ON THE PRECIPE OF E-DISCOVERY: CAN LITIGANTS OBTAIN EMPLOYEE SOCIAL NETWORKING WEB SITE INFORMATION THROUGH EMPLOYERS?

Aaron Blank[†]

I. INTRODUCTION

In today's global economy, many businesses rely on instant communication,[1] requiring employees to be continuously "connected" through the use of the latest forms of technology.[2] An increasing number of employers require employees to use cell phones, text messages, e-mails, and the Internet to communicate with each other and with clients.[3] A relatively new and growing form of communication is social networking Web sites.[4] Social networking Web sites are Internet communities where individuals can interact with other users to discuss common interests and share information.[5] Some businesses have begun using social networking Web sites to connect with customers[6] and to recruit new employees.[7] Even if a business is not yet connected to social net-

† J.D. Candidate, May 2011, The Catholic University of America, Columbus School of Law. The author would like to give a special thanks to Professor Megan La Belle, Professor Marin Scordato, and Josh Rabinowitz for their assistance with this Comment. He would also like to thank the *CommLaw Conspectus* staff for their dedication and hard work.

1 *See* Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 85 (2008).

2 *See id.*

3 *See* Anthony J. Oncidi & David Gross, *Blackberrys on the Beach: A Ripening Concern for Employers*, 51 ORANGE COUNTY LAW., Jan. 2009, at 10.

4 *See* Danah M. Boyd & Nicole B. Ellison, *Social Networking Site: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 1 (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

5 *Id.*

6 *See, e.g.*, Facebook, Facebook Advertising, http://www.facebook.com/advertising (last visited March 30, 2010) (follow "Case Studies" hyperlink) (discussing advertisers who have used Facebook to target specific potential customers).

7 Jennifer Kavur, *Smart Recruiting Through Social Networks*, NETWORK WORLD, Feb. 23, 2009, http://www.networkworld.com/news/2009/022309-smart-recruiting-through-

working Web sites, employees often use them for personal purposes while at work.

Employers, employees, and customers are communicating less in person and, instead, increasingly relying on electronic communications.[8] By using the Internet and other forms of electronic communication, companies can conduct business at a faster pace. However, the disadvantage of relying heavily on electronic communications in business is that *everything* is either recorded[9] or left behind in an electronic trail of data.[10] Information that once only existed in a paper copy of an office memorandum or water-cooler talk for a moment now may be immortalized in e-mail, on the Internet, or stored on a computer's hard drive. Similarly, when employees conduct personal business at work, they leave an electronic trail on their company's phone system, computers, and on the Internet.[11] When litigation ensues in the age of electronic information, a plaintiff has a new host of records that otherwise would not have been available to use against a defendant-employer.[12]

Since many documents are now primarily or exclusively stored in electronic form,[13] the production of electronic documents has become a vital part of discovery in litigation.[14] In 2006, the Federal Rules of Civil Procedure ("Rules") underwent changes to account for electronic discovery's modernization ("e-discovery").[15] The amendments expansively broadened the production of electronic documents.[16] However, despite the Rules' best efforts, technology will continue to evolve and present challenges to existing laws. The existence of social networking Web sites challenges the current mechanisms of e-discovery, and it remains unknown whether litigants may require an employer to provide information about employees' social networking activity.

This Note will address some of the substantive, procedural, and technical problems associated with using e-discovery to obtain information from an em-

---

social.html (last visited Apr. 14, 2010).

8 Sprague, *supra* note 1, at 130.

9 *See* 41 AM. JUR. 3D *Proof of Facts* § 1, at 7 (2009).

10 *See* Leanne Holcomb & James Isaac, Comment, *Wisconsin's Public-Records Law: Preserving the Presumption of Complete Public Access in the Age of Electronic Records*, 3 WIS. L. REV. 515, 532 (2008).

11 *See* 41 AM. JUR. 3D *Proof of Facts* § 1, at 7–8.

12 *See id.* at 7–9.

13 Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 8 (2006) ("[M]ore than 90% of all business records are digital, and many businesses never commit those records to paper.").

14 *See* Richard L. Marcus, Essay, *The Impact of Computers on the Legal Profession: Evolution or Revolution?*, 102 NW. U. L. REV. 1827, 1843 (2008).

15 *See generally* Andrew Peck, *The December 2006 Federal Rules Amendments Governing Electronic Discovery*, 783 PLI/Lit 37 (2008) (discussing how the changes to the Federal Rules of Civil procedure affect e-discovery).

16 *See* FED. R. CIV. P. 34 advisory committee's note (2006).

ployee's social networking Web site activity conducted in the workplace. Little precedent exists for when an employer must produce the information it possesses on an employee's social networking activities at the workplace.[17] Part II provides background information about social networking Web sites and how employee misuse of them in the workplace may impose liability upon an employer, thereby spurring a third party to seek discovery through the employer. Part III examines discovery requests to employers for their employees' social networking Web site accounts, the mechanisms through which the discovery may be produced and difficulties confronted in that process, and why the courts should limit such requests for discovery. Finally, Part IV concludes by outlining the issues that courts and litigants will face in handling discovery requests that seek an employee's social networking activities and suggests principles that should guide future analysis.

II. SOCIAL NETWORKING WEB SITES

Those who belong to social networking Web sites use them to network with others who share common interests.[18] Generally, users of these sites create an online profile displaying their interests and personal information, which can be read by others, in order to search, contact, and make friends with other users.[19] The popularity of these sites is growing tremendously.[20] For example, Facebook currently has "[m]ore than 300 million active users"—50 percent of whom log into Facebook every day—and the "[a]verage user has 130 friends on the site."[21]

Social networking Web site users create profiles to share their photos, videos, and other information with their friends.[22] Facebook believes that users should be able to share *whatever* they want with *whomever* they want, so long as both parties consent and subject to the "limitations of law, technology, and

---

17 Deni Connor, *EDiscovery Affected by California Law, Social Networks*, NETWORK WORLD, July 15, 2009, http://www.networkworld.com/newsletters/stor/2009/071309stor2.html ("There hasn't been a major legal case yet challenged vendors to include Facebook comments and Twitter tweets in their eDiscovery capabilities . . . .").

18 Boyd & Ellison, *supra* note 4, at 1.

19 *See id.*

20 *See, e.g.*, PEW INTERNET & AM. LIFE PROJECT, SOCIAL MEDIA AND YOUNG ADULTS 33 (2010), *available at* http://pewinternet.org/Reports/2010/Social-Media-and-Young-Adults/Part-3/2-Adults-and-social-networks.aspx?r=1 ("The percentage of adults who use online social networks [grew] from 8 percent of internet users in February 2005 . . . to 37 percent in November 2008.").

21 Facebook, Facebook Statistics, http://www.facebook.com/press/info.php?statistics (last visited March 23, 2010).

22 *See* Boyd & Ellison, *supra* note 4, at 1.

evolving social norms."[23] Twitter allows users to stay connected with friends by posting messages, known as "tweets," of 140 characters or less to their profiles.[24] Another popular form of online social networking are blogs, which are like online journals, where users post a series of messages and responses.[25] These social networking Web sites pose difficult legal concerns, however, for employers and employees.

A. General User Concerns

While social networking sites provide users with many valuable benefits, they also present many dangers. Sexual predators have taken advantage of the sites' popularity with young people to find victims.[26] Users of social networking sites also face the possibility that their information may be misappropriated for unintended uses.[27] Although users can control what they post and which users view their personal information and messages, they cannot control how recipients or the site itself subsequently use what has been uploaded to the network. For example, Facebook warns its users that certain information disclosed on its site is available to the entire public.[28] MySpace's terms of use agreement declares that its users own the material that they post on the Web site, but MySpace retains a limited license to "use, modify, delete from, add to, publicly perform, publicly display, reproduce, and distribute such Content . . . ."[29]

B. Why Employers Should be Concerned

The use of computers and the Internet in the workplace has grown tremendously over the past twenty years.[30] However, while modern communications

---

23 Facebook, Facebook Principles, http://www.facebook.com/principles.php (last visited March 24, 2010).

24 Twitter, Twitter Support, http://help.twitter.com/portal (last visited March 24, 2010).

25 *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 197 (25th ed. 2009).

26 *See* Richard M. Guo, *Stranger Danger and the Online Social Network*, 23 BERKELEY TECH. L.J. 617, 625–26 (2008).

27 *See* Samantha L. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 551–53 (2008) (discussing the problems that result when social networking site users unintentionally relinquish their privacy in their personal information to unauthorized and malicious third-party viewers).

28 *See* Facebook, Privacy Policy, http://www.facebook.com/policy.php (last visited March 24, 2010).

