Washington University Law Review

Volume 89 | Issue 3

January 2012

Social Networking v. The Employment- at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking

Catherine Crane

SOCIAL NETWORKING V. THE EMPLOYMENT-AT-WILL DOCTRINE: A POTENTIAL DEFENSE FOR EMPLOYEES FIRED FOR FACEBOOKING, TERMINATED FOR TWITTERING, BOOTED FOR BLOGGING, AND SACKED FOR SOCIAL NETWORKING

I. INTRODUCTION

Everyone is doing it: Grandma Margaret, Ginkgo the Black Labrador, and even President Obama have all jumped into the social networking craze via Facebook and a host of other social media options now available in cyberspace.[1] With more than 800 million active Facebook users, over half of which visit the site daily,[2] more than 181 million blogs bouncing around the blogosphere,[3] and Twitter being the 15th most visited webpage in the world,[4] the constant barrage of social media-related firings popping up in the news[5] should thus come as little surprise. Moreover, the rate of these high-profile terminations will probably accelerate in the next few years as the original college-aged Facebook users[6] begin their professional

1. *See* Ginkgo's Facebook Page, FACEBOOK.COM, http://www.facebook.com/home.php#!/pages/Ginkgo/155110637845600 (last visited Jan. 2, 2012); Margaret Strayer's Facebook Page, FACEBOOK.COM, http://www.facebook.com/home.php#!/profile.php?id=100001306798922 (last visited Jan. 2, 2012); President Barack Obama's Facebook Page, FACEBOOK.COM, http://www.facebook.com/home.php#!/barackobama (last visited Jan. 2, 2012).

2. *Statistics*, FACEBOOK.COM, http://www.facebook.com/press/info.php?statistics (last visited Jan. 2, 2012). *Cf.* Mike Ivey, *Facebook on the Clock: Businesses Grapple with Social Media Use at Work*, CAPITAL TIMES (MADISON, WIS.), Mar. 8, 2010, *available at* 2010 WLNR 4891993 (noting in March 2010, there were just 400 million active Facebook users).

3. BlogPulse Stats for Jan. 3, 2012, BLOGPULSE.COM, http://www.blogpulse.com/index.html (last visited Jan. 3, 2012).

4. *The 100 Most-Visited Sites: United States*, GOOGLE.COM, http://www.google.com/adplanner/static/top1000/index.html (as of Jul. 2011) (last visited Jan. 3, 2012).

5. *See* Rafael Gely & Leonard Bierman, *Workplace Blogs and Workers' Privacy*, 66 LA. L. REV. 1079, 1087–88 (2006); Stephen D. Lichtenstein & Jonathan J. Darrow, *Employment Termination For Employee Blogging: Number One Tech Trend for 2005 and Beyond, or a Recipe for Getting Dooced?*, 2006 UCLA J.L. & TECH. 4; Charles Duhigg, *World Wide Water Cooler: Can You Be Fired for Complaining About Your Boss Online?*, LEGAL AFF., Mar.–Apr. 2004, at 8.

6. When Facebook was created in 2004, it was originally only available to college students. Linda Roeder, *Where Did Facebook Come From?: The History of Facebook*, ABOUT.COM, http://personalweb.about.com/od/makefriendsonfacebook/a/whatisfacebook_5.htm (last visited Jan. 2, 2012). Even with Facebook's expansion beyond college dormitories to anyone with access to a computer, the 18–25 age demographic still comprises the largest age group of Facebook users. Justin Smith, *College Students' Facebook Use Easing Up Over the Summer, While Parents Logging On in Record Numbers*, INSIDEFACEBOOK (July 6, 2009), http://www.insidefacebook.com/2009/07/06/college-students-facebook-use-easing-up-over-the-summer-while-parents-logging-on-in-record-numbers/.

lives and enter the workforce. And when you consider that "[y]ounger generations have much less concern about online privacy than older generations,"[7] reflecting a massive societal shift in privacy norms,[8] employer backlash over employee Internet speech is destined to become a permanent landmine in the employment law landscape.

Yet interestingly, the crux of the employee social networking debate lies in the vastly different perceptions held by employers and employees on employee privacy rights. While most business executives assert they have a right to know about all of their employees' social networking activities, most employees believe their bosses have no right to inquire into their non-work lives.[9] This discrepancy explains why efforts to resolve employee Internet speech issues range from giving employers free reign to fire employees over any Internet speech—the classic employment-

7. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1237 (2010) (citing John Palfrey & Urs Gasser, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 82 (2008) and Press Release, Zogby Int'l, What is Privacy? Poll Exposes Generational Divide on Expectations of Privacy, According to Zogby/Congressional Internet Caucus Advisory Committee Survey (Jan. 31, 2007), *available at* http://www.zogby.com/news/2007/01/31/what-is-privacy-poll-exposes-generational-divide-on-expectations-of-privacy-according-to-zogbycongre/).

8. Robison, *supra* note 7, at 1237. "For users of these [social networking] services, the value of networking and communicating with others outweighs the intangible costs to their personal privacy." *Id.* (citing Matt Asay, *Google Privacy Controls: Most People Won't Care*, CNET (Nov. 5, 2009, 9:44 AM), http://news.cnet.com/8301-13505_3-10390456-16.html ("[F]or all our hand-wringing over privacy—and for good reason—the reality is that most of us, most of the time, really don't care. Or, rather, if accessing useful services or getting work done more efficiently requires some privacy concessions, we gladly concede.")).

9. H. Christopher Boehning & Daniel J. Toal, *Social Networking Data Presents New Challenges*, 241 N.Y. L.J., June 30, 2009, at 5 (citing Andrew LaVallee, *Bosses and Workers Disagree on Social Network Privacy*, WALL ST. J., May 19, 2009, http://blogs.wsj.com/digits/2009/05/19/bosses-and-workers-disagree-on-social-network-privacy/).

Perhaps the most alarming example to date of how invasive employer inquiries into the social networking activities of their employees have become can be found in Maryland. Its Department of Corrections, until recently, required job applicants to supply passwords to their social media accounts as part of its hiring process. Marie-Andrée Weiss, *The Use of Social Media Sites Data By Business Organizations in Their Relationship with Employees*, 15 J. INTERNET L. 16, 17 (Aug. 2011) (citing Letter from Deborah A. Jeon, Legal Director, American Civil Liberties Union of Maryland, to Secretary Gary D. Maynard, Maryland Department of Public Safety and Correctional Services (Jan. 25, 2011), *available at* http://www.aclu-md.org/aPress/Press2011/collinsletterfinal.pdf). However, Maryland Public Safety Secretary Gary Maynard suspended the policy after receiving a complaint letter from the Maryland ACLU. Weiss, *supra*, at 17 (citing Letter from Secretary Gary D. Maynard, Maryland Department of Public Safety and Correctional Services, to Sara N. Love, President, American Civil Liberties Union of Maryland (Feb. 22, 2011), *available at* http://www.aclu-md.org/aPress/Press2011/letter_maynard.pdf). The Maryland legislature also responded in March 2011, introducing a bill that "would prohibit an employer from requiring an employee or a candidate to provide his online user names or passwords." Weiss, *supra*, at 17 (citing S.B. 971, 2011 Leg., 428th Sess. (Md. 2011), *available at* http://mlis.state.md.us/2011rs/billfile/sb0971.htm).

at-will doctrine[10]—to claiming an employee has "a right to a life [and a blog] away from work"[11] that should be legally protected through lifestyle discrimination statutes.[12] These and other proposals, however, either privilege the employer's interests above the employee's, or vice versa, always leaving one party almost powerless to defend his or her actions against the other. A more nuanced proposal, therefore, would balance the employer's interest in protecting the image of—and ensuring the smooth functioning of—his or her company[13] with the employee's interest in reveling in the unprecedented phenomena of social networking[14] and blogging.[15] The fulcrum in this balancing act exists as one, seemingly obvious, factor: privacy settings.

The Stored Communications Act of 1986 ("SCA") makes it unlawful to "(1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[] an authorization to access that facility . . . and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage."[16] As applied to blogging, several cases have ruled that an employer who gains unauthorized access to an employee's password-protected blog—and punishes or fires the employee for anything appearing on that blog—may have violated the SCA and thus would be liable to the employee for that unauthorized access.[17] Yet another case, decided in May 2010, held that gaining

10. *See infra* note 20.

11. Gely & Bierman, *supra* note 5, at 1086 (citing Matthew W. Finkin, *Life Away from Work*, 66 LA. L. REV. 945 (2006)).

12. *See* Shelbie J. Byers, Note, *Untangling The World Wide Weblog: A Proposal for Blogging, Employment-At-Will, and Lifestyle Discrimination Statutes*, 42 VAL. U. L. REV. 245, 247, 266 (2007) (arguing that blogging should be protected under lifestyle discrimination statutes that prevent employers from firing employees for engaging in legal, off-duty activities—like smoking).

13. *See* Ivey, *supra* note 2 (explaining that, in regard to employees using social networking sites, "it's not the waste of time that presents the greatest risks to employers [but rather] the possible damage from leaked company information, negative publicity or worse.").

14. "[T]ime spent on social networks surpassed that for e-mail for the first time in February [2009], signaling a paradigm shift in consumer engagement with the Internet." Teddy Wayne, *Social Networks Eclipse E-mail*, N.Y. TIMES, May 18, 2009, at B3. *See also* Ivey, *supra* note 2 (noting that "[o]ne 2009 report from the University of Melbourne in Australia found that spending time on personal websites provided workers with a 'mental break' that ultimately increased their ability to concentrate, correlating with a 9 percent increase in productivity.").

15. Gely & Bierman, *supra* note 5, at 1081–82 (arguing blogging generates trust between consumers and information sources by allowing people to access information in a much more personal and meaningful way than by gathering information through the mainstream media). *See also* Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231, 237–38 (Ct. App. 2008) (discussing emotional benefits of blogging, especially when done anonymously).

16. 18 U.S.C. § 2701(a) (2006).

17. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002); Pietrylo v.

unauthorized access to private Facebook wall posts and MySpace comments may also constitute a violation of the SCA.[18] Although some commentators and other courts disagree with courts interpreting the SCA in this more expansive way,[19] these recent rulings may nevertheless foreshadow an emerging cause of action for employees fired over their social networking or blogging speech against their former employers.

Therefore, despite the employment-at-will doctrine generally providing private sector employers with free reign to fire employees for any Internet posting the employer finds objectionable,[20] the employer will potentially face legal problems for basing the employee's termination solely on a posting the employer discovered through an unauthorized access of that posting.[21] Consequently, in a legal system that provides little to no redress for private sector employees fired for Internet speech,[22] the SCA may provide such an employee with a cause of action against his or her employer if it can be proven that (1) the employee purposely placed

---

Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009).

18. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

19. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1217–18 (2004).

A New York state trial court, faced with a factually similar scenario, held that a defendant *could* subpoena information about a plaintiff's Facebook and MySpace profiles, regardless of any privacy protections the plaintiff placed on those profiles. Weiss, *supra* note 9, at 22 (summarizing Romano v. Steelcase, Inc., No. 2006-2233, 2010 WL 3936366 (N.Y. Sup. Ct. Sept. 21, 2010) (order granting "Defendant access to Plaintiff's current and historical Facebook and MySpace pages and accounts")). However, *Romano* focused mainly on the plaintiff's expectation of privacy regarding her Facebook account, only mentioning that the court considered the SCA's application to the case without any analysis of how the SCA would affect the case's outcome. *Romano*, 2010 WL 3936366.

