2010

Legal Implications of the Use of Social Media: Minimizing the Legal Risks for Employers and Employees

Damian R. LaPlaca

Noah Winkeller

Damian R. LaPlaca & Noah Winkeller*

Legal Implications of the Use of Social Media: Minimizing the Legal Risks for Employers and Employees

Introduction

The explosion of online social media for business purposes has increased the liability risks for employers and employees. The use of technology and social media has raised new workplace issues that require a constant review of employer Internet and email use policies. Many of the workplace issues involve whether the employer had in place a policy covering the use of the technology or social media for business and incidental personal use and whether the employee had a reasonable expectation in the privacy of messages sent or received. What was once verbally discussed in private is now communicated in a way that creates a permanent record, and more often than not is the subject of an email, text, or instant message, all of which can fairly easily be retrieved, printed, forwarded, and made public. In fact, the Supreme Court recently accepted for review *City of Ontario v. Quon*,[1] which addresses whether a California city's SWAT team employees had a reasonable expectation of privacy in personal messages sent via city-owned pagers.[2] In most cases, the adoption and enforcement of the use policy will drive the analysis of whether the employee could reasonably expect his messages to be free of employer scrutiny and otherwise remain a private communication between two (or more) people.

Most employers have adopted policies that govern the use of email and the Internet for business and personal use and state that the employee should expect no privacy in these communications or sites visited. For legitimate business purposes, many employers monitor email communications and websites visited, though not

* Damian LaPlaca is a partner at Donovan Hatem LLP in Boston, Massachusetts. Noah Winkeller is a student at the Northeastern University School of Law. The purpose of this article is to provide general information, rather than advice or opinion. It is accurate to the best of the authors' knowledge as of the date of this article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of retained counsel.

1. 130 S. Ct. 1011 (2009).
2. *Id.*

nearly as many monitor the use of social media.[3] It is by now almost universally recognized that email generated from employer-owned computers is the ownership of the employer and that the employee has no basis to expect that his emails are private communications.[4] The same is true for Internet sites visited by an employee on a company computer.[5] Almost every litigation seeks the smoking gun email, and some employees still have not gotten the message that their careless emails and texts can be found and prominently displayed in a courtroom drama in virtually any kind of civil or criminal trial.[6]

The explosion of social media has intensified the workplace issues relating to the risks of employee computer use. Examples of common social media that are used for business purposes include LinkedIn, Twitter, and Facebook, and the main ways in which social media is used in the business context is for marketing, gathering information, and relationship-building. Though the law on social media is in early stages of development, and the authors found no reported decisions in which an employer was found liable for an employee's use of social media, the use of social media may expose employers and employees to civil and even criminal liability.

3. According to *The Latest on Workplace Monitoring and Surveillance*, Am. Mgmt. Ass'n, Mar. 13, 2008, http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx [hereinafter *Workplace Monitoring*], sixty-six percent of employers monitor employee Internet connections, forty-three percent of employers monitor employee email, and only ten percent of employers monitor employees' use of social media.

4. *E.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (ruling that an employee has no reasonable expectation of privacy when emailing over the company email system despite assurances made by the company that such communications would not be intercepted); Lawyers.com, Employee Privacy in the Workplace, http://labor-employment-law.lawyers.com/human-resources-law/Employee-Privacy-in-the-Workplace.html (stating that generally any email that is sent over an employer's network is accessible to the employer and that an employer may read and make copies of an employee's emails even after they have been deleted).

5. *E.g.*, Lawyers.com, *supra* note 4 (noting that an employee has essentially no right to privacy regarding Internet access over an employer's network using a work computer and that an employer may monitor any Internet activity either at work or whenever connected through the employer's network and keep a record of websites employees visit).

6. *E.g.*, *In re* Parmalat Sec. Litig., 258 F.R.D. 236, 251–52 (S.D.N.Y. 2009) (admitting email chains between governing and advisory board members of Parmalat as evidence despite the defendants' claims that the emails should be protected as minutes and notes from committee meetings); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007) (denying claim that email communications between a party and his attorney were privileged because the emails were sent via the party's employer's network, and the employer had an explicit policy banning personal use of the network); Garrity v. Hancock Mut. Life Ins. Co., No. CIV.A. 00-12143-RWZ, 2002 WL 974676 (D. Mass. May 7, 2002) (granting summary judgment motion for defendant-employer in a wrongful discharge case based on the employer's right to monitor employee's email and the content of the emails in question).

I. Reasonable Expectations of Privacy

A. The Death of Anonymity on the Internet

When the Internet first became a part of mainstream society, many users were attracted by the anonymity it offered. A now famous New Yorker Magazine cartoon published in 1993, which depicted one dog using a computer and remarking to another dog sitting nearby that, "[o]n the Internet, nobody knows you're a dog," captured this attraction perfectly.[7] However, for better or for worse, the era of anonymity on the Internet has now passed.[8]

The analysis of potential liability for users of social media begins with the expectation of privacy, as recovery on the basis of most privacy-based causes of action hinges on whether the user had a "reasonable expectation of privacy."[9] In the employment context, the judicially created reasonable expectation of privacy standard is largely an attempt by courts to balance the privacy rights of employees against the legitimate interests of their employers.[10]

"A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms."[11] Since community norms form the basis for reasonable expectations of privacy, a person's privacy interests will only be protected "relative to the customs of the time and place."[12] Thus, it is not surprising that legally recognized privacy rights associated with the use of the Internet on company computers, whether at the workplace or not,[13] have diminished along with the near-death of anonymity on the Internet and the increased monitoring of employees' computer use.[14] Moreover, it is likely that these

7. Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, New Yorker, July 5, 1993, at 61.

8. *See generally* Tadayoshi Kohno et al., *Remote Physical Device Fingerprinting*, 2 IEEE Transactions on Dependable & Secure Computing 93 (2005) (discussing how to remotely "fingerprint" a computer accessing the Internet without the user's knowledge or permission).

9. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008), *cert. granted*, 130 S. Ct. 1011 (2009) (describing a privacy-based claim under the Fourth Amendment as proving both a "reasonable expectation of privacy" and that "the search was unreasonable"); TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 160 (Cal. Ct. App. 2002) (identifying one prong of a privacy-based claim under the California Constitution as proving "a reasonable expectation of privacy in the circumstances").

10. *See* Ali v. Douglas Cable Commc'ns, 929 F. Supp. 1362, 1383 (D. Kan. 1996) ("'The employer's asserted interest in recording the phone calls 'must be balanced against the degree of intrusion resulting from the employer's methods to obtain the information.'" (quoting Pulla v. Amoco Oil Co., 882 F. Supp. 836, 867 (S.D. Iowa 1994), *aff'd in part and rev'd in part on other grounds*, 72 F.3d 648 (8th Cir. 1995))).

11. *TBG Ins.*, 117 Cal. Rptr. 2d at 160 (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Sup. Ct. Cal. 1994)).

12. *Id.* at 161 (quoting *Hill*, 865 P.2d at 655).

13. *See id.* at 157 (finding no reasonable expectation of privacy when an employee used a laptop provided by his employer in his home for personal use).

14. Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *5 (N.D. Cal. Aug. 27, 2009) (discussing diminished expectations of privacy when using an employer's computing equipment); *Workplace Monitoring*, *supra* note 3 (providing data on the prevalence of employers monitoring employees' computer use).

privacy rights will only diminish further as the remaining opportunities for anonymity on the Internet continue to disappear.[15]

B. Employees' Reasonable Expectations of Privacy

A determination of whether an employee had a reasonable expectation of privacy is a factual, case-by-case analysis.[16] If an employee voluntarily consents to activities that impact his or her privacy interests, he or she is less likely to succeed on a claim based on an invasion of privacy.[17] Similarly, an employee generally will have no expectation of privacy with respect to the use of his or her employer's computing equipment if his or her employer has adopted a computer use policy that reasonably removes any such expectation.[18] In addition, an employee's occupation may also be relevant to a determination of whether he or she had a reasonable expectation of privacy.[19] Other factors commonly analyzed by courts examining employees' reasonable expectations of privacy include: 1) whether the employer maintains a policy banning the computer use in question, 2) whether the employer monitors employees' computer use, 3) whether third parties have a right of access to the computers, emails, or computer files in question, and 4) whether the employee was aware of the employer's applicable use and monitoring policies.[20]

C. Public Employees' Reasonable Expectations of Privacy

Although public employees may appear to enjoy additional privacy protections under the Fourth Amendment, which protects them from unreasonable searches by the government as their employer,[21] reasonable expectations of privacy analyses are

15. *See* Warshak v. United States, 532 F.3d 521, 526–27 (6th Cir. 2008) (discussing permissible government searches and noting that email users' reasonable expectations of privacy in their email communication will shift over time).

16. O'Connor v. Ortega, 480 U.S. 709, 718 (1987) (plurality opinion) ("Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.").

17. *TBG Ins.*, 117 Cal. Rptr. 2d at 160–61.

18. *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257–58 (Bankr. S.D.N.Y. 2005). The *Asia Global* court identified four factors to measure an employee's expectation of privacy in computer files and email. *Id.* at 257. One of the four factors is whether "the corporation maintain[s] a policy banning personal or other objectionable use." *Id.*

19. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 903–04, 907–08 (9th Cir. 2008) (noting that the "operational realities" of the workplace, which include the realities of the particular occupation, impact reasonable expectations of privacy and that occupations that subject employees to frequent public records requests could provide for diminished reasonable expectations of privacy); *TBG Ins.*, 117 Cal. Rptr. 2d at 161 (noting that the expectation must take into account "community norms," including the plaintiff's occupation).

20. *E.g.*, *In re Asia Global*, 322 B.R. at 257.

21. *Ortega*, 480 U.S. at 717 ("[W]e reject the contention made by the Solicitor General and petitioners that public employees can never have a reasonable expectation of privacy in their place at work. Individuals do not

nearly identical regardless of whether an employee is a public- or private-sector employee.[22] This is because public employers have a "direct and overriding interest in ensuring that . . . [their work] is conducted in a proper and efficient manner," and are thus able to conduct searches notwithstanding the Fourth Amendment as long as the measures adopted are "reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."[23] It is also important to note that, as long as a public employer's investigation is not "excessively intrusive," the employer will not be required to utilize a less-intrusive investigative method, even if doing so would allow for a sufficient investigation.[24]

Another important consideration with public employers is applicable public records laws. These laws can diminish a public employee's reasonable expectation of privacy regarding certain computer files and communications, though they may not necessarily have such an effect if public records requests are unlikely or infrequent.[25]

The Supreme Court's decision in the recently accepted *City of Ontario v. Quon*[26] could have huge ramifications for the manner in which public employers adopt and implement computer use policies. If the Supreme Court rules against the City of Ontario, public employers may be more reluctant to monitor their employees' use of technology or may choose to implement and enforce stricter monitoring so as to eliminate any possibility of employees obtaining a reasonable expectation of privacy. In the alternative, if the Supreme Court rules in favor of the City of Ontario, public employers may monitor employees' use of technology more frequently because of a reduced fear of liability.

D. Reasonable Expectations of Privacy with Online Social Media

As common sense suggests, when a person maintains a social media profile that is accessible to the general public, he or she will almost certainly not have a reasonable expectation of privacy with respect to the content on that profile.[27] On the other

lose Fourth Amendment rights merely because they work for the government instead of a private employer."); *cf.* Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989) (discussing employees' Fourth Amendment rights for protection from unreasonable searches conducted by their employer, the United States Customs Service).

22. *See Ortega*, 480 U.S. at 717.

23. *Id.* at 724–26 (alteration in original) (internal quotation marks omitted) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

24. Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989).

25. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 907 (9th Cir. 2008) ("There is no evidence before the [c]ourt suggesting that CPRA requests to the department are so widespread or frequent as to constitute 'an open atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable.'" (alteration in original) (quoting Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001))).

