

Pace Law Review

Volume 31

Issue 1 *Social Networking and the Law*

Winter 2011

Article 1

January 2011

Social Networking and Workers' Compensation Law at the Crossroads

Jaelyn S. Millner

Fitch, Johnson, Larson & Held, P.A.

Gregory M. Duhl

William Mitchell College of Law

Follow this and additional works at: <http://digitalcommons.pace.edu/plr>

 Part of the [Workers' Compensation Law Commons](#)

Recommended Citation

Jaelyn S. Millner and Gregory M. Duhl, *Social Networking and Workers' Compensation Law at the Crossroads*, 31 Pace L. Rev. 1 (2011)

Available at: <http://digitalcommons.pace.edu/plr/vol31/iss1/1>

This Article is brought to you for free and open access by the School of Law at DigitalCommons@Pace. It has been accepted for inclusion in Pace Law Review by an authorized administrator of DigitalCommons@Pace. For more information, please contact cpittson@law.pace.edu.

Social Networking and Workers' Compensation Law at the Crossroads

Jaclyn S. Millner* and Gregory M. Duhl**

Abstract

Over the past decade, social networking has increasingly influenced the practice of both civil and criminal law. One way to illustrate those influences is to examine a “system” of laws and the parties and lawyers in that system. In this Article, we examine how social networking has influenced workers' compensation law. In particular, this Article looks at the intersection of professional responsibility, discovery, privacy, and evidence with social networking in state workers' compensation systems.

Workers' compensation laws are no-fault insurance systems designed to resolve disputes efficiently. Consequently, the rules of evidence are often more relaxed and the rules of discovery often more restricted than in state and federal court litigation. The flexible and self-contained structure of workers' compensation systems provides an ideal backdrop against which to examine how information from social networking sites

* Jaclyn S. Millner is an attorney at Fitch, Johnson, Larson & Held, P.A., a workers' compensation defense firm in Minneapolis, Minnesota. She is licensed to practice in Wisconsin and Minnesota. She has a B.A. from the University of Michigan and a J.D. magna cum laude from the William Mitchell College of Law in St. Paul, Minnesota. She was an editor of the *William Mitchell Law Review*.

** Gregory M. Duhl is an Associate Professor of Law at the William Mitchell College of Law in St. Paul, Minnesota, as well as the executive editor of *The Business Lawyer*, the flagship publication of the ABA Section of Business Law. Professor Duhl received a B.A. summa cum laude from Yale University, a J.D. cum laude from Harvard Law School, and an LL.M. in Legal Education from the Temple University James E. Beasley School of Law. He thanks Kathleen Byrne, Nicky Kurtzweil, and Jill Schrader for their excellent research assistance.

can be used as evidence to resolve civil disputes.

A state's workers' compensation system should use the rules that have traditionally applied to non-electronic information as a starting point to address issues arising from lawyers gathering and introducing into evidence information stored on social networking sites. At the same time, because of the efficiency of workers' compensation law and the large discretion vested in its judges, workers' compensation systems have the potential to be laboratories for new technologies and how they can be used in the resolution of disputes, both inside and outside of workers' compensation.

I. Introduction

Workers' compensation systems¹ provide a backdrop against which to examine how lawyers and judges can use evidence from social networking sites to help resolve civil disputes. An employee² alleging a workplace injury can communicate feelings, information, or photographs on a social networking site that contradict her claim. While the employee's attorney should counsel her client to exercise caution in making such communications, defense counsel³ faces the

1. Each state has its own workers' compensation system governed by state statute and administrative rules. See *Office of Disability Employment Policy*, U.S. DEP'T OF LABOR, <http://www.dol.gov/odep/pubs/fact/employ.htm> (last visited Aug. 22, 2010) ("Workers' Compensation laws are administered at the state level. . . . Because each state has its own system, coverage varies."). In this Article, we focus on the common elements of those systems.

2. We use "employee" and "plaintiff" interchangeably in this Article to refer to the workers' compensation claimant. The claimant could be a former employee if employed at the time the alleged injury occurred.

3. In workers' compensation litigation, the "defense" includes both the employer and insurer. The employer contracts with the insurer to provide workers' compensation coverage. We use "defense counsel" in this Article to refer to counsel for the employer and the insurer, whether the same or different. The insurer typically controls the litigation, as the insurer is the party paying workers' compensation benefits to the employee. See, e.g., *Herring v. Jackson*, 122 S.E.2d 366, 371-72 (N.C. 1961) (finding the insurer to be the "real party in interest" because the employer had nothing to gain or lose in the action and any recovered amount would inure to the insurance company); *Russell v. W. Oil Co.*, 174 S.E. 101, 104 (N.C. 1934) ("The insurer is practically the real party to the controversy and controls the litigation."). Most workers' compensation insurance policies also provide language

challenge of gathering and introducing such communications into evidence.⁴

Despite this potential for social networking evidence, its use in workers' compensation cases and civil litigation more generally is uncommon. Consequently, there is a relative absence of cases, statutes, rules, and ethics opinions that prescribe attorney conduct in gathering and introducing such evidence. Because workers' compensation systems are intended to be discrete, efficient, and discretionary, they are ideal systems within which to explore how social networking and other new technologies can be used in the resolution of disputes.

Workers' compensation laws are no-fault, providing compensation for job-related injuries⁵ and offering a more efficient mechanism for claim resolution than trial courts.⁶ They protect employees by providing assured and prompt compensation for work-related injuries and consequential loss of income without the parties and attorneys expending the excessive time and resources typical of state and federal court litigation.⁷

indicating that the insurer controls the litigation, and the employer must assist the insurer in litigation against the employee upon request.

4. See Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, MINN. BENCH & B., Nov. 2009, at 23, available at <http://www.mnbar.org/benchandbar/2009/nov09/networking.html>

("Experienced attorneys know that embracing new technologies—such as social networking sites—can make the difference between winning and losing cases.").

5. See, e.g., CAL. CONST. art. XIV, § 4 ("The Legislature is hereby expressly vested with plenary power, unlimited by any provision of this Constitution, to create, and enforce a complete system of workers' compensation, by appropriate legislation, and in that behalf to create and enforce a liability on the part of any or all persons to compensate any or all of their workers for injury or disability, and their dependents for death incurred or sustained by the said workers in the course of their employment, irrespective of the fault of any party."); *Curtis v. G.E. Capital Modular Space*, 155 S.W.3d 877, 884 (Tenn. 2005) ("To do so would confuse the fault-based liability of tort with the statutorily imposed 'no fault' liability of workers' compensation.").

6. *United Airlines, Inc. v. Indus. Claim Appeals Office*, 993 P.2d 1152, 1161 (Colo. 2000) ("Traditionally, workers' compensation laws have provided an efficient system for remedying the effects of allocating the costs of industrial injuries.").

7. *Ruggery v. N.C. Dep't of Corr.*, 520 S.E.2d 77, 81 (N.C. Ct. App. 1999)

Similarly, social networking sites enable individuals to exchange information efficiently over the Internet.⁸ Social networking provides a structure for people to express their personalities and identities, and meet people with similar interests.⁹ Individuals can have online profiles,¹⁰ friends,¹¹ blogs, discussions, and groups.¹² Users may also post pictures, videos, and other information to their social networking profiles.¹³ By facilitating connections with friends, relatives, and those with similar interests, social networking creates a sense of intimacy and community for users.¹⁴

("The policy underlying the Worker's Compensation Act is to 'provide a swift and certain remedy to an injured worker and to ensure a limited and determinate liability for employers.'" (quoting *Matthews v. Charlotte-Mecklenburg Hosp.*, 510 S.E.2d 388, 393 (N.C. Ct. App. 1999))); *Lascio v. Belcher Roofing Corp.*, 704 A.2d 642, 644-45 (Pa. Super. Ct. 1997) ("[The] purpose of [the workers' compensation system] is to protect employees by providing quick and certain compensation for work-related injuries and resultant loss of injuries without wasting time and expenses on litigation.").