20. "The vast majority of private sector employees in the United States are employees-at-will, who can be dismissed 'for any reason, even for no reason, without legal liability attaching.'" Ken Matheny & Marion Crain, *Disloyal Workers and the "Un-American" Labor Law*, 82 N.C. L. REV. 1705, 1708 (2004) (quoting Deborah A. Ballam, *Employment-At-Will: The Impending Death of a Doctrine*, 37 AM. BUS. L.J. 653, 653 (2000)).

21. This argument will be developed throughout this Note, but for a general overview, see *Konop*, 302 F.3d at 880 (holding an employee's claim that his employer violated the SCA by gaining unauthorized access to the employee's password-protected blog the employee maintained for discussions about employment conditions will survive the employer's motion for summary judgment); *Pietrylo*, 2009 WL 3128420, at *3 (holding that, despite the fact that a fellow co-worker and authorized user of an employee's password-protected MySpace.com chat group provided their employer with her log-in information, the claim that the employer violated the SCA will survive a motion for summary judgment because the employer coerced—and thus did not gain truly authorized access—to the employee's website); and *Crispin*, 717 F. Supp. 2d at 991 (holding that MySpace comments and Facebook wall posts could be considered private, and thus not subject to subpoenas in a civil suit, if the MySpace or Facebook user configured his or her privacy settings to prevent the general public from accessing his or her information).

22. *See* Deon Roberts, *Commentary: Facebook Posts Can Come Back to Haunt Employees*, NEW ORLEANS CITYBUSINESS, June 29, 2009; Jake Tapper & Audrey Taylor, *Blogging Can Get You in Trouble at Work*, ABCNEWS.COM (Feb. 9, 2005), http://abcnews.go.com/WNT/Business/story?id=485895&page=1.

privacy settings on his or her social networking or blog website to allow access to the site for only a select group of the general public, rather than the public at-large,[23] (2) the employer was not a member of the group granted such access by the employee,[24] (3) the employer viewed the Internet posting without authorized access,[25] and (4) the employer was not shown the posting by someone granted access to the employee's social networking or blog website.[26]

First, this Note will explore how the courts have generally dealt with social networking and blogging disputes in both the public and private sectors.[27] Second, this Note will analyze critiques of the courts' handling of these cases and survey alternative solutions. Third, this Note will discuss various cases interpreting the SCA and how those rulings could apply to an employer-employee Internet speech dispute. Fourth, this Note will examine two cases—*Konop v. Hawaiian Airlines, Inc.*[28] and *Pietrylo v. Hillstone Restaurant Group*[29]—actually using the SCA to provide an employee a cause of action against his employer for retribution over the employee's Internet speech. Fifth, this Note will look at the principles established in *Crispin v. Christian Audigier, Inc.*,[30] and explore whether the reasoning of *Konop* and *Pietrylo* can be extended to protect employee speech on social networking sites like MySpace and Facebook. Finally, this Note will conclude that while SCA protection for this type of Internet speech ultimately will be limited, the SCA provides the greatest protection to employees who place restrictive privacy settings on their social networking sites.

---

23. *See Crispin*, 717 F. Supp. 2d at 991.

24. *See Konop*, 302 F.3d at 879–80; *Pietrylo*, 2009 WL 3128420, at *1.

25. *See Konop*, 302 F.3d at 879–80; *Pietrylo*, 2009 WL 3128420, at *1.

26. *Cf. Pietrylo*, 2009 WL 3128420, at *3 (holding an employee with access to a website cannot grant an employer authorization access if the employer coerces the employee to provide that information); *see also* § 2701(c)(2) (noting that no SCA violation occurs "with respect to conduct authorized . . . (2) by a user of that service with respect to a communication of or intended for that user").

27. While this Note focuses on employer-employee disputes over Internet speech in the private sector, an overview of the law's treatment of the issue in the public sector will provide some background and set up a contrast to its treatment of the topic in the private sector.

28. 302 F.3d 868, 880 (9th Cir. 2002). For a general explanation of *Konop*'s reasoning, see *supra* note 21.

29. No. 06-5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009). For a general explanation of *Pietrylo*'s reasoning, see *supra* note 21.

30. 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010). For a general explanation of *Crispin*'s reasoning, see *supra* note 21.

II. BACKGROUND: STANDARD APPROACHES TO INTERNET SPEECH DISPUTES IN THE PRIVATE AND PUBLIC SECTORS

A. Public Sector[31]

Government employees enjoy much stronger free speech protections because, unlike private sector employers, government employers are subject to the restraints of the U.S. Constitution.[32] The First Amendment[33] limits the ability of the government to discipline its employees for protected speech.[34] *Garcetti v. Ceballos*[35] sets out the most current test for determining whether an employee's speech garners First Amendment protection and insulates him or her from termination by a government employer.[36] First, the employee must prove that he spoke as a citizen—rather than in his capacity as a government worker—and that his speech involved a matter of public concern.[37] Next, a court must decide whether the government had a legitimate justification for not providing its employees with the same First Amendment protection it affords to normal private citizens.[38] Consequently, while this test provides public employees much more speech protection than private employees, the Court nevertheless recognizes that government employers have as much of a right as private employers to control, manage, and discipline their employees when their speech or actions adversely interfere with their job responsibilities.[39] In this aspect, at least, government and private

31. The two main cases discussed in this section, Synder v. Millersville Univ., No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008) and Evans v. Bayer, 684 F. Supp. 2d 1365 (S.D. Fla. 2010), also appear on a social-networking litigation outline developed by the Smithsonian Institution. Lauryn H. Guttenplan, *Social Media Resources*, A.L.I.-A.B.A. CONTINUING LEGAL EDUCATION, Mar. 24–26, 2010, *available at* WL SR005 ALI-ABA 487.

32. Tanya E. Milligan, *Virtual Performance: Employment Issues in the Electronic Age*, 38 COLO. LAW., Feb. 2009, at 29, 30.

33. U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . .").

34. While the First Amendment represents the most obvious defense against government employers who fire employees over Internet speech, the Fourth Amendment, preventing the government from engaging in unreasonable searches and seizures, U.S. CONST. amend. IV, also prevents employees from unreasonably searching the computer files of their employees. The "employees' expectations of privacy and the reasonableness of the search" determine whether the government has a right to search through its employees' digital files. Milligan, *supra* note 32, at 31. The Fourteenth Amendment incorporates these rights against state action, preventing states from violating these protections.

35. 547 U.S. 410 (2006).

36. Milligan, *supra* note 32, at 30 (citing *Garcetti*, 547 U.S. at 418).

37. *Id.*

38. *Id.*

39. *Id.* at 31 (citing *Garcetti*, 547 U.S. at 418–19). Note that even speech containing both matters

employees tend to receive identical treatment from their respective employers if their employers can characterize the employee Internet speech as disruptive to the work environment.[40]

Law regulating student Internet use provides some clues as to what constitutes punishable Internet speech in the employment context. For example, *Synder v. Millersville University*,[41] which discusses a student-university relationship, upheld a university's decision to deny a student teacher her education degree because of postings she made on her MySpace page during her student-teaching practicum.[42] Despite being told in her orientation not to name any students or teachers on her personal social networking pages,[43] the student teacher told her high school students about her MySpace page,[44] discussed students on her MySpace page,[45] posted inappropriate pictures of herself on the site,[46] and generally referred to her teaching supervisors in a negative context on her MySpace

---

of public concern and disruptive, derogatory content cannot always protect a public employee from termination. *Id.* (citing Curran v. Cousins, 509 F.3d 36, 48–49 (1st Cir. 2007) (holding a corrections officer referring to a sheriff, who allegedly harassed and allegedly wrongly disciplined political rivals, as Hitler in an employee-union-run blog could be terminated without violating the First Amendment)).

40. For examples of public employees getting fired or being forced to resign over disruptive speech, see Sewell Chan, *Facebook Postings Prompt Quick Exit of a City Politician's Aide*, N.Y. TIMES, July 29, 2009, at A18; Andria Simmons, *Bus Driver Sues, Saying She was Fired Over Facebook Post*, ATLANTA J.-CONST., Oct. 7, 2010, http://www.ajc.com/news/gwinnett/bus-driver-sues-saying-649005.html; Tom Troy, *Election Worker Fired for Facebook Posting*, TOLEDO BLADE, May 12, 2010, *available at* http://www.toledoblade.com/Politics/2010/05/12/Election-worker-fired-for-Facebook-posting.html. For private employees fired over disruptive speech, see Stephanie Armour, *Warning: Your Clever Little Blog Could Get You Fired*, USA TODAY, June 15, 2005, at 1B; *supra* note 22.

41. No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008).

42. *Id.* at *15.

43. During the orientation, the student teacher's supervisors warned that a student teacher had previously been dismissed from his teaching job after posting comments about his host school on "his personal webpage." *Id.* at *5.

44. When the student teacher later told one of her supervisors that she discussed her MySpace page with her students, she received a second warning that "it was not proper to discuss her MySpace account with [her] students [or] allow students to become involved in her personal life." *Id.*

45. After the student teacher discovered that one of her students saw a picture of one of the student teacher's friends on her MySpace page and approached her friend outside of school, the student teacher reprimanded the student by saying it was inappropriate to contact the student teacher's friends outside of school. The student teacher then posted on her own MySpace page, "First, Bree [the student teacher's friend] said that one of my students was on here looking at my page, which is fine. I have nothing to hide. I am over 21, and I don't say anything that will hurt me (in the long run)." *Id. See also* T. Keung Hui, *Teacher's Facebook rant leads to suspension: Comments on religion irked parents*, CARY NEWS, Feb. 24, 2010, *available at* http://www.carynews.com/2010/02/24/16203/teachers-facebook-rant-leads-to.html (detailing how a teacher was suspended when she posted on her Facebook page that she considered it a "hate crime" when her students placed a Bible on her desk and that she "was able to shame her kids" over the occurrence).

46. The student teacher posted a picture of herself "wearing a pirate hat and holding a plastic cup with a caption that read 'drunken pirate.'" *Snyder*, 2008 WL 5093140, at *6.

page.[47] These MySpace postings, in part, caused her host school to dismiss her from the practicum program,[48] which in turn caused the student's university to deny her an education degree.[49]

Conversely, other student cases show how the First Amendment can insulate Internet speech from punishment. For instance, *Evans v. Bayer*[50] involved a principal suspending[51] a student for creating a group on Facebook called "Ms. Sarah Phelps is the worst teacher I've ever met."[52] The student sued the school to revoke her suspension and prevent the principal from keeping it on her permanent record, arguing that the principal's actions violated her First Amendment rights because she had "engaged in an off-campus activity in a non-violent and non-threatening public forum" when the speech in question occurred.[53] The court denied the principal-defendant's motion to dismiss, finding that the student's "actions cannot be construed as even remotely disruptive, nor was her speech in any way lewd, vulgar, defamatory, promoting drug use or violence as seen in other cases."[54] The court determined that while the Court's ruling in *Tinker v. Des Moines Independent Community School*

47. The student teacher also posted, "I figure a couple of students will actually send me a message when I am no longer their official teacher. They keep asking me why I won't apply there. Do you think it would hurt me to tell them the real reason (or who the problem was)?" *Id.* at *5. One of the student teacher's supervisors, who wrote in her mid-term evaluation that she was poorly prepared for class and that she shared her personal life with her students in an unprofessional way, *id.* at *4, believed the student teacher's MySpace posting was directed at her, *id.* at *6. The student teacher also admitted in trial that she "greatly disliked [this supervisor], believing her criticisms to be unfair." *Id.* at *5 (citing Tr. May 6, 2007 at 66, 70–74).