26. City of Ontario v. Quon, 130 S. Ct. 1011 (2009).

27. *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 860–61 (Cal. Ct. App. 2009) (holding that plaintiff could not maintain a cause of action for invasion of privacy or intentional infliction of emotional distress when an article that she posted on MySpace.com was taken by another person and submitted for re-publication in a newspaper).

hand, when a person maintains a "private" social media profile that can only be accessed by people he or she selects, it is unclear whether he or she has a reasonable expectation of privacy with respect to the content on that profile.[28] Regardless of whether or not a person has a reasonable expectation of privacy in the contents of his or her private social media profile, discretion should be exercised in posting content to this profile because "[t]hings go from private to global in a nanosecond in this world,"[29] and it only takes one person to download or forward "private" content for it to become accessible to the general public.[30]

In addition to the relevant privacy setting, a social media website's "Terms of Use" will also impact its users' reasonable expectations of privacy. These Terms of Use generally contain important rules and regulations relating to content posted on the website, including who owns or controls the content, what the owner or controller of the content is authorized to do with it,[31] how long the content will remain on the website (in some cases it may not be able to be permanently deleted and will remain indefinitely),[32] and whether the content will or can be modified by the operator of the website.[33] Violating a website's Terms of Use can lead to civil and, in rare cases, criminal liability. Since Terms of Use can create contractual agreements between websites and their users, users who violate a website's Terms of

28. *Compare* Kathryn L. Ossian, *Legal Issues in Social Networking* at 1-9, April 2009, http://www.millercanfield.com/media/article/200120_LEGAL%20ISSUES%20IN%20SOCIAL%20NETWORKING.pdf (noting that in 2009, a Canadian court held that a plaintiff's Facebook profile was discoverable regardless of the applicable privacy setting that the plaintiff selected), *with* Dionne Searcey, *Employers Watching Workers Online Spurs Privacy Debate*, Wall St. J., Apr. 23, 2009, at A13, *available at* http://online.wsj.com/article/SB124045009224646091.html (quoting Floyd Abram, "First Amendment expert and partner at Cahill Gordon & Reindel LLP," as affirming an employee's right to privacy in "non-work created [electronic] communications with each other" and quoting Lewis Maltby, president of the National Workrights Institute, as stating that "[y]ou can't post something on the Internet and claim breach of privacy when someone sees it").

29. John D. Sutter, *Survey: 15 Percent of Teens Get Sexual Text Messages*, CNN.com, Dec. 15, 2009, http://www.cnn.com/2009/TECH/12/15/pew.sexting.survey/index.html (quoting Bill Albert, the spokesman for the National Campaign to Prevent Teen and Unplanned Pregnancy).

30. *E.g.*, *id.* (reporting on Pew Internet & American Life Project's survey, which found that teens send sexually explicit pictures via text message "only to people with whom they are in a relationship; but those messages are often forwarded to people outside the relationship, especially after a breakup").

31. Twitter, Terms of Service, https://twitter.com/tos (last visited Mar. 23, 2010) ("By submitting, posting or displaying Content . . . you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content . . . .").

32. *Websites 'Keeping Deleted Photos'*, BBC News, May 21, 2009, http://news.bbc.co.uk/2/hi/8060407.stm ("User photographs can still be found on many social media websites even after people have deleted them, Cambridge University researchers have said.").

33. Twitter, *supra* note 31 ("We may modify or adapt your Content in order to transmit, display or distribute it . . . and/or make changes to your Content as are necessary to conform and adapt that Content to any requirements or limitations of any networks, devices, services or media.").

Use can be civilly liable for breach of contract and related claims.[34] Terms of Use violations can also lead to civil liability under the federal Computer Fraud and Abuse Act ("CFAA").[35] In the most notorious example of the potential for criminal liability, a mother, her daughter, and a family friend created a fake MySpace.com account and sent cruel messages to a thirteen-year old girl, who subsequently hung herself.[36] The incident generated a huge amount of publicity, and in its aftermath, the mother was charged with four potential felonies and convicted of three misdemeanors, though these convictions were overturned on a motion for a judgment of acquittal.[37] The district judge overturned the misdemeanor convictions because the statutes on which they were based were overly vague, but in doing so he noted that he would have upheld convictions on the felony charges.[38]

II. POTENTIAL SOURCES OF LIABILITY FROM SOCIAL MEDIA

A. Adverse Employment Actions Based on Online Social Media Profiles

An employer generally will not be liable on the basis of any adverse employment action taken as a result of content posted in a social media profile[39] unless it accesses an actual or potential employee's profile in violation of a website's terms of use, for example, by posing as another person,[40] or by accessing a profile without the freely given consent of the owner.[41] The exception to this rule is if the adverse

34. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 401–04 (2d Cir. 2004) (upholding the district court's award of a preliminary injunction on a breach of contract claim based on the plaintiff's likelihood of success that the terms of use on its website created a contractual relationship with defendant, who used plaintiff's website daily).

35. 18 U.S.C. § 1030 (2006); *see* Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 438–40 (N.D. Tex. 2004) (denying motion to dismiss claims under the CFAA because the defendant was potentially liable under the CFAA for unauthorized access to a computer on the basis of its violations of the terms of use of the plaintiff's website).

36. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

37. *Id.* at 468.

38. Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED, July 2, 2009, http://www.wired.com/threatlevel/2009/07/drew_court/ ("[District court Judge] Wu told Assistant U.S. Attorney Mark Krause that if Drew had been convicted of the felonies, he would have let the convictions stand . . . . But the misdemeanor convictions troubled him, because of the vague wording of the statute.").

39. *See, e.g.*, Spanierman v. Hughes, 576 F. Supp. 2d 292, 297–99 (D. Conn. 2008) (granting summary judgment to defendant-employer in a suit filed by an employee who was terminated for his use of MySpace.com).

40. *E.g.*, MySpace.com, Terms of Use Agreement, June 25, 2009, http://myspace.com/index.cfm?fuseaction=misc.terms ("When you sign up to become a Member . . . . [y]ou agree not to use the account, username, email address or password of another Member at any time or to disclose your password to any third party.").