8. See Kristi L. Gustafson, *Social Networks Alter Class Reunion Dynamics*, ALBANY TIMES UNION (Apr. 29, 2010), <http://www.chron.com/disp/story.mpl/life/main/6980262.html> ("Social networking is an efficient, cost-effective way to share information.").

9. See Daniel Nations, *What Is Social Networking?*, ABOUT.COM, <http://webtrends.about.com/od/socialnetworking/a/social-network.htm> (last visited Aug. 20, 2010).

10. Profiles include basic information, including a person's age, location, and interests. See *id.*

11. "Friends are trusted members of [an individual's profile] [who] are allowed to post comments on [the] profile or send [the individual] private messages." *Id.* When a person sends an invitation to someone to become a "friend" on Facebook or another social networking site, if the individual accepts, the inviter and invitee have access to each other's information and can communicate with one another. See *Definition of Friending*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=friending&i=61604,00.asp (last visited Aug. 20, 2010). After "friending" another social networking user on the same site, friends can be subsequently "defriended" or "unfriended," which terminates the "friendship" and users' access to each other's information. *Id.* Not all social networking sites use the term "friends"; LinkedIn, for example, uses the term "connections." See Nations, *supra* note 9. However, all sites permit a user to designate another member as trusted and give that person access to the user's information. *Id.*

12. See Nations, *supra* note 9. Groups enable social networking users on a site to find people with similar interests or backgrounds. *Id.* A group can have any sort of focus, from "Diet Coke Lovers" to "Valley High School Class of 1999" to a particular book, television show, or movie. *Id.*

13. See *id.*

14. See Awsumb, *supra* note 4, at 23 ("Social networking sites are now

Nearly half of all adult Americans have a social networking profile,¹⁵ with Facebook and MySpace being the most popular sites.¹⁶ As social networking continues to play an increasingly prevalent role in society, lawyers and judges involved in workers' compensation will have to confront discovery, professional responsibility, privacy, and evidentiary issues that arise in connection with social networking evidence.¹⁷

Part II of this Article discusses legal issues related to gathering information stored on a social networking site from both the employee and social networking site operator. Part III goes on to address professional responsibility issues that arise for plaintiffs' and defense attorneys in connection with an employee maintaining, and defense counsel gathering, information stored on a social networking site. Part IV discusses issues relating to admitting social networking evidence at the time of a workers' compensation hearing or trial, after it has been obtained by defense counsel. We conclude in Part V that workers' compensation systems should use the existing rules governing the discovery and admissibility

widely recognized to be a key source of information regarding a person because "[a]lthough these sites provide users with a sense of intimacy and community, they also create a potentially permanent record of personal information that becomes a virtual information bonanza about a litigant's private life and state of mind." (quoting Ronald J. Levine & Susan L. Swatski-Lebson, *Are Social Networking Sites Discoverable?*, LAW.COM (Nov. 13, 2008), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202425974937>)).

15. See TOM WEBSTER, *THE SOCIAL HABIT—FREQUENT SOCIAL NETWORKERS: THE EDISON/ARBITRON INTERNET AND MULTIMEDIA STUDY 2010* (2010), http://www.edisonresearch.com/The_Social_Habit_Edison_Social_Media_Study_2010.pdf

(stating that a survey from February 2010 found 48% of Americans have a profile on Facebook, MySpace, or another social networking site); *Adults on Social Network Sites, 2005-2009*, PEW INTERNET (Oct. 8, 2009), <http://www.pewinternet.org/Infographics/Growth-in-Adult-SNS-Use-20052009.aspx> (stating that 46% of American adults use some type of social networking site).

16. See Awsumb, *supra* note 4, at 23.

17. See *id.* ("Experienced attorneys know that embracing new technologies—such as social networking sites—can make the difference between winning and losing cases.").

of electronic and non-electronic information as a starting point in addressing issues that arise at the crossroads of social networking and workers' compensation law. As efficient systems, providing considerable discretion to the judge, workers' compensation laws offer lawyers and judges the ability to address and explore the role of social networking evidence in dispute resolution.

II. Discovering Employee Information Stored on Social Networking Sites

This Part explores the legal issues that can arise when defense counsel seeks an employee's communications and other information stored on a social networking site. We address two topics: (A) the extent to which an employee's information stored on a social networking site is discoverable from the employee in a workers' compensation case; and (B) the extent to which an employee's information stored on a social networking site is discoverable from the third-party site operator in a workers' compensation case. The employee's privacy and the Stored Communications Act,¹⁸ part of the Electronic Communications Privacy Act,¹⁹ potentially limit discovery from the site operator.

A. *Discovery of Social Networking Information from the Employee*

This Part focuses on the rules regulating discovery²⁰ in

18. 18 U.S.C. §§ 2701-2712 (2006).

19. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

20. This Part uses the Federal Rules of Civil Procedure to discuss discovery in state workers' compensation courts. To date, the majority of states have adopted the Federal Rules of Civil Procedure, with minimal changes. See *Rules of Civil Procedure*, USLEGAL.COM, <http://civilprocedure.uslegal.com/rules-of-civil-procedure/> (last visited Aug. 20, 2010) ("[T]hirty-five states have adopted the federal rules as their own procedural code."). In most states, though workers' compensation courts are governed by administrative rules, they have adopted the state's rules of civil procedure with regard to discovery. See, e.g., FLA. ADMIN. CODE ANN. r. 60Q-6.114 (2006) (applying the Florida Rules of Civil Procedure to workers' compensation proceedings); GA. CODE ANN. § 34-9-102(d)(1) (West 2008 & Supp. 2009) ("Discovery procedures shall be governed and controlled by Chapter 11 of Title 9, the 'Georgia Civil Practice Act.'"); IDAHO JUDICIAL R.

PRAC. & P. 7(C) (2008) (“Procedural matters relating to discovery, except sanctions, shall be controlled by the appropriate provisions of the Idaho Rules of Civil Procedure.”); IND. CODE ANN. § 22-3-1-3(a) (West 2009) (“The worker’s compensation board may adopt rules under IC 4-22-2 to carry into effect the worker’s compensation law (IC 22-3-2 through IC 22-3-6) and the worker’s occupational diseases law (IC 22-3-7).”); IOWA ADMIN. CODE r. 876-4.35(86) (2009) (“The rules of civil procedure shall govern the contested case proceedings before the workers’ compensation commissioner”); OKLA. STAT. ANN. tit. 85, ch. 4, app. r. 30 (West 2005) (“[P]roduction of documentary evidence shall be obtained in accordance with Title 12 of the Oklahoma Statutes [Oklahoma state rules of civil procedure].”); OR. REV. STAT. ANN. § 656.285 (West 2003) (“ORCP [Oregon Rule of Civil Procedure] 36 C shall apply to workers’ compensation cases, except that the Administrative Law Judge shall make the determinations and orders required of the court in ORCP 36 C, and in addition attorney fees shall not be declared as a matter of course but only in cases of harassment or hardship.”); *Camelback Contractors, Inc. v. Indus. Comm’n*, 608 P.2d 782, 785 (Ariz. Ct. App. 1980) (holding that discovery before the industrial commission in Arizona “should not be more restrictive than that employed in superior court”); *Mid-Delta Home Health, Inc. v. Robertson*, 749 So. 2d 379, 388 (Miss. Ct. App. 1999) (“[The Workers’ Compensation] Commission will not disregard the time-honored guidelines of discovery”).

States such as Minnesota, which follow more restrictive rules for discovery in workers’ compensation cases to speed up the claim-resolution process, do permit the compensation judge to order discovery under the state’s rules of civil procedure. *See* MINN. R. 1420.2200, subpt. 3 (2006) (“The judge may order discovery available under the Rules of Civil Procedure for the district courts of Minnesota provided that the discovery: . . . is needed for the proper presentation of a party’s case”); *Edeogu v. Bauerly Bros., Inc.*, No. WC05-202, 2005 MN Wrk. Comp. LEXIS 247, at *5 (Minn. Work. Comp. Ct. App. Aug. 30, 2005) (stating that the workers’ compensation court may rely on the Minnesota Rules of Civil Procedure).