29 MySpace.com, Terms & Conditions, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited March 24, 2010).

30 Erin M. Davis, Comment, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by their Employees*, 12 ALB. L.J. SCI. & TECH. 683, 684 (2002).

technologies can increase employee productivity, workers have gotten into trouble using the Internet at work for accessing pornography,[31] sending sexually related messages,[32] visiting gambling Web sites,[33] and misappropriating trade secrets and other intellectual property rights.[34] Employers have been exposed to various forms of civil liability from employees' misuse of the Internet.[35] Some employee misuse of workplace computers can even result in criminal liability.[36] One of the most common forms of liability that employers face is from sexual harassment and hostile work environments created by an employee distributing pornographic or other sexually inappropriate jokes, pictures, and other materials on computers in the workplace.[37] Employers are vulnerable to sexual harassment charges when their employees use company computers and e-mail to download and distribute sexually explicit materials.[38] An employee's open viewing of sexually explicit material in the workplace can create an uncomfortable work environment for other employees, for which the employer may be held liable.[39]

Social networking sites provide employers with a new online medium from which they may incur liability.[40] Like e-mail, messages sent over social networking sites are less formal than written letters. The danger in this informality is that people will often say things or distribute materials over these sites that would they would not say in person.

---

31 *E.g.*, David Nakamura, *9 D.C. Workers Fired For Looking at Porn*, WASH. POST, Jan. 24, 2008, at B1.

32 *See, e.g.*, Haybeck v. Prodigy Serv. Co., 944 F.Supp. 326, 327 (S.D. N.Y. 1996) (discussing an employee who had been communicating with the plaintiff in an online sex chat room while at work).

33 Lesley Stedman, *Online Bets Placed at the Office*, COURIER-J. (Louisville, KY), Dec. 23, 2002, at 7A, *available at* LEXIS, News & Business Library.

34 *See, e.g.*, Ameriwood Indus., Inc. v. Liberman, No. 4:06CV524-DJS, 2007 WL 5110313, at *1 (E.D. Mo. July 3, 2007) (providing that the plaintiff alleged that the defendant, a former employee of the plaintiff, had used the plaintiff's computers during the course of their employment to obtain the plaintiff's business secrets and then used the information to divert business to defendant's own business).

35 *See, e.g.*, Doe v. XYC Corp., 887 A.2d 1156 (N.J. Sup. Ct. App. Div. 2005).

36 *See* The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006); *see also* Davis, *supra* note 30, at 696 (stating that computers can be used to commit criminal activities including "theft, misappropriation of trade secrets, fraud, libel, sexual harassment, racial harassment, securities fraud, embezzlement, trespass, and copyright infringement").

37 *See* Davis, *supra* note 30, at 697.

38 Louis J. Papa & Stuart L. Bass, *How Employers Can Protect Themselves from Liability for Employees' Misuse of Computer, Internet, and E-mail Systems in the Workplace*, 10 B.U. J. SCI. & TECH. L. 110, 112 (2004).

39 *See id.* at 112 (citing Meritor Savings Bank v. Vinson, 477 U.S. 57, 65 (1986)).

40 *See* discussion *infra* Part II.C.

C. Potential Employer Liability

Businesses increasingly utilize social networking sites to connect their employees with one another and with their customers.[41] If an employee's tortious use of a social networking site occurs within their scope of employment, then the victim who sustains the resulting injury may seek to hold the employer vicariously liable under the doctrine of respondeat superior.[42] Acts of employees in the workplace that are strictly personal in nature will fall either within or outside the scope of the employee's employment, depending on the circumstances.[43] "Purely personal acts" that employees perform while they are working, "such as . . . smoking and eating . . . may be within the scope of employment because they are incidental to the employee's performance of assigned work."[44] In contrast, employees who commit malicious torts on personal grounds typically have not acted in a capacity related to their job.[45] A leading factor in determining whether an employer will be vicariously liable for the employee's tortious act is whether the personal behavior was within the employer's control.[46]

An employee's use of a workplace computer to access social networking Web sites for personal purposes could be considered within the scope of employment when: such use is incidental to the employee's comfort and welfare, such use is reasonably expected in the modern workplace, and the possibility exists that the employer maintains control over use of the computer.[47] However, the content of the material sent through an employee's social networking account may be considered too personal in nature to be deemed in furtherance of the employer's business.

In *Booker v. GTE.net LLC*, a customer sued their e-mail provider over an unauthorized e-mail that an employee of the e-mail provider sent from the cus-

---

41 *See* Madeline Kriescher, *Professional Benefits of Online Social Networking*, COLORADO LAW., Feb. 2009, at 62.

42 *See* RESTATEMENT (THIRD) OF AGENCY § 2.04 (2006) (providing that under respondeat superior, an employer may be liable for torts committed by their employees if the acts occurred within the scope of the employee's employment); *id.* at § 7.07 cmt. c. (stating that vicarious liability under respondeat superior can extend from both intentional and negligent torts, so long as they occurred within the scope of employment). The doctrine of vicarious liability is based on a policy of risk allocation that when injuries are "caused by the torts of employees . . . in the conduct of the employer's enterprise," the burden of that injury should be, "placed upon that enterprise itself, as a required cost of doing business." Delfino v. Agilent Techs, Inc., 52 Cal. Rptr. 3d 376, 396 (Ct. App. 2006).

43 *See* RESTATEMENT (THIRD) OF AGENCY § 7.07 cmt. d (2006).

44 *See id.*

45 *Id. See also* Tomka v. Seiler Corp., 66 F.3d 1295, 1317 (2d Cir. 1995) ("[A]n employer is not liable for torts committed by the employee for personal motives unrelated to the furtherance of the employer's business.").

46 *See* RESTATEMENT (THIRD) OF AGENCY § 7.07 cmt. d (2006).

47 *See id.* at § 7.07 cmt. b–d.

tomer's account.[48] The United States Court of Appeals for the Sixth Circuit held that sending such an e-mail was "'reasonably incident to [the] employment.'"[49] But the court concluded that the e-mail's highly offensive nature placed it outside the scope of the employee's employment because it "cannot plausibly be interpreted . . . to advance [the employer's] business goals."[50] Furthermore, even though the e-mail was sent from the employer's computer, the e-mail was not within the scope of the employee's employment because it was sent from a personal account.[51] Similarly in *Delfino v. Agilent Technologies, Inc.*, the California Court of Appeal for the Sixth District held that an employee's sending of threatening Internet messages was "plainly outside the scope of his employment" because using the employer's "computer system to log on to a private Internet account to send messages - threatening or otherwise - was never part of [the employee's] job duties."[52]

If the law considers an employee's use of social networking sites as outside the scope of employment, the employer could still be liable under a negligent retention theory. Negligent retention liability is independent from respondeat superior liability because negligent retention focuses on the employer's actions or failure to act, while the tortfeasor under respondeat superior theory is the employee.[53] Negligent retention liability is found where a plaintiff's injury is the proximate result of an employer's hiring or retaining of an employee who breached a duty of reasonable care.[54] If an employer has exercised due care and diligence in hiring and retaining employees that appear to be "competent, careful, and sober, and fail to discover any vicious habits, they cannot be held liable for negligently retaining incompetent men."[55] Similarly, if an employer promptly corrects an employee's misbehavior, the employer will most likely be immune from a negligent retention claim.[56]

In general, an employer owes third parties a duty of reasonable care to prevent "torts committed by employees on the employer's premises or with the

---

48 Booker v. GTE.net LLC, 350 F.3d 515, 516–17 (6th Cir. 2003).

49 *Id.* at 518 (quoting Coleman v. United States, 91 F.3d 820, 825 (6th Cir. 1996)).

50 *Id.* at 519.

51 *Id*.

52 Delfino v. Agilent Techs., Inc., 52 Cal. Rptr. 3d. 376, 396 (Cal. App. Ct. 2006).

53 *See* Janet E. Goldberg, *Employees with Mental and Emotional Problems — Workplace Security and Implications of State Discrimination Laws, the Americans with Disabilities Act, the Rehabilitation Act, Workers' Compensation, and Related Issues*, 24 STETSON L. REV. 201, 215–16 (1994).