41. A federal jury found Houston's Restaurants violated the federal Stored Communications Act, 18 U.S.C. §§ 2701–11 (2006), when Houston's Restaurants managers accessed a private MySpace.com chat group created by one of their employees to complain about Houston's management. Pietrylo v. Hillstone Rest. Group, *Pietrylo II*, No. 06-5754 (FSH), 2009 WL 3128420, at *1 (D.N.J. Sept. 25, 2009). The jury further found that defendant-employer's actions were malicious and thus awarded punitive damages. *Id.* Plaintiff was a Houston's Restaurant

employment action violates a contractual provision or is taken on the basis of an individual's protected status or protected activities.[42] For example, if an employer learned a job applicant was disabled after viewing his or her social media profile and did not hire him or her for this reason, this would be unlawful.[43] Since employers have almost complete carte blanche to examine social media profiles, and recent studies indicate that forty-five percent of employers research social media websites to screen job applicants[44] and sixty-six percent of employers monitor the Internet connections of current employees,[45] individuals should never post anything they do not want employers to see.

B. Using Social Media Profiles in Investigations

Social media profiles are a great source of information about individuals and entities, and, thus, it is not surprising that people—including lawyers, investigators, and potential business partners—searching for information will utilize them.[46] Though it may give rise to ethical issues in certain scenarios, this use is perfectly legal as long as the Terms of Use of a social media website are not violated when information is obtained.[47]

---

employee who established a private chat group, accessible by invitation only, on MySpace.com for the purpose of complaining about Houston's. Pietrylo v. Hillstone Rest. Group, *Pietrylo I*, No. 06-5754 (FSH), 2008 WL 6085437, at *1 (D.N.J. July 25, 2008). Plaintiff invited another employee, Karen St. Jean, to the chat group, who then showed the site to a manager. *Id.* The court found that Houston's obtained the password from St. Jean without her "freely given" consent. *Pietrylo II*, at *3. Various managers accessed the chat group on multiple occasions, resulting in Houston's terminating two employees for what it considered were "offensive" posts. *Pietrylo I*, at *2. While this may be viewed as a warning to employers, the jury, interestingly, found that Houston's did not violate the plaintiff-employees' common law right of privacy and found that the employees did not have a reasonable expectation of privacy. *Pietrylo II*, at *1.

42. *See generally* U.S. Equal Employment Opportunity Commission, Federal Laws Prohibiting Job Discrimination Questions and Answers, http://www.eeoc.gov/facts/qanda.html (last visited Apr. 18, 2010).

43. *See generally* Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12111–12117 (2006).

44. *45% Employers Use Facebook-Twitter to Screen Job Candidates*, Or. Bus. Rep., Aug. 24, 2009, http://oregonbusinessreport.com/2009/08/45-employers-use-facebook-twitter-to-screen-job-candidates/.

45. *Workplace Monitoring*, *supra* note 3.

46. *See* Ossian, *supra* note 28, at 1-8 to 1-9 (discussing the use of social media information by lawyers and jury consultants).

47. *Cf.* Sw. Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004).

C. Common Grounds for Liability Based on Social Media

Anyone who posts content such as text, video, audio, or pictures onto a social media website is considered an "information content provider" under federal law[48] and can be subject to liability on the basis of that content under state or federal law.

The most common grounds for liability on the basis of social media are likely to be copyright infringement and defamation. Copyright infringement is the unauthorized use or reproduction of copyrighted content.[49] Certain uses of copyrighted content, including the use of such content for a parody or for teaching or research purposes, are allowed under the law as a "fair use," even if permission to use the content is not obtained.[50] However, the line between fair use and copyright infringement is blurry, and it is thus best to err on the side of caution and obtain permission before using or reproducing copyrighted content.[51] This is particularly important because material posted on a social media website may remain available indefinitely for others to view or reproduce,[52] and copyright holders can be surprisingly aggressive when combating copyright infringement.[53]

Defamation is the writing (libel) or uttering (slander) of a false statement of fact about a person or entity that harms his, her, or its reputation.[54] One of the two most common defenses to defamation is truth.[55] However, in situations in which the facts disclosed are not newsworthy and would be highly offensive to a reasonable person, the defense of truth will bar liability for defamation but not for other privacy-based tort claims brought on the basis of the same statements.[56] The second common defense to a defamation suit is that the statement was a statement of opinion.[57]

48. 47 U.S.C. § 230(f)(3) (2006) ("The term 'information provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.").

49. *See also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991) (discussing fundamental copyright law issues). *See generally* Copyright Act, Pub. L. No. 94-553, 90 Stat. 2541 (1976) (codified as amended in scattered sections of 17 U.S.C.).

50. 17 U.S.C. § 107 (2006); Salinger v. Colting, 641 F. Supp. 2d 250, 256–58 (S.D.N.Y. 2009) (discussing the distinction between satires and parodies, the latter of which qualifies as fair use).

51. *E.g.*, United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1121 (N.D. Cal. 2002) ("There is no bright line test for determining whether any particular use is a 'fair use' or is instead an act of copyright infringement, and each use requires a case-by-case determination.").

52. *Websites 'Keeping Deleted Photos'*, *supra* note 32.

53. *See, e.g.*, Getty Images, Policy on Unauthorized Use (Updated), http://contributors.gettyimages.com/article.asp?article_id=889 (last visited Apr. 13, 2010) (setting forth a stern warning that Getty Images diligently monitors and pursues incidents of infringement).

54. *See generally* New York Times Co. v. Sullivan, 376 U.S. 254 (1965) (seminal case on libel).

55. *Id.* at 267 ("Once 'libel per se' has been established, the defendant has no defense as to stated facts unless he can persuade the jury that they were true in all their particulars.").

56. *See generally* RESTATEMENT (SECOND) OF TORTS § 652D (1977) (describing the tort of "Publicity Given to Private Life").