Moreover, some states with more restrictive discovery rules specifically permit surveillance as a form of discovery, *see, e.g.*, MINN. R. 1420.2200, subpt. 8(A) (2006), and informal discovery of social networking evidence is a form of surveillance. *Id.* (“Surveillance evidence under this part includes any photographic, video, digital, motion picture, or other electronic recording or depiction of a party surreptitiously taken or obtained without the party’s expressed permission or knowledge.”); *see also* Anders Albrechtslund, *Online Social Networking as Participatory Surveillance*, FIRST MONDAY (Mar. 2008), <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949> (“First, online social networking is related to the traditional hierarchical surveillance concept. . . . The word *surveillance* is etymologically associated with the French word *surveiller*, which translates simply as *to watch over*. The verb suggests the visual practice of a person looking carefully at someone or something from above. Both in ordinary language and within academic debate, the practice of ‘watching over’ has become a metaphor for all other monitoring activities. Thus, the understanding of surveillance is not limited to a visual practice; rather it involves all senses—data collection and technological mediation.”). Consequently, in states with restricted workers’ compensation discovery rules, defense counsel can discover social networking

workers' compensation cases and the few state and federal cases that suggest defense counsel can acquire relevant information stored on a social networking site from an employee.

1. Background of E-Discovery and the Scope of Discovery

The discovery process makes relevant information available to litigants.²¹ Electronic discovery allows parties to obtain "electronically stored information" (ESI),²² a term adopted by the amendments to the Federal Rules of Civil Procedure in 2006.²³ ESI includes digital information that can

evidence, either by following the rules for conducting surveillance or the state's rules of civil procedure.

21. See Aaron Blank, *On the Precipe of E-Discovery: Can Litigants Obtain Employee Social Networking Web Site Information Through Employers?*, 18 COMMLAW CONSPECTUS 487, 495 (2010) (citing FED. R. CIV. P. 26 advisory committee's note (1983)). "Discovery" describes evidence obtained during the pre-trial stage of a lawsuit. See Ken LaMance, *Electronic Discovery—Can Contents of My Electronic Communications Be Used as Evidence in Court?*, EZINE ARTICLES, <http://ezinearticles.com/?Electronic-Discovery---Can-Contents-of-My-Electronic-Communications-Be-Used-As-Evidence-in-Court?&id=3962081> (last visited Aug. 20, 2010).

22. FED. R. CIV. P. 26(a)(1)(A)(ii), 33(d), 34(a)(1)(A); see also LaMance, *supra* note 21 ("Electronically Stored Information, or 'ESI,' is an actual legal term adopted by the Federal Rules of Civil Procedure in 2006. ESI refers to information that is created, stored, and used in digital form, and requires the use of a computer for access.").

23. Blank, *supra* note 21, at 495-96; LaMance, *supra* note 21; see FED. R. CIV. P. 26. The advisory committee found the amendments to be necessary for two primary 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 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.

REPORT OF THE CIVIL RULES ADVISORY COMMITTEE (July 25, 2005), SL061 ALI-ABA 1101, 1103 (Westlaw).

be accessed only by computer.²⁴ The rules regulating discovery more generally also govern ESI.²⁵

Federal Rule of Civil Procedure 26(b)(1) outlines the scope of discovery, including the discovery of ESI. The scope of discovery is broad, and non-privileged information that is “relevant to any party’s claim or defense” is discoverable.²⁶ States that follow more limited rules of discovery for workers’ compensation claims also use a relevancy standard with respect to discovery of surveillance evidence,²⁷ which includes information stored on a social networking site. The standard for determining “relevance” is “whether there is any possibility that the information sought may be relevant to the subject matter of the action.”²⁸

As social networking continues to become more widespread, information relevant to employees’ workers’ compensation claims could be available on Facebook and other social networking sites.²⁹ Such sites serve as a significant

24. LaMance, *supra* note 21. Examples of ESI include e-mails, websites, and digitally stored documents and pictures. *Id.*

25. *See id.*

26. FED. R. CIV. P. 26(b)(1).

27. *See, e.g.*, MINN. R. 1420.2200, subpt. 8(A) (2006) (indicating that *relevant* surveillance evidence is discoverable).

28. *AM Int’l, Inc. v. Eastman Kodak Co.*, 100 F.R.D. 255, 257 (N.D. Ill. 1981) (citation omitted) (internal quotation marks omitted); *see also* *TBG Ins. Servs. Corp. v. Superior Court*, 117 Cal. Rptr. 2d 155, 160 (Ct. App. 2002) (“[The defendant] is entitled to discover any non-privileged information, cumulative or not, that may reasonably assist it in developing its defense, preparing for trial, or facilitating a settlement.”); Blank, *supra* note 21, at 496 (“[The test for relevance is] whether there is any possibility that the information sought may be relevant to the subject matter of the action.” (quoting *AM Int’l*, 100 F.R.D. at 257) (internal quotation marks omitted)).

29. *See* *Awsumb*, *supra* note 4, at 25 (“Attorneys can discover the user’s postings, list of friends, shared photos and videos, and other valuable information. If a person has heightened security settings, attorneys may still be able to discover the social networking account, but will not be able to access the person’s profile information unless the user provides permission through granting a ‘friend’ request. Even if attorneys can only gather limited information informally, that information can provide a means to tailor subsequent formal discovery.”); Leora Maccabee, *Facebook 101: Why Lawyers Should Be on Facebook*, LAWYERIST.COM (Apr. 23, 2009), <http://lawyerist.com/facebook-101-why-lawyers-should-be-on-facebook/> (“Facebook can be an effective tool for investigating defendants, witnesses, and prosecutors. Evidence revealed from profile searches has been used . . . to show the extent of plaintiffs’ injuries after an accident.”). Take one example

information source because, “[a]lthough [they] provide users with a sense of intimacy and community, they also create a potentially permanent record of personal information that becomes a virtual information bonanza about a litigant’s private life and state of mind.”³⁰ An employee alleging a workplace injury could post photographs, communications, or other information that either contradict a workplace injury claim, or alert defense investigators of times and places to engage in surveillance.³¹

2. Informal Discovery

Social networking information can be discovered both formally and informally. Attorneys can informally discover information by searching on Google, Yahoo!, or any other search engine for the employee and seeing if a link to an employee’s social networking account comes up in the results.³² In addition, attorneys can search individual social networking

from a products liability case. A federal district court dismissed a welder’s claim when defense lawyers discovered pictures of him on Facebook racing motorboats despite his disability claims. See Liz McKenzie, *Poking Around Facebook Could Win Your Case*, LAW360 (Feb. 4, 2010), <http://www.law360.com/articles/147130>.

30. Awsumb, *supra* note 4, at 23 (quoting Levine & Swatski-Lebson, *supra* note 14).

31. Roberto Ceniceros, *Comp Cheats Confess All on Social Networking Sites*, WORKFORCE MGMT. ONLINE (Sept. 2009), <http://www.workforce.com/section/02/feature/26/66/08/> (“Then there is the listing of physical activities [I]nvestigators found the claimant’s Facebook site and learned about his participation in bowling tournaments and a bowling alley he frequented. . . . An investigator visiting the bowling alley found a large banner congratulating the claimant for rolling a perfect game and the date he rolled the game.”); Michael O’Connor & Assocs., LLC, *Workers’ Compensation Investigators Use Social Networking Sites to Nab Fraudulent Claimants*, PA. WORKERS’ COMPENSATION LAW. BLOG (Sept. 30, 2009, 9:19 AM), <http://www.pennsylvaniaworkerscompensationlawyersblog.com/2009/09/workers-compensation-investiga.html> (“By searching for a claimant’s profile on sites like Facebook or MySpace, investigators can uncover a myriad of self-incriminating information, such as dates of sporting events in which the claimant is participating. Social networking sites can also contain time-stamped photos and videos showing claimants involved in physical activities that could be outside the level of disability that the injured worker is claiming.”).