54 Papa & Bass, *supra* note 38, at 124.

55 Hilts v. Chicago & G.T. Ry. Co., 21 N.W. 878, 882 (Mich. 1885).

56 *See* Daniels v. Worldcom Corp., No. CIV.A.3:97-CV-0721-P, 1998 WL 91261, at *4 (N.D. Tex. Feb. 23, 1998) (holding that a claim for negligence against an employer for insensitive e-mails failed because within ten days of being notified about e-mails, the employer disciplined the sender and issued warnings and instruction regarding company e-mail policy).

employer's chattels . . . ."[57] This duty should extend to all employees' use of their employer's computers, including accessing social networking Web sites. For example, in *Doe v. XYC Corp.*, the Appellate Division of the Superior Court of New Jersey held that an employer who had notice of an employee's use of company computers to visit pornographic Web sites, but failed to investigate, had breached its duty of care to the employee's family because had the employer taken corrective actions, the employer would have likely discovered that the employee was uploading pornographic pictures of the family's daughter to the Internet.[58] *Doe* held that an employer may be subject to negligence when the employee has used the employer's computer, the employer knows or has reason to know he can control the employee's computer use, and the employer knows or should have known of the necessity to exercise control.[59]

A third cause of action that has been used to hold employers liable for employee computer and Internet misuse is a hostile work environment claim. In the twin cases *Faragher v. City of Boca Raton* and *Burlington Industries., Inc. v. Ellerth*, the United States Supreme Court held that an employer may be liable to an employee for creating a hostile work environment that amounts to employment discrimination.[60] A hostile work environment is dynamic in nature and can be created from a series of discriminatory actions; it cannot arise from a singular, discrete incident.[61]

Employees' use of computers now commonly expands the work place well beyond the office walls.[62] The traditional, physical workplace includes "areas and items . . . related to work and . . . generally within the employer's control."[63] The modern workplace, however, is much more dynamic than a physical space because computers allow employees to work in a "virtual workplace" where work is done in the office, at home, or on-the-go.[64] An employer's e-

---

[57] Haybeck v. Prodigy Serv. Co., 944 F.Supp. 326, 332 (S.D.N.Y. 1996) (quoting Tomka v. Seiler Corp., 66 F.3d 1295, 1317 (2nd Cir. 1995))).

[58] Doe v. XYC Corp., 887 A.2d 1156, 1158–59, 1167–68 (N.J. Sup. Ct. App. Div. 2005).

[59] *See id.* at 1168.

[60] Faragher v. City of Boca Raton, 524 U.S. 775, 805–09 (1998); Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 746, 763 (1998) ("An employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee.").

[61] *See, e.g.*, Curtis v. DiMaio, 46 F. Supp. 2d 206, 213 (E.D.N.Y. 1999) ("[A] single offensive e-mail does not create a hostile work environment."); *but see* Schwapp v. Town of Avon, 118 F.3d 106, 112 (2nd Cir. 1997) (holding that eight racial slurs made outside the presence of the plaintiff and four made in his presence supported a claim for a hostile work environment).

[62] *See* Davis, *supra* note 30, at 697–98 (discussing how while a hostile work place traditionally was limited to inside the workplace, company e-mail systems can now be used to create hostile work environments outside the "traditional office setting").

[63] O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

[64] *See* Oncidi & Gross, *supra* note 3, at 11 ("Today, thanks to voicemail, the Internet,

mail system may be characterized as part of the work environment because it is related to work and is within the employer's control.[65] In *Blakey v. Continental Airlines, Inc.*, the Supreme Court of New Jersey recognized that a hostile work environment was possible as a result of harassment occurring over the company's online message forum.[66] Although the issue of liability was ultimately remanded, the court reversed the lower court and strongly suggested to the lower court that it should recognize that the online message forum was related to and benefited the airline's business—thus making it an extension of the workplace.[67]

One court recognized that electronic communications may be considered to be a part of the work environment if their use "constitute[s] a substantial means of communication among . . . employees."[68] If a social networking site reaches this level of use in an office then it should fall within the bounds of the modern work environment.

Now that employers face potential liability for employee social networking activity conducted over their computers, they need to know what records of the activity they are required to obtain and produce and how to do so.

III. DISCOVERY

Discovery is intended to "provide a mechanism for making relevant information available to litigants."[69] The use of discovery to obtain electronic documents has become increasingly common with the increased computer use in business.[70] In 2006, amendments were proposed to the Federal Rules of Civil Procedure to implement new e-discovery rules to account for discovery of electronically stored information ("ESI").[71] The committee concluded that the amendments were necessary for two principal reasons:

> First, electronically stored information has important differences from information recorded on paper. The most salient of these differences are that electronically stored information is retained in exponentially greater volume than hard-copy documents; electronically stored information is dynamic, rather than static; and electronically stored

---

BlackBerrys and other mobile devices, employees can, and increasingly do, work anytime, anywhere.").

65 *See* Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 81 (2009) (noting that "e-mail, as well as hardware and software equipment, as employer property . . . is subject to [an] employer's control and monitoring.").

66 Blakey v. Continental Airlines, Inc., 751 A.2d 538, 543 (N.J. 2000).

67 *Id.* at 551.

68 Zubulake v. UBS Warburg, 217 F.R.D. 309, 317 (S.D.N.Y. 2003).

69 FED. R. CIV. P. 26 advisory committee's note (1983).

70 *See* Mike Breen, Comment, *Nothing to Hide: Why Metadata Should be Presumed Relevant*, 56 U. KAN. L. REV. 439, 439 (2008) (discussing the increased use of electronic records in business and how it has affected e-discovery).

71 *See generally* Peck, *supra* note 15.

> information may be incomprehensible when separated from the system that created it. Second, these differences are causing problems in discovery that rule amendments can helpfully address.[72]

Employees' activity on social networking Web sites will become more relevant in lawsuits against employers. However, social networking Web sites do not fit neatly within the current rules and practices of e-discovery and may frustrate litigants. The problem that courts and litigants currently face is that "specific rules governing the discoverability of online personal information have not kept pace with [social networking Web sites], which are being developed faster than regulations can be revised or promulgated."[73]

Amendments to the Rules of Civil Procedure may be necessary to clarify issues regarding employee social networking accounts present under: the scope of discovery, document production, subpoenaing social networking sites, and limitations for privacy.

A. The Scope of Discovery

The scope of discovery under Rule 26(b)(1) is broad, making discoverable "any nonprivileged matter that is relevant to any party's claim or defense . . . ."[74] The test for relevance is whether "there is any possibility that the information sought may be relevant to the subject matter of the action."[75] If a request for information is facially relevant and the party does not wish to produce it, the producing party must establish the document is not relevant.[76] Marginally relevant information may be excluded from production if the "potential harm . . . would outweigh the ordinary presumption in favor of broad disclosure."[77]

---

[72] CIVIL RULES ADVISORY COMM., JUDICIAL CONFERENCE OF THE U.S. REPORT OF THE CIVIL RULES ADVISORY COMMITTEE, INTRODUCTION TO FINAL DRAFT OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE 18 (2005), *available at* http://www.uscourts.gov/rules/Reports/CV5-2005.pdf.

[73] Ronald J. Levine & Susan L. Swatski-Lebson, *Social Networking and Litigation*, E-COMMERCE L. & STRATEGY (Law Journal Newsletters, New York, N.Y.), Jan. 2009, at 1, *available at* http://www.herrick.com/siteFiles/Publications/CBC006F756591FF0160327DA071BDB3F.pdf.

[74] FED. R. CIV. P. 26(b)(1).

[75] AM Int'l, Inc. v. Eastman Kodak Co., 100 F.R.D. 255, 257 (N.D. Ill. 1981) For example, this can mean that the discovery sought should be granted if it "may reasonably assist [a party] in evaluating its case, preparing for trial, or facilitating a settlement." TBG Ins. Serv. Corp. v. Superior Court, 117 Cal. Rptr. 2d 115, 160 (Cal. App. 2002); *see also* Snowden v. Connaught Lab., Inc., 137 F.R.D. 336, 341 (D. Kan. 1991) (stating that a discovery request should be granted "unless it is clear that the information sought can have no possible bearing on the subject matter of the action").

[76] *See* Scott v. Leavenworth Unified Sch. Dist. No. 453, 190 F.R.D. 583, 585 (D. Kan. 1999).

[77] *Id.*

1. How Relevant are Social Networking Sites?

Because social networking sites provide users with "a sense of intimacy and community," the records they leave behind on work computers may offer either highly relevant information about the user's state of mind or irrelevant personal information.[78] The relevancy of such information should be determined on a fact-specific basis and irrelevant information should be excluded from discovery.[79]

In *Perfect 10, Inc. v. Google, Inc.*, Perfect 10 brought multiple copyright and trademark infringement claims against Google for storing the plaintiff's legally protected images on its computer server and displaying those images to Google users.[80] The United States District Court for the Central District of California held that printouts from a blog hosted by Google were potentially relevant to Perfect 10's copyright infringement claim if "they should have triggered a reasonably vigilant litigant to 'put two and two together' and realize that *Google was storing full-size P10 images* on its servers."[81]

Information within social networking sites that is relevant to users, however, may not be legally relevant to a lawsuit. In *Quigley Corp. v. Karkus*, the United States District Court for the Eastern District of Pennsylvania dismissed a plaintiff's allegation that a codefendant's Facebook "friendship" had any legal significance to the case, which involved a corporate shareholder's failure to disclose the disposition of their relationship in violation of the Securities and Exchange Act.[82]

Perfect 10 and *Quigley Corp.* suggest that user activity within a social networking site is only relevant in a cause of action to the extent that a court is willing to recognize its legal significance. The limits of judicial recognition, however, will likely increase with time because social networking sites are growing in popularity, and social norms attached to user interactions should gain legal relevance as they become more widely respected.