57. Ollman v. Evans, 750 F.2d 970, 976–81 (D.C. Cir. 1984) (en banc) (explaining that opinion statements enjoy First Amendment protection from defamation claims because opinions cannot be proven false).

However, this will not be a successful defense if the statement was asserted as a fact.[58]

There are many other possible grounds for liability on the basis of the use of social media, with the most likely of these being sexual harassment, criminal threats, intentional infliction of emotional distress, unauthorized releases of customer or company information, professional malpractice, software piracy, violations of securities laws,[59] and interference with prospective or contractual economic relationships. The unauthorized release of customer or company information is particularly important for employers to be watchful for because it is frighteningly common, as a survey in the United Kingdom found that one in three people had seen sensitive company information posted on social media websites.[60]

While most of the grounds for liability mentioned are self-explanatory, interference with prospective or contractual economic relationships merits further explanation. Interference with prospective economic relations is the wrongful interference with a business relationship between two or more third parties that has a probability of resulting in future economic benefits,[61] while interference with contractual economic relations is the wrongful interference with performance under a contract existing between two or more third parties.[62] The most probable way either tort would arise through social media is if a person used a social media website to spread false rumors that damaged a party's prospective or contractual business relationships.[63]

D. Other Negative Consequences

In addition to civil and criminal liability and adverse employment actions, the most common negative consequences for employers and employees stemming from the use of social media are the loss of business, a damaged reputation, or a damaged business relationship.

---

58. *Id.* at 984 ("If the opinion implied factual assertions, courts have held that it should not receive the benefit of First Amendment protection as an opinion.").

59. Blake A. Bell, *Reducing the Liability Risks of Employee Misuse of the Internet*, June 30, 1999, http://www.stblaw.com/content/publications/pub269.pdf (noting that postings on the Internet "can lead to unwitting disclosures that are materially inaccurate," thus violating federal securities laws).

60. Press Release, Morse, Twitter and Social Networks Cost UK Businesses (Oct. 26, 2009), *available at* http://www.morse.com/press_20.htm.

61. *E.g.*, Youst v. Longo, 729 P.2d 728, 732–33 & n.6 (Cal. 1987) (discussing the tort of intentional interference with prospective economic advantage).

62. *E.g.*, Mem'l Gardens, Inc. v. Olympian Sales & Mgmt. Consultants, Inc., 690 P.2d 207 (Col. 1984) (discussing the tort of intentional interference with contractual relations).

63. *See, e.g.*, Jennifer Fernicola, *Pet Service Says Former Employee Used Craigslist, Yelp to Defame It*, Chicago Bar-Tender, Feb. 2, 2010, http://www.chicagonow.com/blogs/chicago-bar-tender/2010/02/pet-service-says-former-employee-used-craigslist-yelp-to-defame-them.html#more.

III. Employer Liability on the Basis of Social Media

A. Relevant Factors

The common legal principles of agency should apply to employees' use of social media, and employers may be held vicariously liable, even for punitive damages,[64] on the basis of content posted by their employees. Two key determinants of employer liability on the basis of such content are likely to be whether the content was posted in the scope of the employee's employment and whether the employer had a policy regarding the use of social media.[65] Courts may intertwine these two factors, as the content of an employer's computer use policy may help determine whether the content was posted in the scope of the employee's employment.[66] In the alternative, a court might determine whether the content was posted in the scope of the employee's employment "without regard to whether the [employer] authorized, participated in, or ratified the employee's conduct."[67] If an employer has a policy covering the use of social media, its enforcement of this policy may also be a key factor in determining its potential liability, as discussed further below. While employer liability is more likely when employees post content onto social media websites in the scope of their employment, employers may still be held liable on the basis of such content when it is posted by employees acting outside the scope of their employment.

B. Failure to Monitor Employees

In *Scanlon v. Kessler*, a photographer brought a lawsuit against a non-profit organization and three individuals who had been on its board of directors, partly on the basis of the unauthorized display of his photographs on the organization's website.[68] If the events in this case had occurred more recently, these photographs could easily have been displayed in one of the organization's social media profiles. The organization attempted to remove the plaintiff's photographs from its website;[69] however, since the organization failed to keep track of the sources of its photographs, it inadvertently left two photographs on its website in violation of the

64. *E.g.*, Exxon Shipping Co. v. Baker, 128 S. Ct. 2605 (2008); Embrey v. Holly, 442 A.2d 966, 972–73 (Md. 1982).

65. *Cf.*, Marshall v. Nelson Elec., 766 F. Supp. 1018, 1040 (N.D. Okla. 1991) (noting that whether an employer has a policy relating to sexual harassment is relevant to whether it is liable for the creation of a hostile work environment).

66. *See* Brown v. Mayor, 892 A.2d 1173, 1183–85 (Md. Ct. Spec. App. 2006) (noting the relevance of employer authorization and the possible relevance of employer policies in determinations of the scope of an employee's employment).

67. *Embrey*, 442 A.2d at 969–70.

68. Scanlon v. Kessler, 11 F. Supp. 2d 444, 446 (S.D.N.Y. 1998).

69. *Id.* at 448.

photographer's copyrights.[70] Although the court determined that the infringement of these two copyrights was not "willful," the organization was still liable for copyright infringement because the individual defendants posted the photographs to the website in the scope of their duties as members of the organization's board of directors.[71] Ultimately, the photographer received damages and attorneys' fees.[72]

In *Doe v. XYC Corp.*, an employee posted nude pictures of his ten-year old daughter on child pornography websites using his work computer.[73] Although the employer had no direct knowledge that the employee had been visiting child pornography websites from his office computer, it was aware that the employee had previously viewed pornography while at work.[74] The employee's wife later sued the employer for negligence, and the court reversed the lower court's grant of summary judgment to the defendant-employer.[75] In doing so, the court found that the employer had notice that the employee was viewing child pornography on his work computer prior to when he posted nude pictures of his daughter online.[76] As a result, the court held that the employer had a duty to report this to the proper authorities and to take effective internal action.[77] Because the employer did neither, it was potentially liable for the harm suffered by the employee's daughter.[78]

C. Further Grounds for Liability

An employer may also be found liable for an employee's use of social media in a number of other scenarios, including the following: 1) an employee disseminates spam in an effort to generate business,[79] 2) an employee commits defamation or releases confidential information in the scope of his or her employment,[80] 3) an

70. *Id.*

71. *Id.*

72. *Id.* at 449.