32. See Awsumb, *supra* note 4, at 23.

sites, such as Facebook and MySpace, by the name of the employee.³³

Whether an individual's social networking profile and information can be publicly viewed depends on the particular social networking website and the individual's specific security settings. By using the site's control settings, users of Facebook, MySpace, and other social networking sites are able to control whether the information provided on their profile is public or private.³⁴ A user may place his or her security settings on a spectrum ranging from a completely public profile, which may be viewed by anyone, to a private profile, which is accessible only to individuals the user accepts as "friends" or "connections."³⁵ Just as a workers' compensation attorney may use informal discovery to observe an employee in a public place, such as a park or a restaurant,³⁶ so too is a workers' compensation attorney able to use informal discovery to observe and search information publicly available online. When conducting informal discovery, however, attorneys should be cognizant of professional responsibility obligations.³⁷

33. *See id.*

34. *See id.* ("Most social networking sites, including Facebook and MySpace, enable individual users to control whether their information is private or public and to whom it can be disseminated.")

35. *See id.* ("The security settings range from uncensored, public profiles that can be accessed and located through the social networking site or any Internet search engine, to private profiles, accessible only to persons designated as friends.") If a particular user's Facebook account, for example, has low security settings, the general public can access the individual's profile by searching the Internet or by searching for the person's name on the Facebook website. Attorneys and others can discover the individual's list of friends, shared postings, photographs, and videos. *See id.* at 24. If an individual sets high security settings, attorneys may still be able to discover that the individual has a Facebook account but will not be able to view the individual's profile or information unless the individual allows the attorney to do so by extending or accepting a "friend" request. *See id.* Individuals with very high security settings can even prevent the public from uncovering that they have a Facebook account through searches on the Internet or the Facebook website.

36. *See* *Baumann v. Joyner Silver & Electroplating*, 47 W.C.D. 611, 1992 MN Wrk. Comp. LEXIS 622, at *15 n.3 (Minn. Work. Comp. Ct. App. Sept. 1, 1992) (finding that, as a general rule, contact made to acquire information that an employee would normally provide to the public in the course of public activities is not proscribed conduct).

37. *See infra* Part III.

3. Formal Discovery

Social networking information that is not publicly available can be obtained through the formal discovery process. Federal Rule of Civil Procedure 34(a)(1)(A) allows a party to request “any designated documents or electronically stored information—including . . . data or data compilations—stored in any medium” in “the responding party’s possession, custody, or control.”³⁸ Accordingly, defense counsel may request any information posted and stored on social networking websites, including discussion and message postings, pictures, and videos relevant to the employee’s claim.

Employees in workers’ compensation cases should disclose such relevant information in response to narrowly tailored discovery requests.³⁹ If a plaintiff’s attorney objects to the production of this information, the defense attorney must demonstrate its relevance.⁴⁰ If a document request for social networking information is at least facially relevant and the plaintiff is able, but does not wish, to produce the relevant

38. FED. R. CIV. P. 34(a)(1), (a)(1)(A). Rule 34 was “intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.” FED. R. CIV. P. 34 advisory committee’s note. Rules 33 and 26(a)(1) also address formal discovery of electronically stored information. See Michael A. Oakes, Meghan A. Podolny & John W. Woods Jr., *Social Networking Sites and the E-Discovery Process*, DATA PROTECTION L. & POL’Y (Feb. 2010), http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C2856%5CE-Discovery_DPLP_Feb10.pdf (“Firstly, the amendments introduced the phrase ‘electronically stored information’ to Rules 26(a)(1), 33, and 34 to acknowledge that ESI is discoverable.”).

39. See Awsumb, *supra* note 4, at 24 (“Courts are willing to require users to produce social networking information in response to narrowly tailored discovery requests.”); see also *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-CV-01958-WYDMJW, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (“[T]he information sought within the four corners of the subpoenas issued to Facebook, MySpace, Inc., and Meetup.com is reasonably calculated to lead to the discovery of admissible evidence [and] is relevant to the issues in this case.”); *Mackelprang v. Fidelity Nat’l Title Agency of Nev., Inc.*, No. 2:06CV00788-JCM-GWF, 2007 WL 119149, at *8 (D. Nev. Jan. 9, 2007) (finding that the employer could discover MySpace messages relating to issues relevant to the case).

40. See Oakes, Podolny & Woods, *supra* note 38 (“Although ESI is potentially discoverable—in any form—in US litigation, if a party objects to the production of social networking data, the litigant seeking the information will still be required to demonstrate its relevance.”).

document, the plaintiff's attorney has the burden of establishing that the document is not relevant in order to avoid producing it.⁴¹

In *EEOC v. Simply Storage Management, LLC*, an employment law case, a magistrate judge ordered employees to produce social networking profile information from their Facebook and MySpace accounts in response to a discovery request.⁴² The EEOC filed a sexual harassment complaint on behalf of two employees against their supervisor.⁴³ It requested a discovery conference because counsel disagreed about the proper scope of discovery involving social networking documents, including items from Facebook and MySpace.⁴⁴ The

41. See *Scott v. Leavenworth Unified Sch. Dist. No. 453*, 190 F.R.D. 583, 585 (D. Kan. 1999) ("When the discovery sought appears relevant, the party resisting the discovery has the burden to establish the lack of relevance"); Blank, *supra* note 21, at 496 ("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.").

42. *EEOC v. Simply Storage Mgmt., LLC*, No. 1:09-cv-1223-WTL-DML (S.D. Ind. May 11, 2010) (order on discovery issues raised during April 21 conference), *available at* http://www.scribd.com/full/31921843?access_key=key-2i8jdf9a1tammq659sv [hereinafter Order on Discovery].

43. *Id.*

44. *Id.* at 2. The disputed documents requested through the formal discovery process included:

Request No. 1: All photographs or videos posted by Joanie Zupan or anyone on her behalf on Facebook or MySpace from April 23, 2007 to the present.

Request No. 2: Electronic copies of Joanie Zupan's complete profile on Facebook and MySpace (including all updates, changes or modifications to Zupan's profile) and all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, details, blurbs, comments, and applications (including, but not limited to, "How well do you know me" and the "Naughty Application") for the period from April 23, 2007 to the present. To the extent electronic copies are not available, please provide the documents in hard copy form.

Request No. 3: All photographs or videos posted by Tara Strahl or anyone on her behalf on Facebook or MySpace from October 11, 2007 to November 26, 2008.

Request No. 4: Electronic copies of Tara Strahl's complete profile on Facebook and MySpace (including all updates, changes, or modifications to Strahl's profile) and

EEOC objected to the demand for the production of all documents related to the plaintiffs' social networking accounts and to deposition testimony about the employees' social networking profiles on the grounds that the requests were overbroad, not relevant, unduly burdensome, harassing, and embarrassing toward the employees.⁴⁵ Magistrate Judge Debra Lynch found that the standard for discovery's scope is broad⁴⁶ and noted that, where relevance is in doubt, the court should be permissive.⁴⁷

However, she also emphasized that the scope of discovery is not limitless.⁴⁸ The EEOC argued that discovery of Facebook

all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, details, blurbs, comments, and applications (including, but not limited to, "How well do you know me" and the "Naughty Application") for the period from October 11, 2007 to November 26, 2008. To the extent electronic copies are not available, please provide these documents in hard copy form.

Id.

45. *Id.* at 3.

46. *Id.* at 4; *see also* FED. R. CIV. P. 26. Federal Rule of Civil Procedure 26(b) reads:

Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).

47. Order on Discovery, *supra* note 42, at 4; *see also* Truswal Sys. Corp. v. Hydro-Air Eng'g, Inc., 813 F.2d 1207, 1211-12 (Fed. Cir. 1987) (discussing the scope of Rule 26(b)(1)).