48. *Id.* at *6.

49. Millersville University students had to complete the student-teaching practicum in order to receive a B.S. in Education. Since the student teacher was not allowed to finish her practicum, Millersville University could not grant her a B.S. in Education; instead, they awarded her with a B.A. in English. *Id.* at *8-9.

50. 684 F. Supp. 2d 1365 (S.D. Fla. 2010).

51. The principal suspended the student, a high school senior, for three days and made her drop her advanced placement classes for ordinary 'honors' classes. Her official suspension notice stated she was reprimanded for "'Bullying/Cyber Bullying/Harassment towards a staff member' and 'Disruptive Behavior.'" *Id.* at 1367.

52. *Id.* The student started the group to allow fellow students to vent about their dislike of this teacher. The student posted, "Ms. Sarah Phelps is the worst teacher I've ever met! To those select students who have had the displeasure of having Ms. Sarah Phelps, or simply knowing her and her insane antics: Here is the place to express your feelings of hatred." *Id.* While the page included a picture of the teacher, it did not contain any violent threats or disrupt school activities. *Id.* The student created the page on her home computer after school hours, and the teacher never saw the posting. *Id.* The principal did not hear about the posting until the student took it down, which was two days after she created the page. *Id.*

53. *Id.* at 1367–68.

54. *Id.* at 1376–77.

District[55] allows schools to punish students for off-campus speech,[56] the school potentially violated the student's First Amendment rights because (1) her off-campus speech did not cause on-campus disruptions,[57] (2) her speech in general "falls under the wide umbrella of protected [First Amendment] speech,"[58] and (3) her right to engage in this type of speech was clearly established at the time of her punishment.[59] These factors enabled the student to pierce the principal's claim of qualified immunity[60] against lawsuits from those suing him personally while acting in his discretionary responsibility,[61] thus allowing the student's suit to proceed.

B. Private Sector Cases Seeking Government Action (Subpoenas) to Unmask Anonymous Private Speakers

Cases involving one private party requesting a government subpoena in a lawsuit against another private party to unmask anonymous Internet speakers seem to imply that anonymous Internet speech will usually be insulated from disclosure—and thus legal liability—whenever a private

55. 393 U.S. 503 (1969).

56. The court in *Evans* found that student conduct, "in class or out of it, which for any reason—whether it stems from time, place, or type of behavior—materially disrupts classwork or involves substantial disorder or invasion of the rights of others is, of course, not immunized by the constitutional guarantee of freedom of speech." *Evans*, 684 F. Supp. 2d at 1370 (quoting *Tinker*, 393 U.S. at 513).

57. "Student off-campus speech, through generally protected, could be subject to analysis under the *Tinker* standard as well if the speech raises on-campus concerns." *Evans*, 684 F. Supp. 2d at 1370. *See also* J.S. v. Blue Mountain Sch. Dist., 593 F.3d 286 (3d Cir. 2010); Doninger v. Niehoff, 527 F.3d 41, 50 (2d Cir. 2008); Wisniewski v. Bd. of Educ. of Weedsport Cent. Sch. Dist., 494 F.3d 34, 38-39 (2d Cir. 2007)). The *Evans* court, however, determined that the student's off-campus speech did not raise on-campus concerns, and thus could not be restricted, because it was Internet speech "made off-campus, never accessed on-campus, and was no longer accessible when the Defendant [principal] learned of it." *Evans*, 684 F. Supp. 2d at 1372.

58. *Id.* at 1374. The *Evans* court found that the student's Facebook posting did not constitute fighting words, obscenity, libel, defamation, or any other category of unprotected speech outside First Amendment protection, even in a school setting. *Id.* at 1372–74.

59. *Id.* at 1376–77. While the court acknowledges the principal-defendant's argument that the law regarding student Internet speech is confusing, it disagreed that the student's speech rights were not clearly established at the time of the punishment: for more than forty years, *Tinker* has required "an indication of disruption, future or present" before a school can restrict the First Amendment rights of its students. Therefore, because the principal should have been aware of the *Tinker* discipline standard, the student's speech rights were clearly established at the time of the incident. *Id.* at 1375–76.

60. "To overcome qualified immunity, the plaintiff must show (1) that the defendant violated a constitutional right, and (2) the right was clearly established at the time of the alleged violation." *Id.* at 1369 (citing Holloman v. Harland, 370 F.3d 1252, 1264 (11th Cir. 2004).

61. "An official is acting in his discretionary capacity if he was '(a) performing a legitimate job-related function (that is, pursuing a job-related goal), (b) through means that were within his power to utilize.'" *Id.* (citing *Holloman*, 370 F.3d at 1265).

party seeks to use state power to chill Internet speech.[62] For instance, in *Krinsky v. Doe 6*,[63] a California state court ruled that Doe 6's motion to quash Krinsky's subpoena, which Krinsky sought to compel a Yahoo!, Inc., ("Yahoo") message board service to reveal Doe 6's identity, should be granted.[64] Krinsky, an officer of a company suing posters on this message board for defamation,[65] subpoenaed Yahoo for the identity of several anonymous posters. Consequently, Doe 6—one of the posters—moved to quash the subpoena because the "plaintiff had failed to state a claim sufficient to overcome [Doe 6's] First Amendment rights for . . . defamation."[66] After deciding that only a plaintiff making "a prima facie showing of the elements of libel"[67] could stop a defendant's motion to quash a subpoena to reveal the defendant's identity,[68] the court decided that, when "viewed *in context*,"[69] Doe 6's messages were not actionable: "[r]ather, they [fell] into the category of crude, satirical hyperbole which, while reflecting the immaturity of the speaker, constitute protected opinion under the First Amendment."[70]

Furthermore, protecting the right to speak anonymously does not extend only to defendants; third parties can also be insulated from being

62. *See* McVicker v. King, 266 F.R.D. 92, 97 (W.D. Pa. 2010) ("While disclosure of the anonymous speakers' identities may certainly be helpful to Plaintiff, the [c]ourt does not believe that this is the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speakers."). Also note "[t]he United States Supreme Court has consistently held that 'an author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment.'" *Id.* at 94 (quoting McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (omissions in original)).

63. 72 Cal. Rptr. 3d 231 (Ct. App. 2008).

64. *Id.* at 234.

65. "Nine of the [ten anonymous] defendants were accused together of libel based on false and misleading Internet statements imputing dishonesty, fraud, improper professional conduct, and criminal activity to the plaintiff." *Id.* at 235. Doe 6's posting in particular accused Krinsky of engaging in lewd sexual acts with her co-workers, along with having "fat thighs, a fake medical degree . . . and poor feminine hygiene." *Id.*

66. *Id.*

67. *Id.* at 245. While the case ended up in a California court because Yahoo is based in that state, the case began in Florida because the defendants were from there. *Id.* at 235. Libel occurs in Florida when "(1) it charges that a person has committed an infamous crime; (2) it charges a person with having an infectious disease; (3) it tends to subject one to hatred, distrust, ridicule, contempt, or disgrace; or (4) it tends to injure one in his trade or profession." *Id.* at 247 (quoting Richard v. Gray, 62 So. 2d 597, 598 (Fla. 1953)). Krinsky argued "Doe 6 implied that she was dishonest by calling her a 'crook' and asserted that she had a 'fake medical degree,' thereby accusing [her] of being dishonest or . . . engaging in conduct incompatible with her employment." *Id.* Krinsky further argued Doe 6 "subjected [Krinsky] to ridicule and disgrace and damaged her reputation by stating that she had 'poor feminine hygiene.'" *Id.*

68. *Id.* at 245.

69. *Id.* at 248 (emphasis in original).

70. *Id.* at 250.

forced to comply with subpoenas from civil plaintiffs trying to gather information against their defendants.[71] In *McVicker v. King*,[72] the court reaffirmed that compelling the disclosure of a non-party is actually much harder than compelling the disclosure of a defendant[73] by making the plaintiff pass a four-part test:

> "whether (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source."[74]

The court held that forcing the website to disclose the identity of its bloggers was not warranted because the plaintiff failed to establish elements (3) and (4) of the test: relevancy and the blog being the only source where the plaintiff could get material information for his case.[75]

C. Private Sector

Without the protections provided by virtue of being a government employee, private sector employees and other litigants suffering adverse action due to their Internet postings try—usually unsuccessfully—to sue on discrimination and invasion of privacy claims.[76] For instance, in *Nguyen v. Starbucks*,[77] an employee claimed Starbucks fired her because

71. *See* McVicker v. King, 266 F.R.D. 92, 97 (W.D. Pa. 2010). In suing a city council for wrongful termination, the plaintiff wanted to subpoena a website that posted anonymous blogs discussing the activities of the city council. The plaintiff sought the names of the anonymous posters in his attempt to contradict the testimony of some of the defendant councilmembers. *Id.* at 93.

72. 266 F.R.D. 92 (W.D. Pa. 2010).

73. *Id.* at 95 (citing Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001)).

74. 266 F.R.D. at 96–97 (quoting the test developed in *Enterline v. Pocono Med. Ctr.*, 751 F. Supp. 2d 782 (M.D. Pa. 2008)).

75. 266 F.R.D. at 97 ("Distilled to its essence, Plaintiff's attempt to obtain the personally identifiable information of the anonymous internet [sic] speakers is a fishing expedition based on speculation that the anonymous bloggers will be able to impeach the deposition testimony of the [i]ndividual [d]efendants.").

76. *See* Nguyen v. Starbucks Coffee Corp., Nos. CV 08-3354 CRB, CV 09-0047, 2009 WL 4730899, at *3 (N.D. Cal. Dec. 7, 2009), *aff'd*, 418 Fed. App'x 606 (9th Cir. 2011) (Plaintiff sued employer for wrongfully terminating her because of her religion); Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 860–61 (Ct. App. 2009) (A college student sued a high school principal for invasion of privacy when he submitted her MySpace entry to a local newspaper for publication).

77. 2009 WL 4730899.

of the religious views she expressed on her MySpace page.[78] But because the posting contained both religious speech and threats against her co-workers,[79] and Nguyen had engaged in other disturbing behavior at work,[80] the court granted Starbucks' motion for summary judgment without much analysis—concluding Nguyen failed to offer any substantial support for her religious discrimination claim.[81] Admittedly, this is a case where, regardless of the presence of the employee's religious Internet speech, the employer was justified in terminating the employee. Nevertheless, the case also implies that as long as the employer has a valid reason to fire an employee, there are very few categories[82] of Internet speech that will convince a court to rule against an employer in an Internet-speech related wrongful termination case.

Moreno v. Handford Sentinel, Inc.,[83] while not being a wrongful termination case, shows the limits of an Internet-related invasion of privacy claim. Here, a college student sued a high school principal for

78. After making what turned out to be frivolous religious discrimination and sexual harassment complaints against her co-workers to her manager, Nguyen took a leave of absence from Starbucks due to the mental and physical pain she claimed were brought on by her negative work environment. *Id.* at *1-2. A few weeks later, a co-worker showed an assistant manager Nguyen's MySpace page, which Nguyen had consistently referenced during her employment. One of the postings on her MySpace page read:

> Starbucks is in deep shit with GOD!! I am now completely disenchanted with humans n I have NO MO Energy left 2 deal w/ their negativity. I've worked Tirelessly 2 not cause trouble, BUT I will now have 2 to turn 2 my revenge side (GOD'S REVENGE SIDE) 2 teach da world a lesson of stepping on GOD. I thank GOD 4 pot 2 calm down my frustrations n worries or else I will go beserk [*sic*] n shoot everyone . . . Prepare to See Crazy Trang [the Plaintiff] in public eye soon IN UR TELEVISION n other news vehicles. I don't know when EXACTLY "cause only GOD knows of our Exact timing in his PERFECTED-CREATED NETWORK (fate!) BUT all I know is I will fight 2 be heard beyond my death.;) N I will not be happy unless I win because I AM GOD N GOD DON'T LOSE.