2. Third Party Discovery of Employee Social Networking Accounts

Gauging the relevance of discovery requests for information contained on these sites is a newly emerging area of the law.[83] In *Mackelprang v. Fidelity*

---

78 *See* Levine & Swatski-Lebson, *supra* note 73, at 3.

79 *See supra* notes 74–77 and accompanying discussion.

80 Perfect 10, Inc. v. Google, Inc., No. CF 04-9484 AHM (SHx), 2008 WL 4217837, at *1 (C.D. Cal. July 16, 2008).

81 *Id.* at *5 (emphasis in original).

82 Quigley Corp. v. Karkus, Civil Action No. 09-1725, 2009 WL 1383280, at *3–5 (E.D.Pa. May 15, 2009). The court noted that "[f]or purposes of this litigation, the Court assigns no significance to the Facebook 'friends' reference . . . ." *Id.* at *5 n.3.

83 Connor, *supra* note 17.

National Title Agency of Nevada, Inc., Mackelprang alleged that she had been sexually harassed by her employer, Fidelity.[84] Fidelity sought discovery of private messages Mackelprang sent using her MySpace accounts as a way to impeach the plaintiff's credibility because the company believed that the messages would show that Mackelprang was involved in extra-marital affairs.[85] The court denied Fidelity's motion to compel because it did not contain "information regarding the identities of the persons with whom Plaintiff has exchanged email messages or what the subject matter or content of those email messages are."[86] The court stated that Fidelity's ability to compel discovery from Mackelprang's MySpace account was limited to those messages that directly related to the plaintiff's employment with Fidelity.[87] *Mackelprang* suggests that parties should not be allowed to engage in a fishing expedition for information contained within an employee's account. Courts should grant such a discovery request served on an employer only to the extent that it specifically targets relevancy and relates to the employment setting as an issue in the case.[88]

B. Document Production

The 2006 amendments to the Federal Rules of Civil Procedure seek to treat ESI and paper documents "on equal footing."[89] Rule 34(a)(1)(A) provides that a party may request production of "any designated documents or electronically stored information – including . . . data or data compilations–stored in any medium" that are within "the responding party's possession, custody, or control."[90] As one court noted, "[A] party need not have actual possession of documents to be deemed in control of them."[91] Rather, documents are within a party's possession, custody, or control if the party has the "legal to right to control

---

> [S]ocial networks such as Facebook and Twitter may cause problems for companies that use the services to communicate with customers or exchange information among employees. There hasn't been a major legal case yet challenging vendors to include Facebook comments and Twitter tweets in their eDiscovery capabilities – although a spa manager fired an employee over Facebook—but there will be soon as more companies adopt social media sites such as Twitter and Facebook.

Id.

84 Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, *1, *1 (D. Nev. Jan. 9, 2007).

85 *Id.* at *3.

86 *Id.* at *2.

87 *Id.* at *8 ("This, however, does not include private email messages between Plaintiff and third persons regarding allegedly sexually explicit or promiscuous emails not related to Plaintiff's employment with Fidelity.").

88 *See supra* part II.C.

89 FED. R. CIV. P. 34 advisory committee's note (2006).

90 FED. R. CIV. P. 34 (a)(1)–34 (a)(1)(A).

91 *In re* Folding Carton Antitrust Litig., 76 F.R.D. 420, 423 (N.D. Ill. 1977).

or obtain them."[92] Thus, an employer may be obligated to produce documents pertaining to or created by an employee to the extent that the employee's actions and the created records are within the employer's control.[93] Hence, if an employer has possession, custody, or control of an employee's social networking messages and activity, those records may be requested through discovery.

The amendments to Rule 34 were designed to broadly expand traditional document production to include contemporary forms of electronic information and account for future developments.[94] An employer who reasonably anticipates or who is a party to litigation has a duty to preserve their business records, including those in electronic format.[95] Employers have a self-interest in monitoring the use of their computers and they should obtain possession, custody, and control of records reflecting all of their employees' activities on social networking sites. However, employers may be reluctant to implement such monitoring because such records could also be used against their interests by an opposing party who obtains them from discovery.

1. Employee Monitoring Software

Employers have access to software that allows them to monitor and record their employees' online activities.[96] Employee monitoring software can record Internet activity including all "e-mails sent and received, instant messages, web sites visited and documents used or attached to electronic communications."[97] These tools could effectively capture a significant portion of social networking activity conducted over an employer's computer network. This software can also be installed on computers issued by their employer that are used outside of the office.[98] Using this software allows an employer to easily comply with an e-discovery request because the software creates a record of the employee's online activities.[99] Utilizing employee monitoring software provides employers with an early warning of potential unlawful online activi-

---

92 *Id.*

93 *See, e.g.*, Herbst v. Able, 63 F.R.D. 135, 138 (S.D. N.Y. 1972) (stating that because the employees were within the control of the employer, the testimonies of the employees, regardless of their participation in the lawsuits, were related to the employer's affairs and may be produced).

94 *See* FED. R. CIV. P. 34 advisory committee's note (2006).

95 *See* FED. R. CIV. P. 34(E).

96 *See, e.g.*, Pearl Software, Electronic Discovery Act, http://www.pearlsw.com/news/eimArticles/electronicDiscoveryAct.html (last visited March 29, 2010) [hereinafter Pearl Software].

97 *Id.*

98 *See* Pearl Software, Internet Monitoring Tailored to Your Environment, http://www.pearlsw.com/news/eimArticles/integratingEIM.html (last visited March 29, 2010).

99 *See* Pearl Software, *supra* note 96.

ties by their employees.[100] However, before employers decide to use this software to protect themselves, they should consider that the software can negatively affect employee morale and productivity.[101]

If an employer does not implement a sufficient form of employee Internet monitoring, records of user activity may be too difficult or expensive to access,[102] thus placing them beyond the employer's possession, custody, or control.

2. Producing Employee Social Networking Activity through Network Monitoring

A party who seeks discovery of electronic files from an employer will have access to more detailed information if the employer utilizes monitoring software that logs a detailed record of employee computer use.[103] In this case, the employer can comply with a discovery request simply by having their computer services department prepare a record of the employee's Internet activity.

If an employer has Internet monitoring software that only logs Internet timestamps and does not log the content visited and created by the user, the employee's social networking activity will not be recorded. However, the timestamp can help litigants discover which Web sites the employee visited. This information may help the plaintiff link the employer's computer use to the employer to establish employer liability. Furthermore, an employee who accesses their social networking accounts at work may be granting their employer access and permission to access their password protected accounts because timestamping software may provide employers with the login information needed to access the employee's social networking accounts.[104]

Although the courts have examined whether an employee has a right to privacy in the content that they password protect and store online, no bright-line rule exists for such rights. In *McLaren v. Microsoft Corp.*, the Court of Appeals of Texas held that an employee who stored personal e-mails in password-protected "personal folders" on his employer's computer had no reasonable expectation of privacy in the e-mails.[105] The court noted that because the e-

---

100 *See* Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 122–23 (2005).

101 *See id*. at 124 (noting that employers' monitoring of their employees computer activities can result in employee "[s]tress, depression, and anxiety").

102 *See* Martha A. Mazzone, *The New E-Discovery Frontier—Seeking Facts in the Web 2.0 World (And Other Miscellany)*, BOSTON BAR J., Jan./Feb. 2009, at 8.

103 *See* Shannon M. Curreri, *Defining "Document" in the Digital Landscape of Electronic Discovery*, 38 LOY. L.A. L. REV. 1541, 1561 (2005).

104 *See* Levine & Swatski-Lebson, *supra* note 73, at 1.

105 McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4–5 (Tex. App. May 28, 1999).

mails were stored on a computer provided to him by his employer for work purposes, the employee had no reasonable expectation of privacy in them.[106] By contrast, in *Stengart v. Loving Care Agency, Inc.*, the Superior Court of New Jersey rejected an employer's argument that it could access the Web-based e-mail account of one of its employees because the employee had used a company-owned computer to access the e-mail account.[107] The court stated that when an employee uses a company computer for personal communications, the employer may have a more limited interest in accessing the communications when they have an "impact on its business or reputation."[108] For example, if an employer believes that their employee is not being productive, the employer has a limited right to access the communications to determine whether disciplinary action is warranted, but such access does not grant the employer the right to confiscate the communications.[109]Although *McLaren* and *Stengart* help clarify the rights employers and employees have in e-mail communications, it remains unknown how such rights apply in the context of an employer's right to access an employee's social networking account in order to comply with a third party's discovery request.