48. *See* Order on Discovery, *supra* note 42, at 4 (citing *Rozell v. Ross-Holst*, No. 05 Civ. 2936(JGK)(JCF), 2006 WL 163143, at *2 (S.D.N.Y. Jan. 20, 2006)). Federal Rule of Civil Procedure 26(b)(2)(C) provides that:

On motion or on its own, the court must limit the frequency

and MySpace profiles should be limited to information that directly relates to issues raised in the complaint.⁴⁹ Ultimately, Magistrate Judge Lynch found all social networking content revealing, relating, or simply referring to allegations raised in the complaint to be discoverable.⁵⁰ Judge Lynch also found that the fact that a user's profile is private and not available to the public does not shield information in that user's profile from discovery.⁵¹

Similarly, in *Bass v. Miss Porter's School*, a case involving harassment of a high school student at an elite boarding school, the plaintiff objected to a discovery request for information from his Facebook profile.⁵² Again, the court found a low threshold for the discovery of social networking information. The court held:

Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting. Therefore, relevance of the content of [p]laintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to [p]laintiff's own determination of what

or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

- (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
- (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
- (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

49. Order on Discovery, *supra* note 42, at 5.

50. *Id.* at 9-10. This content included third-party communications, videos, and photographs posted on Facebook and MySpace. *Id.*

51. *Id.* at 6.

52. No. 3:08CV1807(JBA), 2009 WL 3724968, at *1 (D. Conn. Oct. 27, 2009).

may be “reasonably calculated to lead to the discovery of admissible evidence.”⁵³

Thus, the court in *Bass* upheld the broad relevancy standard for discovery of social networking information, and the result should be no different in the workers’ compensation context. Defense counsel should be able to discover information that is relevant to allegations raised in the employee’s initial pleading,⁵⁴ including information relating to the employee’s alleged work injuries or employment abilities.

Moreover, a federal magistrate judge in New Jersey found writings shared on social networking sites to be discoverable.⁵⁵

53. *Id.* (citations omitted); *see also* Oakes, Podolny & Woods, *supra* note 38 (“The court disagreed, holding that ‘Facebook usage depicts a snapshot of the user’s relationships and state of mind at the time of the content’s posting’ and that the content’s relevance to both liability and damages would be ‘more in the eye of the beholder than subject to strict legal demarcations’ of what one party determines might be ‘reasonably calculated to lead to the discovery of admissible evidence.’”).

54. The plaintiff’s initial pleading in non-workers’ compensation state court matters is typically known as the “complaint,” pursuant to the state’s rules of civil procedure. Workers’ compensation courts and rules, however, refer to the employee’s first pleading by different terms, including “Claim Petition” and “Employee Claim.” *See, e.g.*, MINN. STAT. § 176.291 (2008); MINN. R. 1415.1000, subpt. 1 (2006); *How to File a Claim*, N.Y. ST. WORKERS’ COMPENSATION Bd., <http://www.wcb.state.ny.us/content/main/onthejob/howto.jsp> (last visited Aug. 20, 2010).

55. *Beye v. Horizon Blue Cross Blue Shield of N.J.*, No. 2:06-cv-5377-FSH-PS, slip op. at 5-6 (D.N.J. Dec. 14, 2007) (order denying motion for reconsideration), *available at* <http://www.onpointnews.com/docs/anorexia2b.pdf> [hereinafter Order Denying Motion for Reconsideration]. This order modified an October 31, 2007, order as follows:

(1) [N]o later than *January 15, 2008*, plaintiffs shall produce writings shared with others including entries on websites such as “Facebook” or “MySpace”; (2) plaintiffs shall preserve journals, diaries and writings not shared with others and if defendants’ experts believe they are needed to render an opinion then they can make an application seeking their production; and (3) writings shared with health care professionals shall be produced as part of the medical records.

Id. at 5-6.

In *Beye v. Horizon Blue Cross Blue Shield of New Jersey*,⁵⁶ an insurer sought production of all e-mails, journals, diaries, and communications involving minor children's eating disorders or manifestations and symptoms of the eating disorders.⁵⁷ Magistrate Judge Patty Shwartz ordered the minors to produce all entries on web pages, such as Facebook and MySpace, which the minors had shared with others.⁵⁸ Again, *Beye* indicates that there is precedent for workers' compensation courts to permit discovery of all entries on social networking sites that relate to an employee's physical abilities.

4. Defenses to Formal Discovery

Even if a party establishes that discovery of an employee's social networking profile information is relevant, a court may exclude it from discovery "if it is privileged," if its production would impose an undue burden on the employee, or if the employee "has superseding privacy interests in the account."⁵⁹ Federal Rule of Civil Procedure 26(b)(5) states that discoverable information may be withheld if it is privileged.⁶⁰ Privileged information may include information subject to the attorney-client privilege, commercial trade secrets, private settlement agreements, and employment confidentiality agreements.⁶¹ Federal Rule of Civil Procedure 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.'"⁶²

56. CIV. 06-5337, 2008 WL 3064757 (D.N.J. July 29, 2008).

57. Order Denying Motion for Reconsideration, *supra* note 55, at 5-6.

58. *Id.*

59. Blank, *supra* note 21, at 506; *see also infra* Part II.B.2 (discussing employee's defense of privacy).

60. FED. R. CIV. P. 26(b)(5).

61. *See* Blank, *supra* note 21, at 506. Such forms of privileged information are generally not applicable to workers' compensation litigation, where information is obtained from either the employee or social networking provider directly, and the employer previously signed an insurance policy agreeing to provide information to the insurer to assist in the defense of any workers' compensation claim.

62. FED. R. CIV. P. 26(b)(2)(B). In practice, courts use a balancing test to weigh the benefit and relevance of the information versus the burden and cost of producing it. *See* Blank, *supra* note 21, at 506.

5. Suggestions for Workers' Compensation Attorneys Relating to Formal Discovery

In order to generate disclosure of social networking information from the employee through the formal discovery process, workers' compensation defense attorneys should ask in their interrogatories (or other form of discovery demand pursuant to their state's rules governing discovery) for the names of any social networking sites used by the employee and request copies of all relevant photographs, videos, postings, communications, and discussions from social networking sites relating to the employee's physical or employment abilities.⁶³ Defense attorneys should include similar questions during the employee's deposition.⁶⁴ In order to comply with the rules governing discovery, plaintiffs' attorneys should encourage employees to disclose relevant social networking photographs, videos, postings, and other communications in response to a valid discovery request from defense counsel.

B. *Discovery from Site Operators*

In addition to obtaining social networking profile information from the employee directly through the formal discovery process, attorneys can recover the employee's profile information from the social networking site operator under some circumstances.⁶⁵ In situations where an employee refuses to disclose social networking profile information, or where the defense attorney believes or knows the employee has deleted all or part of his or her account, or has failed to disclose all information, defense counsel should consider using a narrowly tailored subpoena to the social networking site operator, as the

63. See Awsumb, *supra* note 4, at 24 ("Include interrogatories seeking the identification of social networking sites used by a person and all user profiles and accounts. Include document requests seeking production of relevant information maintained or shared by a person on social networking sites, including video and photos.").

64. See *id.* ("Inquire regarding social networking usage during deposition questioning.").

65. See FED. R. CIV. P. 37(a). Rule 37(a) permits a party to make a motion for an order to compel discovery from either a party or nonparty.

records custodian, to provide copies of relevant photographs, videos, and postings.⁶⁶ Defense attorneys may also request that information on a social networking site be preserved by sending a preservation order to the site operator.⁶⁷

In circumstances where an employee deactivated or deleted her Facebook or other social networking account, the site operator may continue to have a record of the user's account information.⁶⁸ If that information exists, social

66. See Blank, *supra* note 21, at 504 (“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.”). The subpoena should be very specific, including the user's full name, birthday, e-mail addresses, and time period of the requested activity.