Id. at *2 (omission in original).

79. *Id.*

80. Before taking her leave of absence, Nguyen would lash out at her colleagues when asked to perform job-related tasks. Nguyen aimed steam at a co-worker, almost burning him; asked customers questions about their national origin and religion, causing customers to complain; and informed a female co-worker how much money to charge for sexual acts should the co-worker ever become a prostitute. *Id.* at *1. Nguyen also wrote her boss a letter in support of her worker's compensation claim, writing "she would 'rather be saving da world via a pornstar instead of working as a barista' and 'Bring out your best boys & whores because I'm really cute, HOT & HORNY! I [love] POT!!!.'" She also wrote '"God is here to save you . . . But 4 only da price of $250,000,000."' *Id.* at *2.

81. *Id.* at *3, *5.

82. *See infra* notes 109–11. If an employer discovers an employee's Internet posting where the employee talks about his religion, sexual orientation, race, or other Title VII protected categories, and the employer subsequently fires the employee, the employee might be able to claim wrongful termination by arguing the employer fired the employee over one of the Title VII protected categories the employee discussed on his Internet posting. *See* Paul S. Gutman, Note, *Say What?: Blogging and Employment Law in Conflict*, 27 COLUM. J.L. & ARTS 145, 184 (2003).

83. 91 Cal. Rptr. 3d 858 (Ct. App. 2009).

submitting one of her MySpace page postings to a local newspaper for publication.[84] The MySpace posting contained several disparaging comments about the student's hometown, where her family still lived.[85] Consequently, upon publication, the student's family received death threats and was forced to move out of the town.[86] However, the court refused to recognize Moreno's invasion of privacy claim,[87] ruling that information posted on MySpace cannot be considered private, and thus could not alone establish an invasion of privacy tort claim.[88] Furthermore, the court declined to accept Moreno's argument that her MySpace postings were private because they were intended for only a limited audience.[89] It also rejected Moreno's argument that because she did not post her last name on her MySpace page, her last name was a private fact that should not have been disclosed in the newspaper article about her posting.[90]

---

84. Moreno, a college student at the University of California at Berkeley, wrote the following on her MySpace page "[f]ollowing a visit to her hometown of Coalinga," California: "'the older I get, the more I realize how much I despise Coalinga,' [followed by] a number of extremely negative comments about Coalinga and its inhabitants." *Id.* at 861. Before Moreno removed the post six days after she put it on her MySpace page, the principal of Coalinga High School had seen the posting and submitted it to a local newspaper for publication. *Id.* The paper then published Moreno's comments in the Letters to the Editor section, attributing them to Moreno using both her first and last names even though Moreno had not listed her last name on her MySpace page. *Id.*

85. Moreno's parents and sister, who attended Coalinga High School at the time of the publication, still lived in Coalinga. *Id.*

86. "The community reacted violently to the publication of the [posting]. [The family] received death threats and a shot was fired at the family home, forcing the family to move out of Coalinga. Due to severe losses, [Moreno's father] closed the 20-year-old family business." *Id.*

87. *Id.* In California, "[t]o state a claim for violation of the constitutional right of privacy, a party must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest." *Id.* at 862 (citing Int'l Fed'n of Prof'l & Technical Eng'rs, Local 21, AFL-CIO v. Super. Ct., 165 P.3d 488 (Cal. 2007)). Finding that Moreno was suing for public disclosure of private facts, the court stated the elements of that tort are: "'(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern.'" 91 Cal. Rptr. 3d at 862 (quoting Shulman v. Grp. W Prods., Inc., 955 P.2d 469 (Cal. 1998)). The court further explained that all elements must be present to establish a claim. *Id.*

88. *Id.* Stating that "[a] matter that is already public or that has previously become part of the public domain is not private," *id.* (citing Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665 (Ct. App. 1984)), the court concluded that by posting comments on "a hugely popular internet site," Moreno "made her article available to any person with a computer and thus opened it to the public eye." *Id.* Thus, "no reasonable person would have had an expectation of privacy regarding the [MySpace] published material." *Id.*

89. *Id.* at 863. While conceding that information disclosed to only a select group of people can still serve as the basis of an intrusion of privacy claim, the court determined that Moreno's argument that she only wanted a few people to see her MySpace page still would not establish the privacy of her postings. Rather, "[b]y posting the article on myspace.com, [Moreno] opened the article to the public at large. Her potential audience was vast." *Id.*

90. *Id.* While Moreno only listed her first name on her MySpace page, the court found the

Despite not being discussed in the opinion, the result of *Moreno* raises the question of whether the outcome would have differed if Moreno had placed privacy protections on her MySpace page.[91] The court found it relevant that her postings were available to anyone with a computer,[92] so perhaps Moreno's "limited audience" argument would have held more weight if, for example, Moreno had chosen to only allow her MySpace "friends" to read her postings. Applying this rationale to the employment context, therefore, would indicate that a court might classify Internet speech that an employee had purposely prevented his or her employer from seeing as private. But to overcome the strength of the employment-at-will doctrine, which usually leads courts to side with employers in wrongful termination cases,[93] privacy suits typically have not proven to be

---

presence of her picture on her page dispositive of her privacy claim. Stated otherwise, one could determine the identity of the author of the postings without knowing Moreno's last name, thus rendering the information public. So "[i]n disclosing [Moreno's] last name, [the principal] was merely giving further publicity to already public information," which "does not provide a basis for the [invasion of privacy] tort." *Id.*

91. "Myspace Members . . . can control how Visitors, other Members and Myspace communicate with them by controlling their account settings, available within the 'Edit Profile' portion of their Myspace profile." *Privacy Policy*, MYSPACE, http://www.myspace.com/Help/Privacy (last revised Dec. 7, 2010) (last visited Jan. 2, 2012). For example, a MySpace user can make his or her profile viewable by only the user's "friends," or other MySpace users the user has given permission to view his or her profile. *MySpace Account Settings and Privacy*, MYSPACE, http://www.myspace.com/my/settings/account/privacy (last visited Nov. 20, 2011) (MySpace users with active profiles can access this link to view the permissions granted to the user's "friends").

On the other hand, Facebook offers more options for users to control who views which portions of their profiles. For instance, users can limit who can look at their profiles, who can send them friend requests, who can post on their walls, and a host of other options to limit the audience of their profiles. *Privacy Settings*, FACEBOOK.COM, http://www.facebook.com/#!/settings/?tab=privacy (last visited on Jan. 2, 2012) (Facebook users with active profiles can access this link to view and change the privacy settings). Facebook users thus have the ability to limit their profiles and posts (including status updates, pictures, and wall posts) to friends, friends of friends, or a customized group of people of their choosing if they do not want all of their information to be available to the general Internet public. *Facebook Help Center*, FACEBOOK.COM, http://www.facebook.com/help/?faq=120939471321735 (last visited on Jan. 2, 2012) (Facebook users with active profiles can access this link to review the Facebook Help Center).

92. *See supra* note 88.

93. See below:

> Private employees have little recourse if they are fired for what they write on blogs or social networking sites, because a private employer does not engage in state action. For instance, in 2004 Delta Airlines fired a flight attendant for keeping a blog in which she posted provocative pictures of herself in her flight attendant uniform.

Cydney A. Tune, *Blogging and Social Networking: Current Legal Issues*, *in* INFO. TECH. L. INST. 2008: NEW DIRECTIONS: SOC. NETWORKS, BLOGS, PRIVACY, MASH-UPS, VIRTUAL WORLDS AND OPEN SOURCE, at 84 (PLI: Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Ser., 2008), *available at* WL 929 PLI/Pat 73.

the best vehicle.[94] Thus, employees need a stronger cause of action to succeed in overcoming the employment-at-will doctrine in such cases.

III. DESCRIPTIONS & CRITIQUES OF ALTERNATIVE PROPOSALS TO RESOLVE EMPLOYER-EMPLOYEE INTERNET SPEECH DISPUTES

A. Lifestyle Discrimination Statutes

Concluding that "neither the currently enacted lifestyle discrimination statutes nor the judicially enforced public policy exceptions to the employment-at-will doctrine adequately protect lawful off-duty activities, such as blogging and the speech that is associated with those blogging activities,"[95] one law review note recommends that legislatures enact tougher lifestyle discrimination statutes to insulate at-will employees from being fired over blogging outside the office.[96] Lifestyle discrimination statutes protect an employee's right to engage in "lawful off-duty activity," such as smoking, thus making it illegal for an employer to fire an employee for those activities.[97] None of the current lifestyle discrimination statutes specifically shield blogging, but the note argues that such statutes are "the most likely source" of law to provide bloggers protection.[98] Therefore, the author proposes her own model lifestyle discrimination statute[99] that prevents employers from firing employees for almost any off-

94. *See supra* Part III.B.2; *supra* note 82.

95. Byers, *supra* note 12, at 247.

96. *Id.*

97. *Id.* at 266.

> Lifestyle discrimination statutes protect an employee's use of lawful products or participation in lawful off-duty activities, conduct, or speech. Specifically, lifestyle discrimination statutes usually protect some form of lawful off-duty activity from intrusion by private sector employers. For instance, statutes in thirty states and the District of Columbia protect smokers, or others who use lawful consumable products from termination based solely on such activities.

Id. (citing FUNDAMENTALS OF EMPLOYMENT LAW 425 (Karen E. Ford et al. eds., 2d ed. 2000); Ann L. Rives, Note, *You're Not the Boss of Me: A Call for Federal Lifestyle Discrimination Legislation*, 74 GEO. WASH. L. REV. 553, 558 (2006); and various state statutes).

98. *Id.* at 268.

99. See proposed statute below:

> (1) It shall be a discriminatory or unfair employment practice for *any* employer to *refuse to hire an applicant, demote, or* to terminate the employment of any employee, *or to fail or refuse to promote or upgrade an employee*, due to that *applicant's or* employee's engaging in any lawful activity *or conduct or speech associated with the protected activity or conduct when done* off the premises of the employer during nonworking hours unless such a restriction:
>
> (a) Relates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular

duty employee speech, including blogging.[100]

While the author proposes a strong method for strengthening lifestyle discrimination statutes to protect bloggers, her statute might actually exacerbate employer-employee conflict over Internet speech and leave employees even more unsure of what their employers think is permissible Internet activity. For example, the statute appears overbroad and vague because the terms "rationally related to the employment activities"[101] and "conflict of interest with any responsibilities"[102] could encompass almost any activity the employer finds objectionable. Consequently, employers could manipulate the statute in numerous ways to justify firing employees over any Internet speech, leaving employees with scant protection for their blogging and social networking activities. Moreover, while the author justifies her statute by arguing it simply models other state statutes passed to protect employees' rights to engage in lawful off-duty conduct,[103] the soundness of enacting such proposed legislation into law in the first place seems questionable upon consideration of how severely it could prevent employers from effectively managing their employees[104] when implemented.[105]

---

group of employees, rather than to all employees of the employer; or

(b) Is necessary to avoid a *bona fide and actual* conflict of interest with any responsibilities of the employer.

Id. at 286 (emphasis in the original) (struck language omitted). Byers notes that this model statute is based upon a Colorado statute, COLO. REV. STAT. § 24-34-402.5 (2001). *Id.* at 285.