3. Hard Drive Searches

The most direct and inexpensive way ESI can be discovered is through the production of specific, easily retrievable data that parties possess in accessible forms.[110] Although preferred, it is not always feasible to produce ESI this way because relevant computer files may not be indexed properly, may exist in remote areas of a computer's memory, may exist in an unusable form, or potentially have been deleted.[111] Because files of this nature can still be recovered and track much of the computer activity of a person or company, some litigants are now "waging legal wars with floppy disks and hard drives,"[112] in search of the electronic "smoking gun" that wins their case.[113] Similarly, when an employer has not used monitoring software, a party seeking discovery could use

---

106 *Id.*

107 Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 399 (N.J. Super. Ct. App. Div. 2009).

108 *Id.*

109 *Id.* at 401.

110 *See* 41 AM. JUR. 3D *Proof of Facts* § 1, at 7 (2009).

111 *See id.* at §§ 6–8 (2009).

112 *Id.* at § 1.

113 *See* Susan J. Becker, *Discovery of Information and Documents from a Litigant's Former Employees: Synergy and Synthesis of Civil Rules, Ethical Standards, Privilege Doctrines, and Common Law Principles*, 81 NEB. L. REV. 868, 943 (2003) ("[T]he dreaded 'smoking gun' and other telling documents may lie smoldering in a[n] . . . employee's . . . files.").

this strategy to search for employee social networking data on a computer's memory. However, obtaining social networking data in this way may not be realistic or successful.

To conduct this type of search, a party seeking discovery obtains and submits a copy of the opponent's hard drive to a computer forensic expert for analysis.[114] The expert first inspects the hard drive and creates a "digital or mirror image" while at the same time "avoid[ing] unnecessarily disrupting the normal activities and business operations of [the party] . . . ."[115] The expert uses software to search through the computer and retrieve a wide range of files, including deleted files, ranging from e-mail messages to spreadsheets and word processing documents.[116]

a. The Scope of Hard Drive Searches

In order for a hard drive to be subject to discovery, there must be a link between a plaintiff's claim or defendant's defense and the information sought within the hard drive.[117] The scope of the discovery of the hard drive will be limited by boundaries negotiated by the parties, such as limiting the search to key dates, "words, phrases, data, documents, messages, or [data] fragments."[118]

If the files sought in a discovery request are relevant but are in an unusable medium, Rule 34(a)(1)(A) permits a translation of data "into a reasonably usable form."[119] A common misconception among computer users is that the delete button permanently deletes the file from the user's computer.[120] For example, while an employee may delete their Web history from their Internet browser, data recovery services may be able to recover the images accessed by extracting the "temporary Internet files" stored on the computer's cache.[121] Through this "recovery and reconstruction" process, parties are able to obtain

---

114 *See, e.g.*, Cenveo Corp. v. Slater, No. 06-CV-2632, 2007 WL 442387, at *2 (E.D.Pa. Jan. 31, 2007).

115 *Id.*

116 *Id.* at *3; 41 AM. JUR. 3D *Proof of Facts* § 2.

117 *See* FED. R. CIV. P. 26(b)(1); *see also* Apple Computer, Inc. v. Doe 1, No. 1-04-CV-032178, 2005 WL 578641, at *5 (Cal. Super. Ct. Mar. 11, 2005) (stating that in balancing the interests between discovery and privilege, one of the factors the court considers is whether the "discovery sought goes to the heart of the plaintiff's claim").

118 *See* Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 651 (D. Minn. 2002).

119 FED. R. CIV. P. 34(a)(1)(A).

120 Shira A. Scheindlin, Fed. Dist. Judge, S.D.N.Y., Keynote Address at the ARMA International Conference and Expo (Oct. 22, 2006), *available at* http://www.arma.org//podcast/speech.pdf; *see also, e.g.*, E-Hounds, Data Recovery, http://www.ehounds.com (last visited March 29, 2010) (discussing computer data recovery services).

121 100 AM. JUR. 3D *Proof of Facts* 89 § 4, at 117 (2008).

deleted files and translate them into useable form.[122]

b. Determining the Form of Electronically Stored Information

Parties must mutually agree to a format that the ESI discovery will be presented in under Rule 26(f)(3)(C).[123] Rule 34(b)(1)(E) provides that if a party's request does not specify what form electronically stored data is to be produced in then "a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms."[124] It is important for a requesting party to know what form to request ESI in, or the form it will subsequently be received in, so that the party is able to effectively decipher the information. When parties fail to discuss the form of ESI prior to discovery, a party that lacks the technical capabilities to decipher the information will face many problems, such as having to participate in evidentiary hearings and producing "additional evidence and witnesses."[125]

c. Technical Difficulties in Searching for Social Networking Web Site Data

If an employer does not use Internet monitoring software or time-stamping and cannot lawfully access an employee's social network account, hard drive searching may be the only way for the employer to produce information from an employee's account. For example, if the employer can recover images from the "temporary Internet files" then the employer may be able to discover images accessed on an employee's social networking account.[126] If the images are not recoverable, many litigants do not know how to find social networking data in company records.[127]

Typically, a data recovery expert can limit their search of computer data to specific types of files, for example, ".txt" or ".doc" files.[128] But unlike files such as business e-mails that may be stored in a narrow area of the hard drive's cache, social networking data presents more difficulties.[129] Social networking sites and other Web sites rich in content such as photos are harder to trace than earlier forms of Web data, which were primarily text-based, because these sites

---

122 *See* 41 AM. JUR. 3D *Proof of Facts* § 1, at 8 (1997).
123 FED. R. CIV. P. 26(f)(3)(C).
124 FED. R. CIV. P. 34(b)(1)(E).
125 *See* Kevin A. Griffiths, *The Expense of Uncertainty: How a Lack of Clear E-Discovery Standards Puts Attorneys and Clients in Jeopardy*, 45 IDAHO L. REV. 441, 467–68 (2009).
126 *See* 100 AM. JUR. 3D *Proof of Facts* 89 § 4, at 117 (2008).
127 Mazzone, *supra* note 102, at 11.
128 *See* 41 AM. JUR. 3D *Proof of Facts* §11, at 25 (1997).
129 *See* Mazzone, *supra* note 102, at 9–10.

create more data.[130] The search and retrieval process for social networking data is comparable to "finding a needle in a haystack."[131] A search of this magnitude could quickly deem the discovery of such information to be overly burdensome. In this event, the most viable option for a party seeking discovery from an employee's social networking Web site account is to file a motion to compel discovery from the employee or subpoena the employee or social networking site itself.

C. Compelling Discovery

Under Rule 37(a), a party may make a motion for an order to compel discovery from a party or nonparty.[132] If a party or nonparty fails to produce discovery, then a subpoena may be sought to compel discovery.[133]

1. Third Party Subpoenas: Subpoenaing Social Networking Web Sites

The advantage of using subpoenas is that they are equivalent to a court order backed by sanctions.[134] Even nonparties, such as former co-employees, can be compelled by a subpoena "to provide information and materials critical to the outcome of the case."[135] The scope of a subpoena is essentially the same as discovery because it is a formal extension of discovery.[136] When an employee is unable or unwilling to produce information from their social networking account for an opposing party, the use of a subpoena provides an attractive option for the party to compel the employee's compliance.

Social networking Web sites are subject to subpoena just like any other business or person. As the custodian of records, subpoenaing the social networking site itself may be the best way to gain the information sought from the employee.[137] Courts have upheld the issuance of these subpoenas when the dis-

---

130 *See id.* at 10.
131 *Id.*
132 FED. R. CIV. P. 37(a)(1)–(a)(2).
133 *See* FED. R. CIV. P. 45(a)(1)(A)(iii).
134 *See* FED. R. CIV. P. 45(e).
135 Becker, *supra* note 113, at 941.
136 *See id.* at 941–42.
137 *Cf.* Declan McCullagh, *Facebook Fights Virginia's Demand for User Data, Photos*, CNET NEWS, Sept. 14, 2009, http://news.cnet.com/8301-13578_3-10352587-38.html (discussing objections by Facebook to complying to a subpoena which ordered it to provide an employer with information from a former employee's account). The Electronic Communications Privacy Act of 1986 protects users and subscribers of "computer storage or processing services" on electronic communications systems by placing restrictions on disclosure of their information. *See* Posting of Greg Nojeim, *More on YouTube v. Viacom v. User Privacy*, to CENTER FOR DEMOCRACY & TECHNOLOGY, http://www.cdt.org/blogs/greg-nojeim/more-youtube-v-viacom-v-user-privacy (July 7, 2008). However, it is unclear how

covery sought is relevant to the lawsuit.[138] In *Ledbetter v. Wal-Mart Stores, Inc.*, two employees sued their employer for injuries they suffered at the workplace.[139] The defendant-employer sought to introduce information obtained from the plaintiffs' Facebook and MySpace accounts which showed that the plaintiff-employees were drug users.[140] Despite the employees' objections, the magistrate judge allowed the defendants to subpoena Facebook and MySpace to produce information from the employees' accounts because the discovery was "reasonably calculated to lead to discovery of admissible evidence . . . ."[141]