67. See Lori Paul, *Paralegal Practice Tip: How to Subpoena MySpace and Facebook Information*, PARALEGAL BLAW BLAW BLAW (Oct. 10, 2009), <http://lorijpaul.com/?tag=litigation>. Although sending a preservation order allows the site operator to identify a user's account in order to preserve information, a site operator cannot provide this information to a defense attorney without a valid subpoena or permission of the user. See *id.* The preservation order, however, can ensure a site operator retains access to an employee's social networking profile information even after the employee deletes or loses access to his or her account. See *id.*

68. See, e.g., *Privacy Policy: Deactivating or Deleting Your Account*, FACEBOOK, <http://www.facebook.com/policy.php> (last visited Aug. 21, 2010) (“If you want to stop using your account you may deactivate it or delete it. When you deactivate an account, no user will be able to see it, but it will not be deleted. We save your profile information (connections, photos, etc.) in case you later decide to reactivate your account. Many users deactivate their accounts for temporary reasons and in doing so are asking us to maintain their information until they return to Facebook. You will still have the ability to reactivate your account and restore your profile in its entirety.”). Facebook also provides an option for users to delete an account permanently. Even after a user requests to delete his or her account, Facebook retains the account information for an undisclosed period of time, and may save information indefinitely. See *Privacy: Deactivating, Deleting, and Memorializing Accounts*, FACEBOOK, <http://www.facebook.com/help/?page=842> (last visited Aug. 21, 2010) (“Our system delays the deletion process in case you change your mind and no longer want to permanently delete your account.”); see also Maria Aspan, *After Stumbling, Facebook Finds a Working Eraser*, N.Y. TIMES, Feb. 18, 2008, at C5, available at http://www.nytimes.com/2008/02/18/business/18facebook.html?_r=1 (stating that deleting a Facebook account can be a very difficult and drawn-out process, and “[a]fter deletion, there may still be a record in Facebook's archives”); *Don't Forget Social Media in E-Discovery*, WISC. L.J. (Mar. 31, 2010), <http://www.wislawjournal.com/blog/2010/04/05/Don8217t-forget-social-media-in-ediscovery/> (discussing destruction of electronic evidence and stating that “Facebook and Twitter retain user pages”); *Facebook's Privacy*

networking websites' privacy policies, including those of Facebook and MySpace, specifically allow the social networking provider to disclose user information in response to subpoenas, court orders or a consent executed by the employee.⁶⁹

Courts have upheld subpoenas to social networking site operators "when the discovery sought is relevant to the lawsuit."⁷⁰ Obtaining social networking information from the site operator, however, would likely be a very lengthy and costly process, contrary to workers' compensation's underlying goal of efficiency.⁷¹ Therefore, obtaining such information from the site operator would rarely be worth the cost and time to defense counsel. This option, however, serves as a check on the employee's ability to destroy or hide social networking information in a workers' compensation case and provides for more honest disclosure by employees.

Two potential defenses that employees⁷² and social

Policy: Limitations on Removal, FACEBOOK, <http://www.facebook.com/policy.php> (last visited Aug. 21, 2010) ("Additionally, we may retain certain information to prevent identity theft and other misconduct even if deletion has been requested.")

69. Awsumb, *supra* note 4, at 24 ("The privacy policies of many service providers, including Facebook and MySpace, permit the disclosure of user information in response to subpoenas or court orders."); *see also* Romano v. Steelcase Inc., No. 2006-2233 (N.Y. Sup. Ct. July 7, 2009) (order) (directing the plaintiff to execute a consent to give the defendant access to the plaintiff's deleted MySpace and Facebook pages and accounts).

70. *See* Blank, *supra* note 21, at 504-05. In *Ledbetter v. Wal-Mart Stores, Inc.*, an employment law case, the magistrate judge upheld a subpoena to Facebook and MySpace requiring them to produce user information because the information sought was "reasonably calculated to lead to discovery of admissible evidence." No. 06-cv-01958-WYD-MJW, 2009 WL1067018, at *2 (D. Colo. Apr. 21, 2009).

71. *See supra* note 6 and accompanying text.

72. While generally a party in litigation does not have standing to object to a subpoena served on a non-party to the action, it appears that an employee has standing to object to a subpoena duces tecum that defense counsel serves on a third-party site operator to the extent that defense counsel seeks personal information or communications of the employee protected by the Stored Communications Act. *See, e.g.,* J.T. Shannon Lumber Co. v. Gilco Lumber Co., No. 2:07CV119, 2008 WL 3833216, at *1 (N.D. Aug. 14, 2008) (holding that employee has standing to seek to quash subpoena served on Internet service provider for production of employee's personal information protected by the Stored Communications Act), *quoted in* Crispin v. Christian Audigier, Inc., No. CV-09-09509 MMM (JEMx), 2010 WL 2293238, at *5 (C.D. Cal. May 26, 2010).

networking site operators alike have to the production of employee information and communications by site operators are that (i) the employee information and communications are protected by the Stored Communications Act; and (ii) an employee has a privacy interest in her social networking information and communications that precludes disclosure by the site operator.⁷³ We analyze each of these defenses in turn.

1. Stored Communications Act

Congress enacted the Stored Communications Act (SCA)⁷⁴ in 1986, as part of the Electronic Communications Privacy Act,⁷⁵ to address voluntary and compelled disclosure of “stored wire and electronic communications and transactional records” by Internet service providers. Congress defined first what was not allowed, with exceptions for what was, rather than defining what was permissible, with exceptions for what was not.⁷⁶ Congress also repeatedly distinguished between an “electronic communication service” (ECS) provider and a “remote computing service” (RCS) provider, delineating disclosure prohibitions for each type of service.⁷⁷ This distinction has given courts headaches as they attempt to decide which category describes various electronic communications, with

73. The employee could raise this second defense in response to a discovery request she receives from defense counsel to produce information and communications stored on a social networking site. *See supra* Part II.A.3. But because, at least in the published case law, an employee has used that defense only when discovery has been sought from the site operator, we analyze it here.

74. 18 U.S.C. §§ 2701-2712 (2006).

75. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

76. For example, subsection (a) of section 2702 states first, “Prohibitions. Except as provided in subsection (b) or (c)—a person or entity providing an electronic communication service to the public shall not knowingly divulge . . .” 18 U.S.C. § 2702(a)(1). Subsection (b) is titled “Exceptions for disclosure of communications.” *Id.* § 2702(b).

77. “[The term] ‘electronic communication service’ means any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). “[T]he term ‘remote computing service’ means the provision to the public of computer storage or processing services by means of an electronic communications system.” 18 U.S.C. § 2711(2).

varying results.⁷⁸ Social networking sites provide a unique challenge, because they are neither purely e-mail-centered (like Hotmail), nor purely community-based (like electronic bulletin boards).⁷⁹

It appears that courts have reached a consensus that social networking sites, despite their variation in function, are ECS providers to the extent they provide private messaging and the messages have not been opened. Outlining the precedent it followed, one court remarked that, since an ECS provider is “any service which provides to users thereof the ability to send or receive wire or electronic communications,” and “all three [social networking] sites [(Facebook, MySpace, and Media Temple)] provide private messaging or email services, the court is compelled to . . . [hold] that such services constitute ECS.”⁸⁰ Once the private e-mails have been opened by the recipient, the social networking site operator is functioning as a “remote computer service” provider, storing the messages for the recipient.⁸¹ Whether the social networking sites are operating as an ECS or RCS provider as to any particular message at any particular time, they cannot disclose an employee’s communications without permission of the employee.⁸²

The one court that has decided the precise issue of whether personal information and communications on social networking sites are protected by the SCA said that social networking sites

78. See *Crispin v. Christian Audigier, Inc.*, No. CV-09-09509 MMM (JEMx), 2010 WL 2293238, at *13-15 (C.D. Cal. May 26, 2010) (discussing cases with divergent holdings).

79. See *id.* at *9; see also *id.* at *14 (“[T]he difficulty in interpreting the statute is ‘compounded by the fact that the [SCA] was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [Facebook and MySpace]. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.’” (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002))); *Blank*, *supra* note 21, at 488 (“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.”).

80. *Crispin*, 2010 WL 2293238, at *9 (quoting 18 U.S.C. § 2510(15)) (internal quotation marks omitted).

81. *Id.* at *13.

82. See 18 U.S.C. § 2702(a).

are alternatively either an ECS or RCS with regard to posts on message or bulletin boards or a user's Facebook "wall,"⁸³ and regardless of a site's classification, it cannot disclose such posts without permission of the employee.⁸⁴ However, if there are no privacy settings protecting the employee's social networking profile, such that her message board or "wall" is available to the public,⁸⁵ the SCA would not apply.⁸⁶

Social networking site operators can disclose employee information or communications to defense counsel with permission of the employee.⁸⁷ The SCA allows site operators to "divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))" with the customer's consent.⁸⁸ So, for example, if an employee has deleted her account but authorizes a social

83. *See Crispin*, 2010 WL 2293238, at *14-16.