100. *Id.* at 286.

101. *See supra* note 99.

102. *Id.*

103. Several states, including California, Colorado, and New York, have enacted statutes that prevent employers from firing employees for various off-duty activities. *Id.* at 269–74 (citing CAL. LAB. CODE § 96(k) (West 2003), COLO. REV. STAT. § 24-34-402.5(1) (2001), and N.Y. LAB. LAW § 201-d(2) (McKinney 2002)). Connecticut's Free Speech Act most explicitly prohibits employees from being fired for speech, "extend[ing] the same protection for free speech that the First Amendment gives public employees, with the exception that the speech is not protected if it substantially or materially interferes with the employee's job." *Id.* at 271–72 (citing CONN. GEN. STAT. § 31-51q (2003) and Julian N. Eule & Jonathan D. Varat, *Transporting First Amendment Norms to the Private Sector: With Every Wish There Comes a Curse*, 45 UCLA L. REV. 1537, 1581 (1998)).

104. Consider the following hypothetical. Such a statute appears to prevent an employer from firing his company's accountant, who never interacted with customers or had any job responsibilities requiring him to deal with customers, for posting numerous pictures of his tattoos and piercings publicly, without any privacy controls, on Facebook. (Suppose the employer was worried about those pictures hurting his company's reputation as a middle-class, suburban friendly business, even though the employer has no evidence that his business has been hurt thus far. Nevertheless, it does not sound completely irrational for the employer to think this might hurt his business, considering the clientele he is trying to target.)

105. Under Byers' proposed statute, particularly § (1)(a), it would seem that the employer could not fire the accountant (discussed in the hypothetical in *supra* note 104) because maintaining the company's public image probably would not be considered as "relat[ing] to a bona fide occupational

B. Disclaimers, Anonymity, & the Introduction of Blogging Guidelines in the Workplace

Rather than depending on broad lifestyle discrimination statutes to protect almost all forms of employee Internet speech, employers and employees can take more discrete measures to resolve Internet speech conflicts at the office. For example, to prevent people from associating an employee's non-work related blog or social networking site with his or her employer, the employee can place a disclaimer on the entrance to those web pages announcing that the following content does not reflect the employer's views.[106] Such disclaimers could insulate the employee from accusations that he is reflecting the employer in a bad light because the disclaimer explicitly dissolves the connection between the employee's Internet speech and the employer.[107] However, such disclaimers might actually cause, rather than prevent, problems between employee bloggers and their employers because the disclaimers might attract more, not less, attention to the fact that the blogger works for that particular employer.[108] As a result, disclaimers alone will not resolve the current employer-employee Internet speech disputes.

Alternatively, bloggers and social networkers could speak either anonymously or through aliases on the Internet to avoid employer

---

requirement" of the accountant or as "reasonably and rationally related to the employment activities and responsibilities . . . of a particular employee [the accountant] . . . rather than to all employees of the employer." *See supra* note 99. It is also questionable whether the employer could legally fire the accountant under § (1)(b) because to do so, the employer must prove that firing or reprimanding the accountant "[i]s necessary to avoid a *bona fide and actual* conflict of interest with any responsibilities of the employer." *Id.* Stated otherwise, what may be considered a "conflict of interest" to the accountant's employer (here, that the accountant's Facebook postings undermine the employer's desire for the company to have a middle-class family image) may not be considered as an "actual conflict of interest" by an outside court because, as discussed in *supra* note 104, the employer has no evidence that the accountant's Facebook postings are driving away middle class clientele. The case would be even harder if the accountant could present evidence that he was an excellent employee with an outstanding reputation at the company.

106. Gutman, *supra* note 82, at 182–83.

107. *Id.* at 182.

108. *Id.* at 183.

> An author's explicit disavowal that the blog does not reflect the views of his or her employer may increase the visibility of his complaints or concerns. In other words, a disclaimer may exacerbate an employer's concerns about blogging and that particular employee since mentioning the employer's name may cause the site to be increasingly indexed by search engines.

Id. (citing Jeremy Wagstaff, *Why Don't You Get the Net?*, FAR E. ECON. REV. 36 (Sept. 5, 2002) and Rick Klau, *How I Learned to Love the Blog*, LAW TECH. NEWS (Nov. 7, 2002), *available at* http://www.law.com/jsp/article.jsp?id=900005532887 (the article appears in its full form on the Law Tech. News website archives—a free registration is required to view the article in full)).

repercussions over their speech. Bloggers could therefore have an invasion of privacy claim against employers who fire them over their Internet speech if the blogger does not explicitly identify himself or his employer.[109] However, much of this cause of action will be tied to whether (1) the employer discovers certain personal characteristics of the blogger—such as an employee's sexual orientation or national origin—and (2) the employee can prove a wrongful termination via discrimination charge against his employer by linking the employer's discovery of those personal characteristics through the employee's website to his firing.[110] Accordingly, only a narrow subset of bloggers and social networkers will be able to make these invasion of privacy claims against their employers,[111] leaving the majority of employees fired for Internet speech without redress.

Finally, companies could attempt to confront the problem head-on by establishing company blogging and social networking guidelines for their employees.[112] Such companies could even go a step further by encouraging their employees to blog and communicate on social networking sites to foster creativity and insight.[113] But since many employers do not want to deal with the hassle of determining for their employees what is and is not an appropriate use of blogging and social networking sites, many just have blanket bans on various forms of Internet speech.[114] Furthermore, current employer liability schemes may actually punish employers who have blogging and social networks policies more than those who do not.[115] These types of employers are unlikely to see

109. *Id.* at 184.

110. *Id.*

111. *Id.* at 183–84.

112. *Id.* at 184–85.

113. *Id.* at 185.

114. For example, "ESPN recently issued 12 guidelines to its employees prohibiting some forms of social networking. On-air talent, reporters, and writers cannot have sports-related blogs or websites, and are required to obtain permission to discuss sports on any social networking site." Lori E. Lesser, *Social Networks and Blogs*, *in* INFO. TECH. L. INST. 2010: OPPORTUNITIES IN CLOUD COMPUTING, BLOGS, BRAND PROTECTION AND TARGETED MARKETING, at 158 (PLI: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROP. COURSE HANDBOOK SER., 2010), *available at* WL 1001 PLI/Pat 101 (citing Richard Sandomir, *ESPN Limits Social Networking*, N.Y. TIMES, Aug. 5, 2009, http://www.nytimes.com/2009/08/05/sports/05espn.html).

115. See below:

> Current labor law leaves substantial uncertainty as to whether employers should create an employee blogging policy. The law states that an employer is liable for employee conduct if the conduct is within the scope of employment. Thus, a company without a formal blogging policy appears to have less to worry about, because that company is not explicitly encouraging blogging activity. The company could argue that any employee blogging activity was not within the scope of employment. Just as the company should not be liable for an e-

blogging and social networking as anything more than a nuisance to the company's well-being; therefore, this solution also fails to find a happy medium between banning all employee Internet speech and completely preventing employers from being able to effectively manage their employees.

C. Decreasing An Employer's Liability for the Internet Speech of Its Employees

Passing legislation to decrease or to eliminate an employer's liability for unlawful comments made by its employees represents another alternative solution to employer-employee Internet speech disputes. Hence, another law review note suggests that making employers less liable for harmful comments their employees post on their personal blogs might alleviate the problems of employee Internet speech.[116] Employers, under this model, should not be held vicariously liable for any speech torts, such as libel or defamation, employees commit through their personal social networking or blogging sites.[117] The note thus proposes that courts encourage employers to draw up blogging policies and develop a more nuanced employer liability scheme than one resulting solely in strict liability for the employer.[118] Nonetheless, it might be unreasonable to expect employers to draw up blogging guidelines for the reasons previously mentioned: spotlighting blogging in this way might actually subject the employer to even more litigation than before the blogging guidelines were put into place.[119] Furthermore, it is unknown whether courts would embrace this more tiered level of employer liability,[120]

> mail sent by a malicious employee, it should not be liable for unauthorized activity beyond its control.

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, 228 (2006) (citations omitted).

116. *Id.* at 232–33.

117. *Id.*

118. *Id.* at 233. For example, the employer, rather than being strictly liable for the employee's blog, could develop an affirmative defense if "(1) the employer exercised reasonable care to prevent illegal activity; and (2) the claimant failed to take advantage of available procedures of the employer that could have reasonably avoided harm." *Id.*

119. *See supra* note 108.

120. "Generally, courts will find vicarious liability for defamatory statements posted by an employee if the 'defamation is referable to the duty owing by the agent to the corporation and was made in the discharge of that duty.'" Pham, *supra* note 115, at 225 (quoting Mars, Inc. v. Gonazalez, 71 S.W.3d 434, 437 (Tex. App. 2002)). Additionally,

> [c]ourts have further extended liability to employee conduct that takes place outside of the company's location or facilities. In *Blakey v. Continental Airlines, Inc.*, the court held that a

regardless of the guidelines employers adopt to encourage a more nuanced view of employer liability for employee Internet speech.

IV. A FRESH APPROACH TO A GROWING PROBLEM: THE STORED COMMUNICATIONS ACT & CASES INTERPRETING IT

A. The SCA

Enacted in 1986, the SCA's meaning has confounded the legal community since it was first introduced.[121] Its general purpose, however, is somewhat clearer: it "offer[s] network account holders a range of statutory privacy rights against access to stored account information held by network service providers,"[122] especially against unwarranted access by the government.[123] Congress's concern for protecting privacy and civil liberties[124] further suggests Congress wanted to protect as much private Internet material as possible from unauthorized access through the SCA. To achieve this goal, Congress chose to regulate both electronic

> company may be held liable for posting harassing statements on an electronic bulletin board, even when the board is not hosted by the company, when the company "knows or has reason to know that such harassment . . . is taking place in the workplace." . . . Accordingly, companies may be held liable for harassment that takes place both in the workplace and in "settings that are related to the workplace."

Id. at 226 (citing Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 552 (N.J. 2000)).

121. Kerr, *supra* note 19, at 1208 (citing Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820–21 (2003)). This confusion has been exacerbated by the fact that, "[d]espite the rapid evolution of computer and networking technology since the SCA's adoption [in 1986], its language has remained surprisingly static . . . [with the] resulting task of adapting the Act's language to modern technology [falling] largely upon the courts." Robison, *supra* note 7, at 1196.

122. Kerr, *supra* note 19, at 1212.

123. *Id. See infra* note 199.

124. "[The] Congress [enacting the SCA] notes its explicit reliance on a report from the Office of Technology Assessment (OTA) prepared in 1985 to review the potential threats to civil liberties resulting from new or emerging technologies." Robison, *supra* note 7, at 1205 (citing H.R. REP. NO. 99-647, at 18 (1986); OFFICE OF TECH. ASSESSMENT, U.S. Cong., OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985)). *See also In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 610 (E.D. Va. 2008) ("Protecting privacy interests in personal information stored in computerized systems, while also protecting the Government's legitimate law enforcement needs, the [Electronic Communications] Privacy Act [18 U.S.C. §§ 2701–03, which contains the SCA] creates a zone of privacy to protect internet [sic] subscribers from having their personal information wrongfully used and publicly disclosed by 'unauthorized private parties.'" (citing S. REP. NO. 99-541 at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557)); *see also AOL*, 550 F. Supp. 2d at 610 ("[T]he Privacy Act protects users whose electronic communications are stored with an internet [*sic*] service provider and reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications stored at such a facility." (citing Theofel v. Farey Jones, 359 F.3d 1066, 1072–73 (9th Cir. 2004))).

communication services (ECS),[125] which transmit electronic materials such as email, and remote computing services (RCS),[126] which simply provide data storage rather than electronic communication like email.[127] Although distinguishing between an ECS and a RCS can be difficult, recent case law has classified social networking sites like Facebook and MySpace as ECS with RCS capabilities.[128]

While the legislative history of the SCA implies websites configured to be private—and thus not accessible to the general public—are to receive the most privacy protection under the SCA,[129] much of the litigation over the SCA's application to Internet communication stems from whether § 2701(c)(2)'s exceptions from SCA liability apply in a particular situation. These exemptions provide that if access to the Internet communication resulted from "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user,"[130] then plaintiffs suing others for allegedly "unauthorized" access will no

125. An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C § 2510(15) (2006).

126. "[T]he term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system." § 2711(2). *See also* § 2510(14) ("'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.").