Many Web sites allow users to post materials anonymously.[142] A subpoena to a social networking site can be used to unveil the identity of an anonymous user, but neither the Federal Rules of Civil Procedure nor Congress have addressed when these sites must provide information about their users.[143] Courts granting a subpoena served upon a Web site to reveal the identity of an anonymous user must balance the injured party's interest in seeking legal recourse with the user's First Amendment right to speak anonymously on the Internet.[144] However, speech that constitutes a tortious or criminal act has diminished protection under the First Amendment.[145] The Federal Rules of Civil Procedure have not addressed this issue and "courts have reached widely divergent results" in developing tests to determine whether to grant a subpoena revealing the identity of an anonymous Internet poster.[146]

Whether content stored on social networking sites is classified as public or

---

the ECPA applies to social networking Web sites and what protection users have from subpoenas issued to such sites. *Id*.

138 Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009).

139 Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2008 WL 2020313, at *1 (D. Colo. May 9, 2008).

140 Plaintiffs' Motion in Limine to Exclude Any Evidence of Alleged Use of Alcohol and Marijuana by Plaintiff Joel Ledbetter, Ledbetter v. Wal-Mart Stores, Inc., No. 106CV01958, 2009 WL 5863679 (D. Colo. Nov. 13, 2009).

141 Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D. Colo. April 21, 2009).

142 *See* Anthony Ciolli, *Technology Policy, Internet Privacy, and the Federal Rules of Civil Procedure*, 11 YALE J.L. & TECH. 176–79 (2009).

143 *See id.* at 176–77.

144 *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) ("[A]n author's decision to remain anonymous . . . is an aspect of the freedom of speech protected by the First Amendment."); Reno v. ACLU, 521 U.S. 844, 870 (1997) (holding that the level of First Amendment scrutiny should not be qualified for Internet speech); *see also* Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) ("Anonymous [I]nternet speech in blogs or chat rooms in some instances can become the modern equivalent of political pamphleteering.").

145 *See* Beauharnais v. Illinois, 343 U.S. 250, 266 (1952) ("Libelous utterances [are] not [within] the area of constitutionally protected speech."); In re Does 1-10, 242 S.W.3d 805, 820 (Tex. App. 2007) (recognizing that an anonymous tortfeasor's interest in retaining anonymity in his speech is limited).

146 Ciolli, *supra* note 142, at 176–77, 188.

private will affect whether the user is protected by the First Amendment.[147] In *Maldonado v. Municipality of Barceloneta*, the plaintiff sought a protective order to bar the defendant from contacting the plaintiff's witness because the defendant sent a threatening Facebook message to the witness.[148] The court stated that a Facebook message was not equivalent to a blog posting or an e-mail, but rather likely a "hybrid of the two."[149] The court noted that judicial bodies had not yet considered the classification of a Facebook message.[150] The determination of whether a Facebook message is equivalent to a blog posting or an e-mail is important because publically accessible messages are in the public domain and are protected by the First Amendment.[151] The court held that because Facebook messages are not publicly viewable, they were not in the public domain and therefore not entitled to First Amendment protection.[152] Thus, a party seeking to subpoena a social networking site will face two problems: determining whether content is public or private and the unclear standards for determining when an anonymous Internet user's identity can be revealed.

IV. LIMITS ON DISCOVERY

Even if discovery of an employee's social networking account overcomes the challenges of relevancy and is within the employer's possession, custody, or control, it may be excluded from discovery if it is privileged, if it would impose an undue burden or cost on the parties, or if the employee has superseding privacy interests in the account.

A. Limiting Discovery for Privilege; Limiting Otherwise Discoverable Material

Rule 26(b)(5) provides that otherwise discoverable information may be withheld if the information is privileged.[153] Commonly asserted privileges include attorney-client privilege, commercial trade secrets, private settlement agreements, and employment confidentiality agreements.[154] Rule 26(b)(2)(C) provides when a court must limit otherwise discoverable material on a motion

---

147 *See, e.g.*, Maldonado v. Municipality of Barceloneta, Civil No. 07-1992 (JAG)(JA), 2009 WL 636016, at *2 (D. P.R. Mar. 11, 2009).
148 *Id.* at *1.
149 *Id.* at *2.
150 *Id.*
151 *Id.*
152 *Id.*
153 FED. R. CIV. P. 26(b)(5).
154 *See* Becker, *supra* note 113, at 952–78 (2003).

or on its own determination.[155] Discovery requests that are "unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive . . ." may be denied by the court.[156]

The possibility exists that employees will use social networking sites to transfer privileged information. A court's granting or limiting of a discovery request is determined on a fact-specific basis.[157] An employer could seek to use Rule 26(b)(2)(C) to argue that it should not be forced to comply with subpoenas seeking an employee's social networking activities because under the Rules, a party must seek the discovery from the less burdensome source, and in such a case, it would be more appropriate for a party to seek the discovery from the employee themselves or the social networking Web site.

B. Limiting E-Discovery because of Undue Burden or Cost

Rule 26(b)(2)(B) provides that a party does not have to produce ESI that is "not reasonably accessible because of undue burden or cost."[158] The Rule provides exception to the production of discovery when the material is too expensive to obtain in relation to its relevance to the case.[159] One court has ranked computer data from most to least accessible form in the following order: near-line data, offline storage/archives, backup tapes, and erased, damaged, or fragmented data.[160] Generally, backup tapes and erased, damaged, or fragmented data are considered inaccessible forms of data, while the other forms of data are considered accessible.[161] One judge has suggested that data that is routinely used is considered accessible data while disaster recovery data, data from obsolete systems, and some deleted data are considered inaccessible forms of data.[162] Ultimately, a balancing test must be used weighing the benefit versus the burden of recovering the data.[163]

---

155 FED. R. CIV. P. 26(b)(2)(C).

156 FED. R. CIV. P. 26(b)(2)(C)(i).

157 *See* 8 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2009, at 124 (2d. ed. 1994).

158 FED. R. CIV. P. 26(b)(2)(B).

159 *See id.*; *see also* Griffiths, *supra* note 125, at 461–62.

160 W.E. Aubuchon Co., Inc. v. BeneFirst, LLC, 245 F.R.D. 38, 42 (D.Mass. 2007) (quoting Zubulake v. UBS Warburg, 217 F.R.D. 309, 318–19 (2003)).

161 *Id.*

162 Peck, *supra* note 15, at *45.

163 *Id.* at *47.

C. Limiting Discovery because of Privacy Interests

Rule 26(c) provides that, upon a showing of good cause, a court may issue a protective order that limits, forbids, or specifies the terms of a discovery request.[164] This is a useful tool to allow for broad production of appropriate discovery, while redacting select information that may expose a party to "annoyance, embarrassment, oppression, or undue burden or expense."[165] Accordingly, protective orders may be used to protect the privacy interests of those whose affairs may be the subject of a discovery request.[166]

Evaluating privacy rights of a user's social networking site account in civil litigation presents difficulties because few cases directly address the issue.[167] Determining whether employee privacy rights may limit the discoverability of their social networking activity on the employer's computers only complicates this problem when considering employer interests in monitoring computer use and third party litigants' interest in obtaining discovery.

1. Employee Privacy

Under the Fourth Amendment, only those reasonable privacy interests are protected.[168] This means that a person must have had a subjective belief of privacy and this expectation must be one that society recognizes as "reasonable."[169] Generally, there is no reasonable expectation of privacy in a conversation held in a public space because no subjective expectation can exist that the conversation will remain private.[170] Whether one's expectation of privacy is reasonable is determined on a case-by-case basis.[171] In the context of an employee's privacy expectation in their workplace, the employee's expectation is "assessed in the context of the employment relation[ship]."[172]

An employee's privacy's interest is limited to those areas that they exclusively control.[173] When an employee has been provided notice by their em-

---

164 FED. R. CIV. P. 26(c)(1).

165 *See id.*

166 *See id.*

167 *See, e.g.*, Don P. Palermo, *The Danger of Self-Inflicted Damage on the Web*, S. CAROLINA LAW., July 2008, at 19.

168 Katz v. U.S., 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

169 *Id.*

170 *Id.*

171 O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.").

172 *Id.* at 717.