73. Doe v. XYC Corp., 887 A.2d 1156, 1160 (N.J. Super. Ct. App. Div. 2005).

74. *Id.* at 1159–60.

75. *Id.* at 1158.

76. *Id.* at 1166–67, 1169.

77. *Id.* at 1167–68.

78. *Id.* at 1168–70.

79. *See* United States v. Cyberheat, Inc., No. CV-05-457 TUC-DCB, 2007 WL 686678, at *8 (D. Ariz. Mar. 2, 2007) (discussing liability for defendant's affiliates who sent "642 sexually explicit, unconsented to emails" in exchange for over $200,000 in commission).

80. Embrey v. Holly, 442 A.2d 966, 972–73 (Md. 1982) ("[I]t is not error . . . to impose exemplary liability on a master for the defamatory utterances of its servant where the employee acted in the scope of his employment and with knowledge of falsity or reckless disregard for truth."); Mia G. Settle-Vinson, *Employer Liability for Messages Sent by Employees via Email and Voice Mail Systems*, 24 T. Marshall L. Rev. 55, 73–74 (1998) ("[O]ne of the exceptions to immunization from employer liability to third parties lies in the doctrine of respondeat superior . . . .").

employee violates federal securities laws,[81] 4) an employee commits professional malpractice when inadvertently giving advice,[82] 5) an employee posts content that creates a hostile work environment or constitutes sexual harassment,[83] and 6) an employee who was negligently hired or negligently retained commits any kind of wrongful act.[84] The critical lesson from these scenarios is that employers may have a duty to monitor employees' computer use and should take prompt corrective action at the first indication of inappropriate use of computing equipment by employees.

IV. TRADITIONAL COMPUTER USE IN CONTRAST TO SOCIAL MEDIA

A. Social Media Compared to Email

Employers should treat employees' use of social media similar to employees' use of email because the two forms of communication share many liability risks, particularly regarding the disclosure of confidential third-party information and harassment of co-employees and non-employees. However, the use of social media by employees should be monitored more closely than employee email because content on social media websites is more likely to be seen by a greater number of third parties than is content of email, creating greater risk of employer liability with online social media in such areas as copyright infringement and defamation.

B. The Inadequacy of Filtering and Blocking Software

Filtering and blocking software is used by some employers to reduce the ability of employees to access or transmit inappropriate content over the Internet. While this software can be effective, it also has limitations. For one, savvy computer users can circumvent filtering and blocking software, negating its effectiveness.[85] In addition,

81. Bell, *supra* note 59. *But see* Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164, 192 (1994) (holding that §10(b) of the Securities Exchange Act of 1934 does not support private suits against aiders and abettors and only authorizes action against primary violators).

82. *See* Peter H. Geraghty, *Legal Ethics Research: Who You Gonna Call?*, YOUR ABA, Dec. 2008, http://www.abanet.org/media/youraba/200812/article11.html (providing advice on how to avoid creating a lawyer-client relationship when participating in online chat rooms and citing several state bar ethics opinions).

83. *See* Carol Tice, *You've Got Email—And a Lawsuit on Your Hands*, HOME CHANNEL NEWS, Oct. 26, 1998, *available at* http://findarticles.com/p/articles/mi_m0VCW/is_1998_Oct_26/ai_53425670/ (discussing a multi-million-dollar settlement that Chevron made after a group of female employees filed a law suit, alleging Chevron's internal email system was used to transmit sexually offensive messages).

84. Settle-Vinson, *supra* note 80, at 71.

85. *See* Dawn C. Nunziato, *Technology and Pornography*, 2007 BYU L. REV. 1535, 1568 ("[E]ven [using] the best filtering software, minors are frequently able to circumvent such filters with the assistance of information that is readily available on the Internet."); Erin Elizabeth Marks, Comment, *Spammers Clog In-Boxes Everywhere: Will the CAN-SPAM Act of 2003 Halt the Invasion?*, 54 CASE W. RES. L. REV. 943, 948 (2004) (discussing the scourge of unsolicited commercial email and so-called "spammers"'s ability to circumvent internet service providers' filtering software).

this software may fail to prevent employees from viewing certain inappropriate conduct.[86] Furthermore, filtering and blocking software may mistakenly block more content than necessary, restricting legitimate computer use and decreasing productivity.[87] Due to the limitations of filtering and blocking software, employers cannot simply install this software and expect to avoid all liability on the basis of their employees' use of social media. Therefore, even if this software is utilized, an employer should still implement a computer use policy to reduce its risk of liability.

V. Computer Use Policies

A. Purpose

By adapting a computer use policy to include social media, an employer can enjoy the benefits of social media while minimizing the associated risks. Even employers who do not use the Internet or social media in their business create risk if they do not adopt a use policy because employee use of the Internet and social media is so widespread.[88] Carefully drafted computer use policies that distance the employer from inappropriate employee conduct will reduce an employer's risk of liability on the basis of such conduct. In addition, a policy will deter employees from inappropriately using an employers' computing equipment in a way that exposes the employer to potential liability.

Employers that monitor employee computer use enjoy benefits in addition to minimizing the risk of liability. For example, monitoring employees' computer use can increase productivity, ensure company information is kept confidential, and improve performance reviews.[89] However, in the absence of a policy that effectively removes employees' reasonable expectations of privacy with respect to work-related

86. Gemma Jones, *A Web of Confusion, Sex Sites Escape Filter*, Daily Telegraph (Austl.), July 29, 2009, at 11, *available at* http://www.news.com.au/technology/features/internet-filter-blocks-education-sites-but-not-porn/story-fn300p73-1225755739583?from=public_rss.

