a blogger to invoke journalistic privilege to protect a confidential source.[142] In *O'Grady*, Jason O'Grady owned and operated O'Grady's PowerPage, a blog dedicated to news and information about Apple Macintosh computers, software, and hardware.[143] In November 2004, PowerPage published an article with O'Grady's byline that included details on a rumored new Apple product known as Asteroid.[144] The article included details regarding Asteroid's price and release date.[145] When PowerPage published a PowerPoint presentation with slides marked "Apple Need-to-Know Confidential," Apple filed suit and sought a subpoena of O'Grady's source.[146] O'Grady invoked journalistic privilege to avoid revealing his source.[147] The California court of appeals held for O'Grady, reasoning that "[t]he shield law is intended to protect the gathering and dissemination of *news*, and that is what [O'Grady] did here. We can think of no workable test or principle that would distinguish 'legitimate' from 'illegitimate' news."[148] The court also declined Apple's invitation to rule against O'Grady because blogs do not have editorial oversight, holding that California's shield law does not depend on such oversight.[149] Finally, the court acknowledged a

138. *Id.* at 344.
139. William E. Lee, *The Priestly Class: Reflections on a Journalist's Privilege*, 23 CARDOZO ARTS & ENT. L.J. 635, 635 (2006) (citing *In re* Grand Jury Subpoena, Judith Miller, 397 F.3d 964 (D.C. Cir. 2005)).
140. *Id.* at 638–39.
141. *Id.* at 669–70.
142. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 106 (Ct. App. 2006).
143. *Id.* at 77.
144. *Id.* at 78. Asteroid was a FireWire port that integrated with GarageBand, a recording software, and allowed easier recording of audio onto the computer. *Id.*
145. *Id.*
146. *Id.* at 79–81.
147. *Id.* at 81.
148. *Id.* at 97.
149. *See id.*

distinction between news published on a news-oriented website and a deposit of information by a casual visitor into an open forum.[150] In light of *O'Grady*, at least one court seems to recognize the application of shield laws to bloggers as well as journalists. Professor Mary-Rose Papandrea proposed a solution to the shield law dilemma modeled on the Federal Election Commission's press exception: "[I]n order to qualify . . . an entity's materials must be available to the general public."[151]

Bloggers not only claim the right to keep their sources anonymous, but some want to remain anonymous themselves. The Delaware Supreme Court recently recognized the right of online bloggers to remain anonymous in *Doe v. Cahill*.[152] Cahill, a public figure, claimed a blog contained defamatory statements about him and demanded that the ISP reveal the identity of the blogger.[153] The court clearly attempted to protect the blogger, noting that "[t]he advent of the Internet dramatically changed the nature of public discourse by allowing more and diverse people to engage in public debate."[154] Ultimately, the court held that plaintiffs need to withstand a summary judgment motion for defamation before the identities of online bloggers will be revealed.[155]

The debate over whether bloggers are journalists could have very real implications for virtual whistleblowing. Blogs could, in a sense, comprise a sort of media that is unbound by geography or physical capacity. Dissemination of information via blogs will continue to grow and legitimate whistleblower complaints may begin to appear on established blogs that are perhaps more mainstream than WikiLeaks. The journalistic status of blogs will doubtlessly affect whether whistleblowers will enjoy legal protections when they blow the whistle online. A blogger's ability to keep his or her sources anonymous may change the incentive structure for whistleblowers that consider coming forward through an online forum. As more media shifts to the Internet and blogs become a powerful media tool, courts should carefully and consistently extend journalistic privileges to bloggers. Those privileges should be directed at those bloggers who are engaged

150. *Id.* at 99.
151. Mary-Rose Papandrea, *Citizen Journalism and the Reporter's Privilege*, 91 MINN. L. REV. 515, 575 (2007).
152. Watson & Piro, *supra* note 133, at 351 (citing *Doe v. Cahill*, 884 A.2d 451, 456 (Del. 2005)).
153. *Id.* (citing *Cahill*, 884 A.2d at 454–55).
154. *Id.* (quoting *Cahill*, 884 A.2d at 455).
155. *Id.* (citing *Cahill*, 884 A.2d at 457).

in collecting and disseminating news that impacts the public, including information gleaned from citizen employees.