173 *See id.* at 718 (stating that an employee had a reasonable expectation of privacy in his desks and file cabinets because the employee did not share them with others); *see also* Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir. 1987).

ployer that their work areas are subject to search for work-related purposes, the employee loses his reasonable expectation of privacy in those areas.[174] Similarly, if other employees or customers have access to the employee's area, then the employee's expectation of privacy is diminished.[175]

The Supreme Court has recognized that employees have two personal privacy interests: protecting personal information from misappropriation ("informational privacy") and freedom from intrusion in making personal decisions ("autonomy privacy").[176] Even when an employee seeks to keep their personal information private, an employer's interest to the information may prevail if the information is related to the employee's employment.[177] Because users of social networking Web sites post considerable amounts of personal information on their accounts, an employer has considerable interest in accessing this information to avoid negligently retaining or hiring employees.[178] When employers discover information on their employees' social networking accounts that suggest the employee has acted in a way that conflicts with their job responsibilities, the employer may seek to terminate the employee. In one instance, a police sheriff was fired from his job after the sheriff's department discovered comments he made on his MySpace page which demeaned women and stated that he drank heavily.[179]

2. Employee Privacy in Computer Use

An employee loses a reasonable expectation of privacy to their computer activity when the information becomes publicly viewable. This can occur when others are able to physically see the employee's computer activities,[180] a com-

---

174 *See O'Connor*, 480 U.S. at 718–19; *Schowengerdt*, 823 F.2d at 1335. *Cf.* United States v. Speights, 557 F.2d 362, 365 (3rd Cir. 1977) (finding that a police officer had a reasonable expectation of privacy in his locker that was secured by a lock provided by the officer where there was no police department practice or policy of searching such lockers).

175 *See, e.g.*, *O'Connor*, 480 U.S. at 715–17; Nelson v. Salem State Coll., 845 N.E.2d 338, 344, 347 (Mass. 2006) (holding that an employee who locked an office door and undressed inside to apply medication had no reasonable expectation of privacy because other employees had access to the office and the office was not limited to the employee's exclusive use).

176 *See* Whalen v. Roe, 429 U.S. 589, 599–600 (1977).

177 *See, e.g.*, French v. United Parcel Serv., Inc., 2 F.Supp.2d 128, 131 (D. Mass. 1998) ("[T]here are circumstances in which it is legitimate for an employer to know some 'personal' information about its employees, so long as the information reasonably bears upon the employees' . . . employment responsibilities.").

178 *See, e.g.*, Joshua C. Gilliland & Thomas J. Kelley, *Modern Issues in E-Discovery*, 42 CREIGHTON L. REV. 505, 519–20 (2009) (discussing situations where employees have been terminated or investigated by their employer for comments they have posted on their personal social networking account pages).

179 *Id.* at 519.

180 *See, e.g.*, Doe v. XYC Corp., 887 A.2d 1156, 1166 (N.J. Sup. Ct. App. Div. 2005).

pany policy allows the employer to monitor and search the computer,[181] the employee sends e-mails over the employer's network,[182] or the employee fails to prevent others from accessing his files while connected to the employer's network.[183] In *In re Asia Global Crossing, Ltd.*, the United States Bankruptcy Court considered the following factors in assessing an employee's expectation of privacy in computer and e-mail files: (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[184]

If any of these questions is answered affirmatively, then an employee has a diminished expectation of privacy in their computer use.[185]

3. Privacy in Internet Use and Social Networking Sites

When employees place information on the Internet without taking measures to protect the information, the employee does not have a legitimate expectation of privacy in such information because the Internet is a public medium.[186] A person cannot maintain a subjective belief that information placed on the Internet will be kept private since such actions show the person wishes to waive their privacy interest.[187] Most notably, one court has suggested that even when protectionist measures, such as password-protecting access to materials placed on the Internet, are taken, the materials are not considered private because they *could* be accessed by the public.[188] In *United States v. Gines-Perez*, the court held that when evaluating privacy on the Internet, the objective nature of the medium in which information is contained is ultimately dispositive and will override the subjective intention of a person who places information on the

---

[181] *See, e.g.*, Biby v. Bd. of Regents, 419 F.3d 845, 850–51 (8th Cir. 2005) (holding that a university employee had no expectation of privacy in their computer files when the university had a policy that allowed it to search files in the event of a discovery request).

[182] *See, e.g.*, Smyth v. Pillsbury Co., 914 F.Supp. 97, 101 (E.D. Pa. 1996) (holding that an employee loses any reasonable expectation of privacy in an e-mail once the employee sends the e-mail over a company e-mail system).

[183] *See, e.g.*, United State v. Barrows, 481 F.3d 1246, 1248–49 (10th Cir. 2007) (holding that an employee who brought his personal computer to work had no reasonable expectation of privacy in the computer because it was used for work purposes on a non-password protected file-sharing network).

[184] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (S.D. N.Y. 2005).

[185] *See id.* at 257–58.

[186] United States v. Gines-Perez, 214 F. Supp.2d 205, 225 (D.P.R. 2002).

[187] *See id.*

[188] *Id.*

Internet.[189]

Therefore, a social networking site user's expectation of privacy should be measured against the degree to which other users and the public can access the information they upload.[190] As in *Maldonado*, litigants will have a significant interest in a court's determination of whether the content they provide on a social networking site is private or public.[191] Unfortunately, users of social networking sites may be relinquishing a significant amount of personal information under the false assumption that the information is not available to the public.[192] An attempt to assert a subjective expectation of privacy in a social networking account that is relevant to the lawsuit will "face an uphill battle."[193] Even if a user restricts access to their information through the site's privacy settings, most social networking sites warn users that they cannot control how recipients may distribute their information.[194] The possibility of inadvertently publicizing "private" user content on social networking Web sites makes an objective expectation of privacy unreasonable.[195]

4. Countervailing Employer Interests

Where an employer furnishes a computer or e-mail account to an employee, the employee's privacy rights tend to be inferior to the employer's property rights in the computer or e-mail network.[196] When an employer has an official policy that reserves the right to inspect employer issued equipment, courts have stated that absent special circumstances, an employee does not have a reasonable expectation of privacy in messages they send using the equip-

---

189 *Id.* at 226. ("[T]he Court underscores that it is not the subjective intention of the person that places information on the web which is important, but the objective use of the medium itself, and the objective nature of the materials, which are truly pivotal.").

190 *Cf.* Millier, *supra* note 27, at 542–43, 550–52.

191 *See* Maldonado v. Municipality of Barceloneta, Civil No. 07-1992 (JAG)(JA), 2009 WL 636016, at *2 (D. P.R. Mar. 11, 2009).

192 Brian Kane & Brett T. Delange, *A Tale of Two Internets: Web 2.0 Slices, Dices, and is Privacy Resistant*, 45 IDAHO L. REV. 317, 332–33 (2009) (discussing the false sense of security users of social networking sites have in sharing personal information).

193 Levine & Swatski-Lebson, *supra* note 73, at 2–3 (discussing why it is not feasible for a user of a social networking site to have a subjective expectation of privacy in their profile).

194 *Id.* at 3 ("To prove a subjective expectation of privacy, users have to first overcome the inherent assumption that they intended to publicize their information.").

195 *See id.* ("Since these sites' privacy policies recognize and even caution that any posted information may become public, a user may not be able to contend reasonably that such information is private and in the case of litigation, non-discoverable.").

196 *See* Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829, 835–36 (2005) (noting that without property rights to a computer, the employee will have no privacy interest).

ment.[197] But even when such policies exist, the Court of Appeals for the Ninth Circuit recently held in *Quon v. Arch Wireless, Inc.*, that an employer's unofficial policy and practice of not inspecting its employees' communications may provide the employee with a reasonable expectation of privacy.[198] The Supreme Court has granted certiorari in the case to review whether an employee has a reasonable expectation of privacy when the employer has conflicting official and unofficial privacy policies.[199]

An employee's privacy rights in a computer will not trump the employer's interest in monitoring the employee's computer to ensure productivity and avoid potential liability.[200] In *Smyth v. Pillsbury Co.*, the court recognized that an employer's "interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee . . ." has in those activities.[201] Monitoring employees often may be an ordinary part of conducting business.[202] Monitoring computer use is not unreasonable, but rather a necessary policy, given the common abuse of workplace computers.[203]

Given the legitimacy of monitoring, employee privacy in computer activity will be inversely correlated to the extent that the employer monitors it.[204] In *Muick v. Glenayre Electronics,* the United States Court of Appeals for the Seventh Circuit held that where an employer has a company policy that permits it to inspect its computers' files, no employee can have any reasonable expectation of privacy in their computer.[205] The court found that an employer may attach conditions to an employee's use of its computer and that an employer's monitoring and searching of the computer, in light of reserving such rights, is permissible.[206]

In *Garrity v. John Hancock Mutual. Life Insurance Co.*, the United States

---

197 Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002).