87. *See generally* Nunziato, *supra* note 85 (discussing the issue of "overblocking," blocking more content than is necessary, when using filtering software).

88. Nielsen Co., Global Faces and Networked Places: A Nielsen Report on Social Networking's New Global Footprint 1 (2009), *available at* http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf (studying nine different countries and reporting that social media and blogging combined became more popular than personal email in December of 2008).

89. *See* Dan McIntosh, Comment, *E-Monitoring@Workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 Hamline L. Rev. 539, 542 n.17 (2000) ("Vault.com reported 78.9% of employees sending between 1 and 10 non-work related e-mails per day and over 37% of employees reported surfing the web 'constantly.' Over half of employers and employees believed that surfing the Internet and sending non-work related email decreased productivity."); Tripp Kuehnis, *Monitoring Employee Computer Use in the Workplace*, Associated Content, Nov. 14, 2005, http://www.associatedcontent.com/pop_print.shtml?content_type=article&content_type_id=14445 (discussing the "significant issue" of lost worker productivity as a result of personal use of company computers).

computer use, an employer that monitors its employees' computer use may be liable for invading their privacy on the basis of such monitoring even if no other adverse action is taken.[90]

B. Adoption

A policy can be contained in an employment agreement or an employee handbook and can also be a separate document distributed to employees. Regardless of its location, it should be in writing,[91] and its receipt should be acknowledged in writing or by email.[92]

C. Content

A policy's effectiveness is determined by how carefully it is drafted and the extent to which it is enforced. It is critical to provide that employees have no reasonable expectation of privacy in the use of their work-related computer and that the employer reserves the right to monitor employee computer use. However, a statement alone that "employees shall have no reasonable expectation of privacy with respect to any use of the employer's computing equipment" may not offer an appropriate level of protection to employers.[93] To diminish any reasonable expectations of privacy, a policy should allow an employer to conduct announced and unannounced inspections of the computing histories of employees and should provide that both types of inspections will regularly occur.[94] A policy should also

90. *E.g.*, Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 906–07, 910 (9th Cir. 2008) (finding that defendant-employer violated employee's Fourth Amendment rights by auditing employee's text-message records because the employer's informal policy created a reasonable expectation of privacy in the text messages despite a formal policy that employees should have no expectation of privacy in their company computing equipment).

91. *See id.* at 906–08 (demonstrating that informal, non-written policies can, in some instances, invalidate the effect of formal, written policies).

92. *See In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (noting that courts should consider whether the corporation notified the employee, or whether the employee was aware, of the corporation's use and monitoring policy in determining whether an employee had a reasonable expectation of privacy in his computer files and email).

93. *Quon*, 529 F.3d at 906–07 (finding that despite a formal policy that employees should have no reasonable expectation of privacy in their employer-provided computing devices, anecdotal evidence revealed an informal policy that supported a reasonable expectation of privacy); Haynes v. Office of the Attorney Gen., 298 F. Supp. 2d 1154, 1161–62 (D. Kan. 2003) (noting that, even though the employer policy stated that, "[t]here shall be no expectation of privacy in using this system," other facts, including oral representations, suggested that the employee had a reasonable expectation of privacy).

94. *See* Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (finding that an employee had some expectation of privacy in his work computer files because although the employer had full access to all its computers, the employer never routinely searched the computers, which gave rise to the employee's reasonable expectation of privacy); United States v. Hatfield, No. 06-CR-0550 (JS), 2009 WL 3806300, at *9 (E.D.N.Y. Nov. 13, 2009). In *Hatfied*, the court considered whether the employee had an expectation of privacy in computer files stored on his work computer. *Hatfield*, 2009 WL 3806300 at *8. Using the same four-factor test utilized in *In re Asia Global*, see *supra* note 20 and accompanying text, the *Hatfield* court distinguished between the right to

state that the employer has the right to access not only an employee's computing history, but also the text or content of computer files, emails, and other content created or accessed by an employee, regardless of whether that content may contain personal or work-related information.[95] In addition, a policy should provide that the employer has a right to, and will, keep copies of all computing passwords and that the existence of a password will not create any reasonable expectation of privacy for an employee.[96]

The first part of a policy should consist of a brief discussion of potential employer and employee liability from the use of computing equipment, including the use of social media, in order to convey the seriousness of the subject and deter computer-related misconduct.[97] The second part of a policy should contain clear definitions of all ambiguous or important terms in the policy. For example, a policy should clearly define what the employer considers to be confidential company and client information and should also define the computing equipment covered by the policy, which should include portable computing equipment such as USB flash drives and CDs. The third part of a policy should list the disciplinary actions available to the employer for violations of the policy, which should range from a verbal reprimand to termination. Subsequent sections of a policy should clearly explain, at a minimum: 1) how, when, and how often computer monitoring will be conducted, 2) what computer-related conduct is prohibited, and 3) what forms of computer use are covered by the policy. With respect to prohibited conduct, a policy should specifically prohibit the following: 1) accessing or transmitting sexually explicit content, 2) accessing or transmitting discriminatory content, 3) sending or posting politically or potentially defamatory content, 4) sending or posting confidential company or client information without authorization, 5) using, reproducing, posting, or sending copyrighted material without authorization, 6) sharing employee passwords and using another employee's passwords

monitor and actually monitoring an employee's computer or email. *Id.* at *9 ("[T]he Policy nowhere expressly indicates that DHB *will* monitor employee computer hard drive[s] or e-mail files, only that it has the *right* to do so.").

95. *See* McIntosh, *supra*, note 89, at 552 ("Longstanding precedent holds that an employer can lawfully intercept a 'business' communication, but cannot lawfully intercept a 'personal' communication beyond the time necessary to ascertain its personal nature."); *cf.* Briggs v. Am. Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (condoning an employer's decision to surreptitiously listen to an employee's telephone call but only to the extent that it was necessary to ascertain the nature of the call).

96. TGB Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 162 (Cal. Ct. App. 2002) ("The policy should further emphasize that the company will keep copies of Internet or e-mail passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications."); Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 404–05 (1995) (providing examples of possible email-monitoring policies).