127. Robison, *supra* note 7, at 1205.

128. "[A] harmonized reading of *Konop*, *Theofel* and *Quon* leads to the conclusion that Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic storage." Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010). "In the alternative, the court holds that the Facebook and MySpace are RCS providers as respects the wall postings and comments." *Id.* at 990. The *Crispin* court explained the RCS analysis by analogizing the Facebook wall posts and MySpace comments to videos posted by users on YouTube, which *Viacom Int'l, Inc. v.YouTube, Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008) found YouTube to be "an RCS provider because it provided storage services for the user, i.e., it stored the video on a web page for the benefit of the user and those the user designates." *Crispin*, 717 F. Supp. 2d at 990.

129. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002) (quoting S. REP. NO. 99-541, at 35–36 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3559 ("This provision [the Stored Communications Act] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public." (omission in original))). *See also id.* ("describ[ing] the [House] Committee's understanding that the configuration of the electronic communications system would determine whether or not an electronic communication was readily accessible to the public") (referring to H.R. REP. NO. 99-647, at 41, 62–63 (1986)).

130. 18 U.S.C. § 2701(c)(2) (2006). In other words, social networkers and bloggers cannot use the SCA against anyone they gave permission to view the content of their social network or blog website, even if that authorized person shows the content to an unauthorized person. *Cf. Konop*, 302 F.3d at 880; Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009); *infra* notes 174, 180–82 and accompanying text.

longer have a cause of action under the SCA. The following cases attempt to establish when and how that exception applies.

B. Cases Interpreting the SCA

In *Devine v. Kapasi*,[131] Devine sued his former business partner under the SCA[132] for illegally accessing a password-protected server both partners had access to until Devine gained sole ownership over the server.[133] Devine's ex-partner used his old password to access the server, which was now part of Devine's solo company, Devine Solutions,[134] and deleted and transferred electronic files on the server after the ownership of the server was transferred exclusively to Devine.[135] Devine claimed that his server was an ECS,[136] and thus protected by the SCA, because the server "provide[d] authorized users with the ability to transmit and receive electronic communications by on-site or remote access, through password protected accounts—including . . . the ability to send and receive e-mail."[137] The defendant moved to dismiss the claim, arguing that he did not violate the SCA because the SCA only prevents unauthorized access to ECSs,[138] and the server could not be described as such a service.[139]

---

131. 729 F. Supp. 2d 1024 (N.D. Ill. 2010).

132. See below:

> [A]ny "aggrieved" party may bring a civil action against a defendant who "intentionally accesses without authorization" or "intentionally exceeds an authorization to access" a "facility through which an electronic communications service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."

Id. at 1026 (quoting 18 U.S.C. § 2701(a)(1)-(2) (2006) (the SCA)) (omission in original).

133. *Id.* at 1025.

134. *Id.* Devine Solutions "comprises computers, servers, and remote access equipment secured by password-protected accounts." *Id.*

135. *Id.* at 1026. After the server was transferred solely to Devine, his "investigation . . . revealed that . . . more than 2000 files and 350 file folders containing electronically stored information and communications were deleted or otherwise transferred from the Devine Solutions network—but not by Devine or anyone working under his direction." *Id.*

136. The SCA applies to an electronic communications service, which is "'any service which provides to users thereof the ability to send or receive wire or electronic communications.'" *Id.* (quoting § 2510(15), (12) and citing § 2711).

137. *Id.* at 1027.

138. *Id. See supra* note 136 for ECS definition.

139. The defendant claimed the server was not an ECS because it did not provide "an electronic communication service to the public." *Id.* He arrived at this conclusion because Devine Solutions, and thus the server, "merely provides . . . technological support for its customers . . . as opposed to . . . 'independently' providing internet [sic] services to their customers.'" *Id.* To make this argument, the defense relied on *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998), which held that the unauthorized disclosure of emails found in a company's internal email service did not violate the SCA. *Devine*, 729 F. Supp. 2d at 1027. Andersen had sued UOP for providing the *Wall Street*

Ruling that the server was an ECS, the court held a claim arises under § 2701 of the SCA when, "as here, a plaintiff pleads that it stores electronic communications on its own systems, and that a defendant intentionally and without authorization got hold of those stored communications through the plaintiff's electronic facilities."[140] Stated otherwise, the court noted that § 2701 does not state that a company must provide an ECS to the public to be covered under § 2701.[141] Rather, the court observed that "no court of appeals has held that § 2701 applies only where the plaintiff is 'in the business' of providing an electronic communication service 'to the public.'"[142]

The defendants in *Kaufman v. Nest Seekers, LLC*,[143] made a similar argument, claiming the plaintiff did not have a cause of action under the SCA because the plaintiff's website, a password-protected electronic bulletin board,[144] was not an electronic service provider and rather "simply a database website that limits access and affords subscribers a place to store information on the Website's server."[145] Yet once again, the court here denied the defendants' motion to dismiss the plaintiff's SCA claim.[146] It determined the website was an electronic service provider qualifying for SCA protection because (1) only paying subscribers, rather than the

---

Journal with emails written by Andersen employees, claiming such conduct violated § 2702 of the SCA: "a person or entity providing an electronic communications service *to the public* shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." *Devine*, 729 F. Supp. 2d at 1027 (quoting 18 U.S.C. § 2702(a)(1) (2006)) (emphasis in the original). But because the company's internal email service "did not 'provide . . . an electronic communication service to the public'" and UOP "was not 'in the business of providing electronic communications services,'" the court dismissed the SCA claim. *Devine*, 729 F. Supp. 2d at 1027 (quoting *Andersen Consulting*, 991 F. Supp at 1043).

140. *Devine*, 729 F. Supp. 2d at 1028 (citing Expert Janitorial, LLC v. Williams, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010)).

141. *Devine*, 729 F. Supp. 2d at 1027–28. While a § 2702 wrongful disclosure claim does require that an ECS be provided to the public, *see supra* note 139, and was dispositive of the plaintiff's § 2702 claim in *Andersen Consulting*, 991 F. Supp. at 1043, this requirement does not bleed over into a § 2701 unauthorized access claim. *See supra* note 132.

142. *Devine*, 729 F. Supp. 2d at 1028. However, the court concedes that "there is some disagreement within and between the district courts as to whether § 2701 can apply to a private employer that is not 'in the business' of providing an electronic communication service 'to the public.'" *Id.* (citing several conflicting district court opinions on the matter).

143. No. 05 CV 6782(GBD), 2006 WL 2807177 (S.D.N.Y. Sept. 26, 2006).

144. *Id.* at *1 (citing Compl. ¶ 22 ("Each . . . subscriber is assigned a non-sharable private member name and password which is used to login to access each subscriber's personal, private, and confidential account")).

145. *Id.* at *3. Additionally, an electronic—or computer—bulletin board "'is a computer program that simulates an actual bulletin board by allowing computer users who access a particular computer [or in the current era, a particular website] to post messages, read existing messages, and delete messages.'" *Id.* at *5 (quoting United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990)).

146. *Id.* at *6.

general public, could access the website, (2) the website's users—mostly real estate professionals—could send listings through the website to customers and colleagues, and (3) users could also send emails directly to other users through the website.[147] Moreover, the court emphasized that in order for an electronic bulletin board to be protected under the SCA, its owner must limit access to the bulletin board to a select group of people. Consequently, such websites available to the public at-large would not merit SCA protection.[148]

Viacom International, Inc. v. YouTube, Inc.,[149] similarly followed the rationale of *Devine* and *Kaufman* by holding Viacom could not gain access to YouTube user videos the users had designated as private, thereby restricting access by the general public.[150] Viacom wanted access to these private videos as part of its lawsuit against YouTube for posting, and allowing others to post, copyrighted material on the YouTube website without Viacom's permission.[151] In ruling for YouTube, the court noted that nothing in the SCA "can fairly be construed as a grant of permission from users to reveal to [Viacom] the videos that they have designated as private and chosen to share only with specified recipients."[152]

However, *Snow v. DirecTV, Inc.*,[153] reverses the trend of the previous cases: it struck down a website owner's SCA claim against a group of people who accessed his site,[154] even though they were explicitly prohibited from entering the site.[155] The court reasoned that if a person

147. *Id.*

148. *Id.* at *5 (citing Snow v. DirecTV, Inc., 450 F.3d 1314 (11th Cir. 2006)). That case found that an "Internet website which operated an electronic bulletin board was not protected under the Stored Communications Act because it was not configured in some way so as to limit access by the general public." *Id.* (describing *Snow*'s holding).

149. 253 F.R.D. 256 (S.D.N.Y. 2008).

150. *Id.* at 264–65.

> YouTube.com users may override the website's default setting—which makes newly added videos available to the public—by electing to mark as "private" the videos they post to the website. Plaintiffs [Viacom] move to compel production of copies of all those private videos, which can only be viewed by others authorized by the user who posted each of them . . . .

Id. at 264.

151. *Id.* at 262–63, 264–65.

152. *Id.* at 265.

153. 450 F.3d 1314 (11th Cir. 2006).

154. The plaintiff created a website "as a 'private support group' website for 'individuals who have been, are being, or will be sued by any Corporate entity.'" *Id.* at 1316. The plaintiff claimed several DirecTV employees, explicitly prohibited from accessing the site, entered the website in violation of the SCA. *Id.*

155. *Id.* at 1319 (striking down the plaintiff's SCA claim). The plaintiff argued defendant DirecTV violated the SCA by accessing his electronic bulletin board website because its homepage "expressly forbids access by DIRECTV and its agents." *Id.* at 1316. Furthermore, a person must affirm that he is not affiliated with DirecTV by clicking "I Agree to these terms" before he "may enter into,

who "ignor[es] an express warning, on an otherwise publicly accessible webpage" is ruled to have violated the SCA, the frequency of SCA litigation would unnecessarily increase and "the merely curious would be prosecuted."[156] The court arrived at this conclusion by looking at the text of the SCA, § 2511(2)(g), which states, "It shall not be unlawful . . . for any person—(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is *readily accessible to the general public*."[157]

While *Snow* could be read as merely an outlier case not in line with mainstream reasoning on this issue, it actually fits in well with *Devine*, *Kaufman*, and *Viacom* when one considers each case's suggestions about the proportional relationship between the strength of a website's privacy settings and the amount of protection a website receives under the SCA. In *Devine* and *Kaufman*, only users with user names and passwords approved by the companies owning the respective websites could access the sites.[158] Similarly, in *Viacom*, only YouTube users who had received explicit permission from the owner of videos labeled "private" could see such videos.[159] Yet in *Snow*, the court emphasized that potential users could access the website by registering under any name and creating any password—without approval of the website's owner—as long as they checked the box agreeing they were not associated with DirecTV.[160] The court thus distinguished *Snow* from *Konop*, to be discussed *infra*, by pointing out "Konop's website . . . required users wishing to view the [website's] contents to have knowledge (an eligible employee's name) that was not publicly available," whereas Snow's website did not require users to possess such "private" information to gain access to his website.[161]

Consequently, these four cases establish that in order for a plaintiff to successfully make an SCA claim against a person accessing his or her website without authorization, he must ensure that the website is truly "private." In other words, a website owner making an SCA claim must ensure that users can only access the site upon receiving access

---

view, and participate in the electronic bulletin board." *Id.* Conversely, a person who clicks "I do not agree to these terms" cannot enter the site. *Id.*

156. *Id.* at 1321.