198 *See* Quon v. Arch Wireless, Inc., 529 F.3d 892, 906–07 (9th Cir. 2008), *cert. granted*, 78 U.S.L.W. 3359 (U.S. Dec. 14, 2009) (No. 08-1332).

199 *Id.*

200 *See* Stengart v. Loving Care Agency, Inc. 973 A.2d 390, 401 (N.J. Super. Ct. App. Div. 2009) (stating that employers maintain a legitimate right to monitor their employees' communications on workplace computers for the purpose of disciplining employees).

201 Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

202 *See* Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 922–23 (W.D. Wis. 2002).

203 *See* Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002) ("[T]he abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.").

204 *See* O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (stating that the employment relationship provides the context for measuring an employee's expectation of privacy).

205 *Muick*, 280 F.3d at 743.

206 *Id*.

District Court for the District of Massachusetts went one step further stating that, "[e]ven if [employees] ha[ve] a reasonable expectation of privacy in their work e-mail, [an employer's] legitimate business interest in protecting its employees from harassment in the workplace would likely trump any [employee] privacy interests."[207] An employer's interest in monitoring employee computer use appears to be on solid legal footing when it involves the employer's resources and work-related channels of communication.

In contrast, an employer's legitimate interest in monitoring employee computer use for personal communications is much weaker. In *Stengart*, the court held that the employer's interest in monitoring the employee's personal computer use was limited to purposes related to monitoring the employee's job performance, not the content of the employee's personal communications.[208] Likewise, employers typically do not have a duty to monitor the private, personal communication of employees.[209]

However, in *Doe v. XYC Corp*., the court recognized that an employer's right to monitor an employee's computer trumps an employee's privacy when the employer has a duty to protect a third party from harm caused by the employee.[210] If an employer is on notice that an employee is using their computer to injure another, then the employer may be required by law to search and monitor the employee's computer use.[211] Therefore, an employer should not be able to monitor an employee's personal social networking accounts unless it is on notice that the employee is using the site at their workplace to harm others. However, an employer should retain the limited ability to monitor its employees' use social networking accounts, excluding the content therein, to ensure employee productivity.

Employers must decide how much access employees should have to the Internet.[212] Although employers have an interest in preventing employees from

---

[207] Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002).

[208] Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 401 (N.J. Super. Ct. App. Div. 2009).

[209] Blakey v. Continental Airlines, Inc., 751 A.2d 538, 552 (N.J. 2000); Doe v. XYC Corp., 887 A.2d 1156, 1162 (N.J. Sup. Ct. App. Div. 2005).

[210] *See XYC Corp.*, 887 A.2d 1156, 1158 (N.J. Sup. Ct. App. Div. 2005) (holding that when an employer has notice that its employees' activities may be harming someone, it has a duty to investigate the employee's activities and to prevent its employee from causing harm).

[211] *See, e.g.*, Garrity v. John Hancock Mut. Life Ins. Co., No. Civ.A. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002) ("[O]nce the [employer] received a complaint about the [employees'] sexually explicit e-mails, it was required by law to commence and investigation.").

[212] *See* MessageLabs, *Employee Web Use and Misuse: Companies, Their Employees, and the Internet* 2–3 (MessageLabs, 2008), *available at* http://whitepapers.zdnet.com/abstract.aspx?docid=397147 (click "download" hyperlink).

engaging in a number of inappropriate activities, allowing some employee access to social networking sites may be innocuous.[213] In addition, businesses may want to vary Internet use restrictions among individuals and departments in the company.[214] For example, an employer may want to permit its human resources department to access Facebook in order to screen potential recruits, while prohibiting its accounting department from accessing the site.[215] Ultimately each employer needs to base its employees' Internet access policy on its own needs and interests.

5. Home Computers

The distinction between personal and work-related uses of an employer's computer is quickly blurred when discovery requests seek such computers that are used in the employee's home. Different privacy issues concerns arise in such a case because home computers contain more personal information than office computers.[216] Requests for ESI from home computers are more carefully scrutinized because home computers are more likely to have "evidence potentially intermingled with private or confidential information."[217]

In *TBG Insurance Services Corp., v. Superior Court,* an employee brought a wrongful termination suit against his employer after he was fired for using a computer furnished by his employer to visit pornographic Web sites at home.[218] The employee asserted that he had a constitutional right to privacy in the computer's contents.[219]

The California Court of Appeal held that the employee had no reasonable expectation of privacy in the home computer because the company's policy agreement with the employee provided that the computer remained company property, the computer was to be used for business purposes only, and the employer reserved the right to inspect the computer.[220] The employee claimed the company had an unofficial policy that permitted home computers to be used for personal purposes.[221] The court rejected the employee's argument on the

---

213 *See id.* (providing that while employers want to prevent their employees from accessing inappropriate content at work, employers often desire to allow their employees to access some non-work related Web sites, such as e-mail, shopping, and social networking sites).

214 *Id.*

215 *Id.*

216 *See* Brian Zayas, *Gaining E-Discovery Access to Home Computers,* L.A. LAW., Dec. 2007, at 12.

217 *Id.*

218 TBG Ins. Servs. Corp. v. Superior Court, 117 Cal.Rptr. 2d 155, 157–58 (Cal. Ct. App. 2002).

219 *Id.* at 158.

220 *Id.* at 163.

221 *Id.* at 164.

grounds that the employee could have no reasonable expectation of privacy given that the company's written policies.[222] Although the court granted the employer's motion to compel production of the employee's home computer, the court stated that the employee may have a "lingering privacy interest" in the financial information and other personal information he kept on the computer.[223] The court sent the case back to the trial court for a determination of what information on the computer was relevant to the case and what should be excluded from discovery.[224]

As with private personal correspondences, an employee's social networking activity that has no rational bearing to litigation should be excluded from discovery during a search of an employer-furnished take-home computer's files by using a protective order like the one in *TBG Insurance Services Corp*. If, however, inappropriate use of social networking sites is relevant to litigation, like accessing pornography in *TBG Insurance Services Corp.*, then an employee's account does not warrant protection during discovery.

6. Employee Privacy v. Third Party Plaintiffs Seeking Discovery

A litigant's right to obtain information relevant to his or her lawsuit will weigh the public need for the information against the opposing party's need to keep the information confidential.[225] In *Harding Lawson Associates v. Superior Court*, the California Court of Appeal held that in weighing these issues, employee privacy will be favored "unless the litigant can show a compelling need for the particular documents and that the information cannot reasonably be obtained through depositions or from nonconfidential sources."[226] Further the court held that "[e]ven when the balance does weigh in favor of disclosure, the scope of disclosure must be narrowly circumscribed."[227] Similarly, in *Beverly Enterprises v. Deutsch*, the District Court of Appeal of Florida held that a party's request for an employee's personnel files must show more than mere relevance and must show a direct relation to the legitimate issues of the case.[228] A litigant should not be allowed to make overbroad discovery requests concerning employees' personal information where a less invasive alternative exists.[229]

---

[222] *Id.* at 163–64.

[223] *Id.* at 164.

[224] *Id.* at 164.

[225] *See* Harding Lawson Assocs. v. Superior Court, 10 Cal. App. 4th 7, 10 (Cal. Ct. App. 1992).

[226] *Id.*

[227] *Id.*

[228] Beverly Enters-Florida, Inc. v. Deutsch, 765 So. 2d 778, 783 (Fla. Dist. Ct. App. 2000).

[229] *See, e.g.*, Adams v. Allstate Ins. Co., 189 F.R.D. 331, 333 (E.D. Pa. 1999) (rejecting a plaintiff's motion which sought to compel defendant insurance company to produce the

The relevancy of a discovery request directed at employees who are nonparties to the lawsuit should be strictly scrutinized and employers should seek protective orders against the request.[230]

V. CONCLUSION

As the popularity and features of social networking Web sites continue to grow, so does the possibility that employees will use them on employer-owned computers within the scope of employment or coincident thereto. The evidence that social networking sites leave behind in an employer's computer network could offer the smoking gun to a third party or co-worker seeking to impose liability against the employer for employee misbehavior. Although e-discovery was designed to provide a mechanism to produce such information, the use of social networking sites raises issues that cannot be neatly resolved by the current Federal Rules of Civil Procedure, case law, and technology. Litigants and courts will spend significant time and money to overcome the growing pains of e-discovery, and e-discovery must evolve to handle employee social networking activity. Further judicial or legislative reform will be required for a streamlined procedure.

---

personnel files of every employee who handled plaintiff's claim because the request was overbroad and "unnecessarily invasive").

[230] Levine & Swatski-Lebson, *supra* note 73, at 1.