97. Bell, *supra* note 59.

or computing equipment without proper authorization,[98] and 7) accessing, sending, or posting unprofessional content. With respect to the forms of computer use covered, a policy should also address remote access to an employer's computing systems or information.[99] A policy should prohibit unauthorized remote access to an employer's computing systems or information as well in order to protect the security of confidential information.[100]

Two additional provisions that should be part of a policy relate to the procedures for amending the policy and for asking questions about the policy. A policy should state that it cannot be amended orally or, if it states that it can be amended orally, that this can only be accomplished by certain upper-level management personnel. Absent such a provision, an employee could expect a reasonable level of privacy based on the oral representations of another employee, even one without actual policymaking authority and even if such representations contradict the explicit terms of the policy.[101] A policy should also state that employees who have questions about the requirements should contact one or more members of upper-level management, and these employees should be chosen based on their knowledge of the policy.

D. Drafting

In order to avoid ambiguity, a policy should include broad definitions that are qualified by specific examples. For instance, the computer uses covered by a policy should be broad enough that the policy covers computer uses that have yet to arise, but should also be specific in identifying many of the existing uses covered, such as social media, instant messaging, and email.[102] Although a policy can be amended, it is better for a policy to attempt to cover uses and technologies not currently in existence to avoid the risk of liability incurring on the basis of employee misconduct involving new technologies or uses that occurs before a policy is amended. A policy should also define prohibited conduct in broad terms, such as viewing or sending inappropriate content, and qualify this definition with specific examples of prohibited content, such as listing individual websites.

If a policy contains only broad definitions, however, an employer risks a court finding that a definition is ambiguous and/or does not cover the intended subject. For example, a court could find that, notwithstanding a policy's definition of the

98. *Id.*

99. *See* Amanda M. Andress, *What You Need to Know Before Setting up a Firewall: Getting to Know Your Needs and Putting Security Policies in Place*, IBM, Dec. 1, 2000, http://www.ibm.com/developerworks/library/s-fire.html.

100. *Id.*

101. *See supra* note 93 and accompanying text.

102. *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 896–97, 910 (9th Cir. 2008) (finding that the City's official use policy failed to cover text messages even though a high-level employee informed his subordinates that the policy covered text messages).

activities it covers, an employee had a reasonable expectation of privacy regarding a specific activity that was not listed in the policy,[103] or that such activity was within the scope of the employee's employment. Conversely, if a policy contains only specific definitions, an employer risks a court finding that the policy does not apply to certain conduct, technologies, or unmentioned uses.

E. Enforcement

Adopting an effective policy is only half the battle and may not be sufficient by itself to insulate an employer from liability on the basis of its employees' computer use, including the use of social media. If an employer fails to enforce an adopted policy, the policy may not shield the employer from liability. For example, even if a policy expressly eliminates an employee's reasonable expectation of privacy in emails and private computer files, if the employer failed to monitor and enforce the policy but later seeks to enforce it, the employer can be liable for violating the employee's reasonable expectation of privacy.[104] Other situations in which an employer's failure to enforce a policy can lead to liability or create a reasonable expectation of privacy for employees include where: 1) the employer failed to conduct regular monitoring, or any monitoring, of computer use,[105] 2) the employer failed to prevent an employee from taking actions that diminish the employer's ability to monitor computer use,[106] and 3) the employer failed to conduct unannounced monitoring of computer use (which can lead to a reasonable expectation of privacy with respect to unannounced monitoring).[107] In addition, employer liability can arise from the failure to properly discipline an employee under a policy, especially if such discipline could have prevented the employee from engaging in further

103. United States v. Hatfield, No. 06-CR-0550, 2009 WL 3806300, at *9 (E.D.N.Y. Nov. 13, 2009) (noting that the employer's computer-use policy prohibited specific activities such as games and pornography but did not expressly prohibit using the computer for personal, legal matters).

104. Haynes v. Office of the Attorney Gen., 298 F. Supp. 2d 1154, 1161–62 (D. Kan. 2003) (denying defendant-employer's motion for summary judgment because plaintiff-employee could have had an objectively reasonable expectation of privacy in his computer files despite an explicit policy otherwise given that "there was no evidence that any AG official had ever monitored or viewed any private files, documents or e-mails of any employee").

105. *See* Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (finding that an announced and infrequent search of employee's computer for maintenance purposes does not destroy employee's reasonable expectation of privacy in computer files).

106. United States v. Slanina, 283 F.3d 670, 676–77 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *remanded to*, 359 F.3d 356 (5th Cir. 2004) (holding that by installing passwords on his work computer and in the absence of a formal policy prohibiting personal use of the computer, employee had a reasonable expectation of privacy in his work computer files).

107. *See supra* note 105.

misconduct.[108] Not only will the failure to enforce a policy expose an employer to an increased risk of liability, but it will also cause an employer to lose the benefits associated with monitoring employees' computer use.

An employer who monitors its employees' computer use is more likely to be on notice of inappropriate conduct and more likely to have a duty to prevent it. Thus, the employer has an increased risk of liability in the event that inappropriate conduct continues. Conversely, an employer who does not monitor its employees' computer use may see an increased risk of liability on the basis of inappropriate employee conduct. Therefore, adopting *and* enforcing a policy that covers social media is an employer's best course of action to minimize liability.

CONCLUSION

Every new workplace phenomenon, from email to text and instant messages, offers benefits and risks to both employers and employees. Employers and employees must be conscious of the risks of social media websites so that they can use them while minimizing risks. This is particularly important in today's ever-changing and global business environment, as employers and employees need to take advantage of every available business tool in order to remain competitive.

108. Doe v. XYC Corp., 887 A.2d 1156, 1167 (N.J. Super. Ct. App. Div. 2005) (finding that actual or imputed knowledge of improper use of workplace computing equipment to view child pornography imposed a duty on the employer to notify law enforcement authorities); *see also* Settle-Vinson, *supra* note 80, at 73 (discussing respondeat superior liability).