C. *Law Reform*

As noted above in previous sections, it would appear that whistleblogging is here to stay and will only increase in years to come. Further, platforms like YouTube and WikiLeaks are providing opportunities for whistleblowers to publicize wrongdoing to a wider audience. As noted above, several aspects of law reform are needed to provide workers—both virtual and those in brick-and-mortar offices—with more effective whistleblowing protections. Law reform should therefore fall into three tracks: 1) to provide protections to virtual whistleblowers directly or through expanded protections to the media, 2) to strive for uniformity among whistleblowing laws so that they will be more easily understood among workers, and 3) to protect off-duty conduct of workers, which would broadly protect blogging activity.

First, existing whistleblower protection statutes could be amended specifically to protect whistleblowers. Alternatively, in those jurisdictions relying upon judicial decisions on public policy to protect workers, courts should take this new form of whistleblowing into account. Another way to accomplish the same goal would be to provide a threshold protection for contact between whistleblowers and the media.[156] Protection for blogs and other online social media may in some sense be derivative of the protection that would attach to traditional media. The first step, therefore, would be to secure more protection for whistleblowers who contact the media directly. The next step would then be to have an expansive definition of the media, which would include those who have their stories featured on a blog as well as those who would whistleblog directly.

Second, protections for whistleblowers, if they are to be effective, must become more uniform across jurisdictions and be better understood by workers. As noted in the introduction, workers do not often understand their rights. Further, the more nuanced and complicated the laws are—and the more they vary by jurisdiction—

156. *See* Elletta Sangrey Callahan & Terry Morehead Dworkin, *Who Blows the Whistle to the Media, and Why: Organizational Characteristics of Media Whistleblowers*, 32 AM. BUS. L.J. 151, 155–58 (1994) (noting that the False Claims Act and some other statutes protect external whistleblowing but that it is not the norm); *see also* Jenny Mendelsohn, Note, *Calling the Boss or Calling the Press: A Comparison of British and American Responses to Internal and External Whistleblowing*, 8 WASH. U. GLOBAL STUD. L. REV. 723, 733–34 (2009) (noting marked British preference to protect internal whistleblowers).

the more difficult it will be to secure enforcement of those rights. As noted by Professor Richard Carlson in his article, *Citizen Employees*:

> The law of citizen employees has evolved by so many separate roads that it remains without any sure center or model. The result is incomplete coverage, thwarted sharing of experience across jurisdictions and regulatory schemes, and impeded development of coherent and widely shared principles. The solution to these problems involves two parts. First, lawmakers should recognize citizen employees as a discreet class having a common set of problems and presenting a common set of challenges. Citizen employees resemble other employee groups defined by conduct, but they are distinguished by the purpose or effect of their conduct—upholding public interests. Recognizing citizen employees as a class would facilitate discussion about the ideal balance of public, employee, and employer interests and about the best rules and remedies for achieving balance.
>
> Second, lawmakers should enact a law with broadly stated principles analogous to the expansive anti-discrimination language of Title VII, granting a mandate for courts to develop a true "common law" for citizen employees. The model for such a law might come from Congress, perhaps by consolidating existing federal laws into a single act, or it might come from the National Conference of Commissioners on Uniform State Laws or the American Law Institute.[157]

Whistleblowing employees—and society—will be better served by a set of uniform laws that are easily understood by employees. In this way, we will be able to reach a more optimal level of whistleblowing and deterrence for wrongdoing that is discovered within organizations. Third, and finally, we also need additional laws providing protections for employees for their off-duty conduct. If employees blog about matters that are unrelated to their job, they should be protected from retaliation by these types of statutes.

VI. CONCLUSION

The journalist and blogger question will eventually be ripe for adjudication. Even before that happens, legislatures and courts should recognize the trend from traditional print and broadcast media towards Internet media. Bloggers should be granted the same privileges as journalists, though the class should be defined and limited appropriately. This is no easy task, but elements such as

157. Carlson, *supra* note 16, at 281–82.

editorial oversight or original intent to gather and disseminate news are two possible approaches. Extending journalists' privileges, like state shield laws, to bloggers would make whistleblowers more secure in their anonymity when revealing confidential information to an Internet-based reporter. This in turn would potentially incentivize more whistleblowers to come forward.

As noted in the previous section, law reform could include three possible directions. The first would be to provide protections to virtual whistleblowers directly or via the expansion of the term *media* and also to extend additional protections to those citizen employees who choose to contact the media. The second avenue, which is more general, would advocate making the whistleblower protection laws more uniform and easily understood by workers. The final reform that might prove useful for workers and bloggers in general would be additional protections for off-duty conduct of workers.