157. *Id.* at 1320 (quoting 18 U.S.C. § 2511(2)(g) (2006)) (emphasis in the original).

158. *See Devine*, 729 F. Supp. 2d at 1025; *Kaufman*, 2006 WL 2807177 at *6.

159. *See Viacom*, 253 F.R.D. at 264–65.

160. *Snow*, 450 F.3d at 1322.

161. *Id.*

information or approval from the owner or poster that is not available to the general public.

V. APPLYING THE SCA TO EMPLOYER-EMPLOYEE INTERNET SPEECH DISPUTES: *KONOP* & *PIETRYLO*

In *Konop v. Hawaiian Airlines, Inc.*,[162] an airline pilot sued his supervisors under the SCA, alleging they had looked at his password-protected website without authorization and divulged information found on the website to others.[163] Konop's website required people to enter a user name and password before they could gain entry to the contents of the site.[164] After creating an exclusive list, predominated by fellow Hawaiian Airlines employees, of those who could enter the site, Konop let people on that list enter the site by entering their pre-approved names and creating passwords.[165] Upon gaining access to the site after clicking the "SUBMIT" button, the user also implicitly agreed to the website's terms of use, prohibiting "any member of Hawaiian's management from viewing the website and prohibited users from disclosing the website's contents to anyone else."[166] A vice president of Hawaiian Airlines, a member of the management group explicitly prohibited from viewing the website under its terms of use, asked a pre-approved employee—who had never personally logged on to Konop's website—if he could use the employee's name to access Konop's website.[167] The vice president explained to the employee that he wanted to see Konop's website because "he was concerned about untruthful allegations that he believed Konop was making on the website."[168] The employee agreed, and the vice president used the employee's name to access the website several times.[169]

Upon finding that no violation of the SCA occurs if an authorized user, such as the pre-approved employee, facilitates access for a non-authorized user, like the vice president,[170] the district court granted Hawaiian

162. 302 F.3d 868 (9th Cir. 2002).
163. *Id.* at 872–73.
164. *Id.* at 872.
165. *Id.*
166. *Id.* at 872–73.
167. *Id.* at 873.
168. *Id.* Despite the management's concern about the comments Konop made on his website, the case does not mention any adverse employment action taken against Konop for those comments. *Id.*
169. *Id.*
170. See Below:

> The SCA makes it an offense to "intentionally access[] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[] . . .

Airlines' motion for summary judgment on the SCA claim.[171] Yet the Ninth Circuit reversed, concluding that because one of the employees who provided the vice president access to Konop's website was not a "user" as defined by the SCA, that employee did not have the legal authority to grant the vice president authorized access; therefore, the SCA's liability exception was inapplicable.[172] Since "§ 2701(c)(2) allows a person to authorize a third party's access to an electronic communication if the person is (1) a 'user' of the 'service' and (2) the communication is 'of or intended for that user,'" the Ninth Circuit reasoned that a non-"user" cannot grant access to a third party under the SCA.[173] Stated otherwise, an employee who, despite being authorized to use Konop's site, never actually logged on to and used the website, is not considered a "user" of the website. Thus, since one must first be a "user" to satisfy the first prong of the § 2701(c)(2) SCA liability exception, the employee does not qualify and therefore could not grant access to the vice president without violating the SCA.[174]

By negative implication, *Konop* suggests that an employer not granted authorized access to an employee's website can still view the website and avoid SCA liability by having another employee (1) with authorized access and (2) who actually views/uses the website show the employer the

---

> access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a)(1). The SCA excepts from liability, however, "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). The district court found that the exception in § 2701(c)(2) applied because [the employees] consented to [the vice president's] use of Konop's website. It therefore granted summary judgment to Hawaiian on the SCA claim.

Id. at 879 (citing various parts of § 2701) (omissions in original).

171. *Id.*

172. *Id.* at 880.

173. "A 'user' is 'any person or entity who—(A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use.'" *Id.* (citing 18 U.S.C. § 2510(13) (2006)).

174. *Id.* at 880. The Ninth Circuit conceded that legislative history reveals that "Congress believed 'addressees' or 'intended recipients' of electronic communications would have the authority under the SCA to allow third parties access to those communications." *Id.* (citing H.R. REP. NO. 99-647, at 66–67 "(explaining that 'an addressee [of an electronic communication] may consent to the disclosure of a communication to any other person' and that '[a] person may be an 'intended recipient' of a communication . . . even if he is not individually identified by name or otherwise')" (alterations in original)). However, the Ninth Circuit declined to classify the employee as a "user" because it could not find any evidence that the employee ever logged on to Konop's website. *Id.* Furthermore, it criticized the district court for not even investigating whether the employee used the website: the district court "simply assumed that [the employee], by virtue of being eligible to view the website, could authorize [the vice president's] access." *Id.* The Ninth Circuit took issue with this analysis because "it essentially reads the 'user' requirement out of § 2701(c)(2)" and contradicts the statute's plain language utilization of "use," which Webster's Dictionary defines as "'to put into action or service, avail oneself of, employ.'" *Id.* (citing Webster's at 1299).

website.[175] However, when a district court in New Jersey faced this exact situation, it still struck down an employer's motion for summary judgment and found that the plaintiff-employee could have a viable SCA claim against the employer.[176] In *Pietrylo v. Hillstone Restaurant Group*,[177] an employee sued his managers under the SCA alleging that they "accessed the Spec-Tator (a chat group [run by the employee] on MySpace.com, accessed by invitation and then the members' MySpace accounts and passwords) without authorization on five occasions."[178] The managers claimed their access was authorized because an authorized user—a fellow restaurant employee—both showed the website to the managers and provided them with her MySpace log-in information to access the employee's MySpace.com chat group.[179]

Nevertheless, the court denied, as a matter of law, the manager-defendants' motion for judgment, determining that a jury could have reasonably concluded that the pressured employee who provided her log-in information to the managers never really "authorized" them to access the private site and that the website owner had a viable SCA claim against the managers.[180] The court arrived at this conclusion by finding that a "jury could reasonably infer from [the testimony of the employee who provided the managers with the log-in information that her] purported 'authorization' was coerced or provided under pressure," thus nullifying any authorization she gave to the mangers to view the website.[181] The court also found harmful to the defense the fact that the managers knew access to the website was by invitation only,[182] and that the managers

175. *Konop*, 302 F.3d at 879 (citing various parts of § 2701), 880 (citing 18 U.S.C. § 2510(13) (2006)), 880 (citing H.R. REP. NO. 99-647, at 66–67).

176. Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009).

177. *Id.*

178. *Id.* at *1. The court noted that the plaintiffs were fired from the restaurant, although it is unclear as to why. *Id.* at *4. However, the terminations were a factor in the court upholding the compensatory damages awarded to the plaintiffs by the jury. *Id.* at *4–5.

179. *Id.* at *3.

180. *Id.*

181. *Id.* The employee:

> testified that she felt she had to give her password to [her manager] because she worked at [the restaurant] and for [that particular manager]. She further testified that she would not have given [her manager] her password if he had not been a manager, and that she would not have given her information to other co-workers. Furthermore, when she asked whether she felt that something would happen to her if she did not give [her manager] her password, she answered, "I felt that I probably would have gotten in trouble."

Id. (quoting Transcript of Proceedings at 94–96, *Pietrylo v. Hillstone Restaurant Group*, No. 06-5754 (FSH) (June 10, 2009) (June 10 Transcript)).

182. The court found that "[a] reasonable jury could conclude that these repeated visits to the

continued to visit the website even after the pressured employee expressed concern over giving them access to the website.[183]

Combining the holdings of *Konop* and *Pietrylo*, therefore, leads to the following conclusions about employer liability under the SCA: if the employer either (1) gains unauthorized access to the employee's password-protected blog or social networking website,[184] or (2) coerces an authorized user of the employee's password-protected blog or social networking website to either (a) give the employer log-in information for the employee's private site or (b) show the employer the employee's private site,[185] the employer most likely has violated the SCA. Conversely, an employer can most likely avoid SCA liability if he or she accesses an employee's website (1) that is available to the general public,[186] (2) because the employee gives the employer authorized access to view the website,[187] (3) because an authorized co-worker voluntarily provides his or her log-in information to the employer so the employer could personally

---

Spec-Tator were intentional or purposeful, as opposed to accidental, and that [the] managers knew that they were not authorized to access the contents of the Spec-Tator." *Id.* at *3. The "managers accessed the Spec-Tator on several different occasions, even though it was clear on the website that the Spec-Tator was intended to be private and only accessible to invited members." *Id.*

183. The managers continued to visit the site, even after they realized that the employee "had reservations about having provided her log-in information." *Id.* One of the managers testified he knew the employee "'was very uneasy with the fact that she had given me and the rest of the managers her password,' and that she was worried about the consequences of having provided such information." *Id.*

184. For *Konop*'s description of what constitutes unauthorized access, see *Konop*, 302 F.3d at 879 (citing various parts of § 2701), 880 (citing 18 U.S.C. § 2510(13) (2006)), 880 (citing H.R. REP. NO. 99-647, at 66–67).

185. *See Pietrylo*, 2009 WL 3128420 at *3 (*Pietrylo*'s explanation of how coerced authorization is not authorization for the purposes of the SCA's liability exception).

186. *See Nguyen*, 2009 WL 4730899 at *1–2, discussing how the website in *Nguyen* appeared to be available to the general public. There was no mention in the case of any privacy settings Nguyen put on her MySpace page, and Nguyen made it well known to her co-workers that she had a MySpace page. *Id.*

187. For example, if the employees in *Konop* and *Pietrylo* had invited their employers to view their websites, they would have granted authorized access to their employers and would have no claim against them under the SCA. Additionally, this logic could be extended to deny an employee an SCA claim against an employer who took adverse action against the employee for information the employer saw on the employee's Facebook or MySpace page by virtue of being the employee's "friend" on those websites. Stated otherwise, a court could look at *Konop* and *Pietrylo* and conclude that by "friending" his employer on MySpace or Facebook, the employee granted his employer authorized access to view his MySpace or Facebook page. At this juncture, perhaps the only way an employee could still have an SCA claim against an employer the employee "friended" would be if the employee only granted limited access to his "friend"-employer. Thus, if an employee (1) placed privacy settings on his social networking website, meaning only "friends" could view every section of the site, and (2) the employee only granted the employer authorized access to view, for example, his profile information and not any blog entries written on the site, an employer-"friend" who somehow managed to gain access to an unauthorized section of the employee's page might still have violated the SCA. This idea will be fleshed out further in this Note's discussion of *Crispin v. Christian Audigier, Inc*.

view the website,[188] or (4) because an authorized co-worker voluntarily shows the employer the website.[189]

This logic seems to be predictive of how disputes arising out of password-protected blogs either existing as separate websites or found within social networking sites will be decided. Very few courts, however, have ruled on whether other unique features found within social networking sites—such as wall posts, status updates, notes, pictures, etc.[190]—could also be protected against employer intrusion under the SCA. While *Crispin v. Christian Audigier, Inc.*,[191] discusses discovery requests rather than a wrongful termination Internet speech claim, its determination that the SCA might cover Facebook wall posts and MySpace comments[192] indicates a possible extension of SCA coverage beyond password-protected blogs to Facebook wall posts and MySpace comments made by users with privacy settings placed on their profiles.