84. *Id.*

85. *Cf. Indep. Newspapers, Inc. v. Brodie*, 966 A.2d 432, 438 n.3 (Md. 2009) ("Social networking sites and blogs are sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others. Web sites, such as Facebook and MySpace, allow the user to tightly control the dissemination of that information. The user can choose what information to provide or can choose not to provide information. The act of posting information on a social networking site, without the poster limiting access to that information, makes whatever is posted available to the world at large.").

86. *See* 18 U.S.C. § 2511(2)(g)(i) ("It shall not be unlawful under this chapter or chapter 121 of this title for any person—(i) to intercept or access an electronic communication made through an electronic communication system that is so configured so that such communication is readily accessible to the general public.").

87. *See, e.g., Barnes v. Cus Nashville, LLC*, No. 3:09-0764, 2010 WL 2196591, at *1 (M.D. Tenn. May 27, 2010) ("Facebook does point out that it is willing to provide information from its files with the consent of [the user]. . . . [T]here was some indication that [said user] would be willing to sign a consent for this material to be furnished to the Magistrate Judge for review. If that in fact could be accomplished, then future problems concerning potential access to this material could be avoided."); *Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc.*, No. 2:06CV00788-JCM-GWF, 2007 WL 119149, at *2 (D. Nev. Jan. 9, 2007) ("In response to the subpoena, MySpace.com produced certain 'public' information regarding the two accounts, but refused to produce private email messages on either account in the absence of a search warrant or a letter of consent to production by the owner of the account.").

88. 18 U.S.C. § 2702(c).

networking site operator to release her information and communications to defense counsel, the site operator can do so. Additionally, it might even be possible in the case of an employee's prosecution of a workers' compensation claim for the judge to compel the employee to sign a consent form for the release of her account information and communications from a site operator, if relevant to the employee's claim.⁸⁹ It is more likely that a judge would not do so, however, and weigh the employee's failure to consent to the release of the information in his or her evaluation of the employee's claim.

2. Privacy

While an employee could argue that she has a privacy interest in her social networking profile information precluding disclosure, that argument is likely to fail in workers' compensation courts.⁹⁰ It is undisputed in the case law that an individual has no reasonable expectation of privacy when she has an account with a social networking site or Internet service provider: "[A] person has no expectation of privacy in Internet subscriber information. . . . [This is consistent with] settled federal law that a person has no reasonable expectation of

89. *See, e.g.,* Grady v. Superior Court, 139 Cal. App. 4th 1423, 1446 (Ct. App. 2006) ("Where a party to the communication is also a party to the litigation, it would seem within the power of a court to consent to disclosure on pain of discovery sanctions."); *see also* Bruce Nye, *More About Facebook: How to Get Facebook Records in the Litigation Arena*, CAL BIZ LIT (Aug. 24, 2009, 6:00 AM), http://www.calbizlit.com/cal_biz_lit/2009/08/more-about-facebook-how-to-get-facebook-records-in-the-litigation-arena.html.

90. *See* Blank, *supra* note 21, at 510 ("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. 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. 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." (citing *United States v. Gines-Perez*, 214 F. Supp. 2d 205, 225 (D.P.R. 2002))). Any right to privacy the employee has is not absolute. In the workers' compensation context, it is likely that an overriding objective is "facilitating the ascertainment of truth in connection with legal proceedings." *See* Kahn v. Superior Court, 188 Cal. App. 3d 752, 765 (Ct. App. 1987).

privacy in information exposed to third parties, like a telephone company or bank.”⁹¹ An employee likewise does not have a privacy interest in what she posts to her profile on a social networking site.⁹² Even if the employee protects her information on a social networking site with privacy settings, she still does not have a privacy interest in what is posted or communicated to or through her account.⁹³

III. Professional Responsibility Issues in Discovery of Employee Information from Social Networking Sites

This Part explores issues of professional responsibility that arise for a plaintiff’s attorney and defense counsel in connection with an employee maintaining and producing, and defense counsel discovering, information about an employee

91. *Courtright v. Madigan*, No. 09-CV-208-JPG, 2009 WL 3713654, at *2 (S.D. Ill. Nov. 4, 2009) (“The logic of these cases extends to subscriber information revealed by Plaintiff to MySpace.com. In sum, because Plaintiff had no reasonable expectation that the fact or existence of his MySpace.com account would remain private, neither the request by the Attorney General’s Office for that information nor the disclosure of that information by MySpace.com violated Plaintiff’s Fourth Amendment rights.”); *see also Doe v. Shurtleff*, No. 1:08-CV-64-TC, 2009 WL 2601458, at *5 (D. Utah Aug. 20, 2009) (“In *Perrine*, for example, when law enforcement obtained records from Yahoo! linking a screen name to an IP address registered to the defendant, the Tenth Circuit held that the Fourth Amendment was not implicated because the defendant had no expectation of privacy in information he had voluntarily transmitted to a third-party Internet provider.” (citing *United States v. Perrine*, 518 F.3d 1196, 1199, 1204 (10th Cir. 2008))).

92. *See Moreno v. Hanford Sentinel, Inc.*, 91 Cal. Rptr. 3d 858, 863-64 (Ct. App. 2009) (holding that an ode posted on MySpace.com was considered sufficiently public that the poster waived any privacy interest in the online rant).

93. *See Blank*, *supra* note 21, at 511 (“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. The possibility of inadvertently publicizing ‘private’ user content on social networking Web sites makes an objective expectation of privacy unreasonable.” (footnote omitted)); *see also Nye*, *supra* note 89 (“So, bottom line: social networking posts may not be private at all; if they are, the privacy right is not absolute, and the defense can overcome the privacy protection by demonstrating their relevance. . . . [O]nce that is done, the court has the authority to require the plaintiff to sign an authorization or release, and at that point, Facebook, MySpace or whomever will have to respond to a subpoena.”).

stored on a social networking site.

A. *Professional Responsibilities of the Plaintiff's Attorney*

Plaintiffs' attorneys should advise their clients of the risks of posting information and photographs, and communicating through, social networking sites.⁹⁴ Employees should not post any information or photographs that they do not want the employer or insurance company's lawyer to know or see—such as descriptions or pictures of the employee engaging in physical activities⁹⁵—and not provide anyone who they do not know access to their profiles.⁹⁶ Additionally, counsel should advise their clients not to post days and times of activities, as that could give investigators additional opportunities to conduct surveillance.⁹⁷ Of course, to the extent the workers' compensation claim is fraudulent and the lawyer knows so, the lawyer cannot represent the client in the prosecution of her claim.⁹⁸ But the mere fact that an employee's information or

94. See, e.g., *Floridians with Workers' Compensation and Personal Injury Cases Should Be Cautious When Posting on Social Networking Sites Like Facebook*, JOHNSON & GILBERT, P.A., <http://www.mylegalneeds.com/library/facebook-posts-could-damage-your-florida-workers-comp-or-pi-case.cfm> (last visited June 7, 2010) ("However, there are some precautions you can take to protect yourself, short of boycotting the Internet all together. First, be vigilant in reviewing the photos and posts on your social networking site. Remove anything that you would not want an insurance company lawyer to see that could help defend against your case. Next, [c]heck your privacy settings which enable you to block certain people from seeing you on a particular site (Facebook allows this). It is also helpful to search your name in the search field and see what comes up to make sure it is acceptable (it is advisable to do this on Google and YouTube as well). Finally never accept friend requests or respond to emails from people you do not know.").

95. See *supra* notes 29-31 and accompanying text.

96. See, e.g., Awsumb, *supra* note 4, at 25.

97. See Cenicerros, *supra* note 31 ("It's common for claimants to load their social networking sites with dates, easing the way for investigators and their cameras to find them.").