VI. *CRISPIN*: POSSIBLE EXTENSION OF *KONOP* & *PIETRYLO* BEYOND BLOGS TO FACEBOOK WALL POSTS & MYSPACE COMMENTS

The *Crispin* defendants subpoenaed information located on the plaintiff's MySpace and Facebook pages to gather information for their

188. *See supra* notes 170, 173, 174, and 181–84. If the *Konop*-authorized employee had actually used the website, and qualified as a user under the SCA, he could have granted authorized access to the employer and the website owner would not have a SCA claim against the employer. *See Konop*, 302 F.3d at 879 (citing various parts of § 2701), 880 (citing 18 U.S.C. § 2510(13) (2006)), 880 (citing H.R. REP. NO. 99-647, at 66–67). Similarly, had the *Pietrylo* employee given the employer her log-in information voluntarily, rather than out of fear of being reprimanded, she could have granted authorized access to the employer and the website owner would not have a SCA claim against the employer. *See Pietrylo*, 2009 WL 3128420 at *3.

189. If the *Pietrylo* employee had voluntarily shown the employer the website, the website owner would not have an SCA claim against the employer. *See Pietrylo*, 2009 WL 3128420 at *3. Had an SCA claim arisen in *Nguyen*, *see Nguyen*, 2009 WL 4730899 at *1-2, the fact that an authorized co-worker voluntarily showed the employer Nguyen's MySpace page would also prevent Nguyen from making such a claim. *Id.* Likewise, the plaintiff in *Synder* would not have a SCA claim against her employer because an authorized user voluntarily showed the plaintiff's employer the plaintiff's MySpace page. Snyder v. Millersville Univ., No. 07-1660, 2008 WL 5093140, at *6 (E.D. Pa. Dec. 3, 2008).

190. Social networking sites like Facebook allow users to post status updates (basically a sentence or two describing what the user is doing or how the user is feeling at a particular moment), wall posts (short messages users write on other users' "walls" that are typically visible to all the user's friends, thus distinguishing wall-posts from "private messages," which only the intended recipient can view), and notes (basically journal-like entries written by the user that are typically visible to the user's friends). *See generally Facebook's "About" Page*, FACEBOOK.COM, http://www.facebook.com/facebook?sk=info (last visited Jan. 2, 2012).

191. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

192. *Id.* at 991.

copyright infringement lawsuit.[193] This information included private messages sent via Facebook and MySpace,[194] Facebook wall postings, and MySpace comments.[195] The plaintiff sought to quash the subpoena, arguing the SCA prohibited Facebook and MySpace from disclosing any of the plaintiff's information to the defendants without the plaintiff's permission.[196] The defendant argued that he should at least be able to subpoena the Facebook wall postings and MySpace comments because they generally can be seen by anyone with an account to Facebook or MySpace and "access to the user's profile page"; stated otherwise, he claimed such communications are not private and thus fall outside the scope of the SCA's protections.[197]

On the subpoena issue, the court held (1) private messages and webmail "are inherently private such that stored messages are not readily accessible to the general public," thus meriting SCA protection, and (2) that, regarding the Facebook wall postings and MySpace comments, the case should be remanded back to the magistrate judge "to develop a fuller evidentiary record regarding [the] plaintiff's privacy settings and the extent of access allowed to his Facebook wall and MySpace comments."[198] The court thus determined that the SCA's overall purpose[199] prevents the disclosure of not only private Facebook and MySpace messages, but also Facebook wall postings and MySpace comments if the plaintiff placed privacy settings on his social networking pages to prevent the general public from viewing those wall postings and comments.[200]

---

193. *Id.* at 968–69.

194. *Id.* at 976 (citations omitted) ("Facebook and MySpace, Inc., are companies which provide social networking websites that allow users to send and receive messages . . . through private messaging services"). In other words, Facebook and MySpace private messages are similar to email Webmail services like Gmail or Yahoo.

195. *Id.* at 991.

196. *Id.* at 969.

197. *Id.* at 976–77.

198. *Id.* at 991.

199. See below:

> The SCA prevents "providers" of communication services from divulging private communications to certain entities and individuals. . . . It "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." . . . First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers. 18 U.S.C. § 2703. "Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute [§ 2703] confers greater privacy protection." . . . Second, the statute limits the rights of an Internet Service Provider ("ISP") to disclose information about customers and subscribers to the government voluntarily. 18. U.S.C. § 2702.

Id. at 971–72 (quoting Kerr, *supra* note 19, at 1212–13).

200. *Id.* at 991.

The court arrived at these conclusions by first noting that prior judicial decisions analyzing the legislative history of the SCA[201] support the conclusion that all email-like functions, even those done through social networking sites like MySpace and Facebook, are subject to the restrictions of the SCA.[202] With the Facebook wall postings and MySpace comments, however, the court had to be a little more creative in determining the applicability of the SCA. It first determined that the wall postings and comments were not strictly public because they can be viewed only by fellow social networking users selected by the owner of the wall postings and comments.[203] This conclusion allowed the court to compare the wall postings and comments to "private electronic bulletin board services ('BBS')," which Congressional history and judicial precedent reveal as being subject to the SCA.[204] Next, the court interestingly commented that the number of approved users who have access to the wall postings and comments—whether it be ten or half a million people—was irrelevant in determining whether the owner of the postings and comments intended them to be private and thus equivalent to the private BBSs protected by the SCA.[205] Rather, the plaintiff's

201. *Id.* at 979. "Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards." *Id.* (quoting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002), which surveyed the meaning of the congressional intent behind the SCA).

202. "[A] 'provider of e-mail services' [is] 'undisputedly an ECS.'" *Id.* (citing Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008), *rev'd on other grounds sub nom*. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010).

203. *Id.* at 980. Facebook and MySpace users will probably need to adjust their privacy settings to prevent the public at-large from being able to view their wall postings and comments, depending on whether the default settings for these social networking sites make such wall postings and comments available to everyone until users alter their privacy settings. *See supra* note 91.

204. *Id.* at 980–81. "Court precedent and legislative history establish that the SCA's definition of an [electronic communications system] provider was intended to reach a private BBS." *Id.* at 981 (citing, e.g., United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); *Konop*, 302 F.3d at 875; Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 462 (5th Cir. 1994); Kaufman v. Nest Seekers, LLC, No. 05 CV6782 (GBD), 2006 WL 2807177 at *5 (S.D.N.Y. Sept. 26, 2006); Inventory Locator Service, LLC v. Partsbase, Inc., No. 02-2695 MA/V, 2005 WL 2179185, at *24 (W.D. Tenn. Sept. 6, 2005)).

Cf. id. (quoting S. Rep. NO. 99-541, at 36, 1986 U.S.S.C.A.N. 3555, 3590) (emphasis added):

> "The bill [the SCA] does not for example hinder the development or use of 'electronic bulletin boards' or other similar services where the availability of information about the service, and the readily accessible nature of the service are widely known and the service does not require any special access code or warning to indicate that the information is private. *To access a communication in such a public system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider.*"

205. *Id.* at 990. "Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing and likely in the anomalous result that businesses such as law firms,

purposeful use of privacy settings to prevent the entire public from viewing his comments and postings was most determinative to the court in deciding whether the plaintiff could quash the subpoena via the SCA.[206]

Although the court did not affirmatively rule on the SCA's extension to Facebook wall postings and MySpace comments, the court's instructions to the magistrate judge imply that the use of any privacy settings—no matter how ineffective they may be—on a social networking site may supply a user a cause of action under the SCA against any other users who access that user's personal page without his or her permission.[207] This scenario, in turn, could plausibly arise in future social networking dust-ups at the office similar to any of the recent terminations stemming from employees posting material to Facebook and MySpace deemed objectionable by their employers.[208] Consequently, cases like *Crispin* could possibly provide these employees with an SCA cause of action against their employers if the employees could prove their employers accessed the objectionable material without the employees' permission.[209]

VII. CONCLUSION: TYING IT ALL TOGETHER

With social media use increasing exponentially every year,[210] employers, employees, and the courts will need to figure out how social media use can exist without disrupting the functioning of the workplace. The courts' currently consistent adherence to the employment-at-will-doctrine, and overall reluctance to support exceptions to the doctrine via invasion of privacy suits in the private sector,[211] mean social networkers must look to other legal doctrines to protect themselves from being fired over their Internet speech. While there is no shortage of solutions to this

---

which may have thousands of employees who can access documents in storage, would be excluded from the statute." *Id.*

206. *Id.* at 991.

> [E]ither the general public had access to plaintiff's Facebook wall and MySpace comments, or access was limited to a few. . . . Because it appears . . . that a review of the plaintiff's privacy settings would definitively settle the question [of whether the SCA applies to the postings and comments], the court . . . remands so that [the magistrate judge] can direct the parties to develop a fuller evidentiary record regarding plaintiff's privacy settings . . . .

Id.

207. *See id.* at 990–91.

208. *See supra* notes 5 and 22.

209. For examples of unauthorized employer access, see *Konop*, 302 F.3d at 879 (citing various parts of § 2701), 880 (citing 18 U.S.C. § 2510(13) (2006)), and 880 (citing H.R. REP. NO. 99-647, at 66–67), and *Pietrylo*, 2009 WL 3128420 at *3.

210. *See supra* notes 2–4 and accompanying text.

211. *See supra* Part II.C.

problem being offered up by legal commentators,[212] each one surveyed in this Note fails to address the problem in a way that balances an employee's desire to engage in social networking with an employer's need to ensure that his company's good image is kept intact.

Therefore, a better solution involves turning to, where applicable, the SCA. Using the SCA in employer-employee Internet disputes, as described throughout this Note, will still provide an employer much latitude in firing employees over blogging or social networking site content the employer finds objectionable. The employer will risk violating the SCA only by basing his decision to terminate an employee on the employer's unauthorized access of the employee's private blog or social networking site. At the same time, the SCA will allow employees who diligently maintain privacy settings on their blogging and social networking sites to finally have a viable claim against their employers for terminating them over private blog or social networking postings. While this proposal will provide only a narrow exception to the general rule that anything an employee posts on-line can lead to his or her termination,[213] it will preserve at least some Internet speech freedom for the private sector employee who takes the proper steps to secure the privacy of his or her blog or social networking site. Such an approach is best suited to protect the interests of both employees and employers, while simultaneously allowing the 21st century communication phenomena known as social networking and blogging to continue flourishing without wreaking havoc on the employer-employee relationship.

Catherine Crane[*]

212. *See supra* Part III.

213. *See supra* Part V, penultimate paragraph.

* B.S. *cum laude* in Journalism (2007), Northwestern University; M.S. in Journalism (2007), Northwestern University; J.D. Candidate (2012), Washington University School of Law. I would like to thank Pauline Kim and Gregory Magarian, Professors of Law, Washington University School of Law, for their helpful insight on my Note topic; my Note editor, Jennifer Freeman, for providing me with excellent feedback throughout my writing process; and my broadcast journalism professors at Northwestern University for instilling in me a life-long passion for all things media. Finally, I would like to especially thank my mother, Martha Crane: without her, none of my past, present or future success would be possible.