98. See MODEL RULES OF PROF'L CONDUCT R. 1.2(d) (2010) ("A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law."); MODEL RULES OF PROF'L CONDUCT R. 4.1(b) (2010) ("In the course of representing a client a lawyer shall not

photographs on a social networking site contradict the plaintiff's claim does not mean an employee's claim is fraudulent, because often interpretation of what a person posts on a social networking site depends on its context.⁹⁹ A plaintiff's attorney also needs to keep in mind that a lawyer "generally has no affirmative duty to inform an opposing counsel of relevant facts."¹⁰⁰ However, the employee's lawyer might have an obligation to provide relevant information or photographs to a defense attorney in response to an interrogatory, document request, or other form of discovery demand, if the plaintiff can still access what the defense attorney seeks.¹⁰¹

However, plaintiff's counsel cannot advise her client to delete information or photographs stored on a social networking site to the extent that what is stored on the site is potentially relevant to the employee's claim. According to Model Rule 3.4(a), "A lawyer shall not [counsel or assist another person to] unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document

knowingly: . . . (b) fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6."). As one plaintiff's attorney commented in response to learning of a non-client plaintiff whose personal injury case was destroyed by information defense counsel learned of on Facebook, "The plaintiff was dishonest, and as a personal injury attorney I don't want anything to do with representing dishonest people. In fact, I tell my clients, I can always deal with the truth but a single lie can kill an otherwise good case." *When Facebook Isn't a 'Friend' to Your Personal Injury Case*, N.Y. INJ. L. BLOG (July 1, 2009, 12:34 PM), <http://www.zifflaw.com/NYInjuryLawBlog/personal-injury-victims-cautious-facebook-privacy>; see also Roberto Ceniceros, *Facebook Job Boast Leads to Workers Comp Fraud Charges*, BUS. INS. (Sept. 14, 2010, 12:29 PM), <http://www.businessinsurance.com/article/20100914/NEWS/100919959>.

99. See Jodi Ginsberg, *How Facebook Can Undermine Your Workers' Compensation Case*, GA. WORKERS COMPENSATION BLOG (July 11, 2009), <http://www.georgiaworkerscompblog.com/2009/07/11/how-facebook-can-undermine-your-workers-compensation-case/> ("Photos and updates can easily be taken out of context. Even your frequency of posting can be used as evidence that you have the capacity to perform clerical type of work. Posts on Facebook and other social media sites can be used against you to put you on the defensive and as leverage to reduce the value of your case.").

100. MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. 1 (2010).

101. See *supra* notes 39-41 and accompanying text.

or other material having potential evidentiary value.”¹⁰² The *Restatement (Third) of the Law Governing Lawyers* counsels similarly: “A lawyer may not destroy or obstruct another party’s access to documentary or other evidence when doing so would violate a court order or other legal requirements, or counsel or assist a client to do so.”¹⁰³ Consequently, the employee’s attorney should advise his or her client to proceed with caution in posting information to a social networking site, but should not advise the client to destroy information that already exists when the attorney assumes representation of the employee.

B. *Professional Responsibilities of Defense Counsel*

There could be a lot of information relevant to an employee’s workers’ compensation case publicly available on Facebook or another social networking site,¹⁰⁴ and defense counsel could find it because many potential plaintiffs in workers’ compensation cases do not protect their profiles with increased privacy settings.¹⁰⁵ There is nothing unethical about a defense attorney or an agent of the attorney accessing an employee’s information and photographs stored on a social networking site that are not protected with privacy settings that block public access.¹⁰⁶ The employee would have no

102. MODEL RULES OF PROF’L CONDUCT R. 3.4(a) (2010); *id.* cmt. 2 (“Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed.”).

103. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 118(2) (2000).

104. *See supra* notes 29-31 and accompanying text.

105. *See* John Browning, *What Lawyers Need to Know About Social Networking Sites*, DALL. B. ASS’N NEWS (Feb. 1, 2009), <http://www.dallasbar.org/about/news-archives.asp?ID=240> (“While both MySpace and Facebook feature various privacy settings and controls, enabling users to restrict certain information from public view, studies have shown that a surprisingly high percentage of users are unfamiliar with the protection afforded by these settings.”).

106. *See* *Moreno v. Hanford Sentinel, Inc.*, 91 Cal. Rptr. 3d 858, 862 (Ct. App. 2009) (“Here, Cynthia publicized her opinions about Coalinga by posting the Ode on MySpace.com, a hugely popular Internet site. Cynthia’s

privacy interest in the information and photographs she has posted.¹⁰⁷ Scouring the Internet for publicly available information on a social networking site is no different than the video surveillance in a public place that defense counsel may authorize in a workers' compensation case,¹⁰⁸ and has actually replaced video surveillance as a popular form of investigation.¹⁰⁹ It should be routine for defense counsel (or, at

affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.”); N.Y. St. Bar Ass’n Comm. on Prof’l Ethics, Op. 843, at 3 (2010) (“A lawyer who represents a client in a pending litigation, and who has access to the Facebook or MySpace network used by another party in litigation, may access and review the public social network pages of that party to search for potential impeachment material.”).

107. See *Moreno*, 91 Cal. Rptr. 3d at 862.

108. See Mara E. Zazzali-Hogan & Jennifer Marino Thibodaux, *Friend or Foe: Ethical Issues for Lawyers to Consider When ‘Friending’ Adverse Witnesses Online*, 197 N.J. L.J. 726 (2009), available at <http://www.gibbonslaw.com/files/1251901206.pdf> (“A good rule of thumb for attorneys before poking around cyberspace is to consider whether an analogous noncyberspace situation would raise concerns. For example, viewing the public portion of a person’s MySpace page or his post on a public message board is analogous to conducting surveillance on a subject. In both instances, there is no communication made with the person, nor is any misrepresentation made about the investigating individual’s identity. The conduct would not invade a zone of privacy in either circumstance. Similarly, videotaping someone walking down the street, such as a plaintiff in a personal injury case, is akin to printing out information a person publicly posts online for all to see. The videotape or printout is a record of what that person has held out to the public.”). Also, the Professional Guidance Committee of the Philadelphia Bar Association said that there is nothing unethical about a lawyer, or an agent of a lawyer, forthrightly asking a witness (who is not represented by an attorney) for access to her social networking profile. Phila. Bar Ass’n Prof’l Guidance Comm., Op. 2009-02, at 1 (2009), available at

http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf (“The inquirer could test that by simply asking the witness forthrightly for access. That would not be deceptive and would of course be permissible.”). However, the lawyer could not ask an employee, represented by an attorney, for such access without going through the employee’s attorney. See MODEL RULES OF PROF’L CONDUCT R. 4.2 (2010) (“In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.”).

109. See Ceniceros, *supra* note 31 (“It’s the new video camera,” Pierre Khoury, a special investigator for Harleysville Group Inc., a Harleysville,

minimum, the insurance company) to search the Internet, at least in a popular search engine such as Yahoo! or Google, for information that is publicly available about an employee.¹¹⁰

But what about information or photographs on a social networking site regarding an employee that are not publicly available because the employee has them protected with security settings?¹¹¹ Can an attorney direct a third-party agent to “friend” the employee in hopes of gathering relevant evidence about the plaintiff?¹¹² A Philadelphia Bar Association opinion addressed a similar question.¹¹³ The inquirer-attorney asked about the propriety of an agent “friending” an unrepresented non-party witness on Facebook and MySpace, whose testimony was adverse to the inquirer’s client.¹¹⁴ The inquirer stated that the agent would state only truthful information—e.g., she would use her real name—but would not state her affiliation with the attorney.¹¹⁵ The inquirer wanted the agent to provide him with access to the witness’s profiles on MySpace and Facebook because “the inquirer believe[d] that

Pennsylvania-based insurer, says of the social networking sites. ‘Now we have a new kind of video camera, but we are not actually the ones filming. They are filming it for us.’”)

110. *Cf.* MODEL RULES OF PROF’L CONDUCT R. 1.1 (2010) (“A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.”).

111. *See* Denise Howell & Ernie Svenson, *Ins and Outs of Social Networking for Lawyers: How Tough Is It to Cast Your Profile Into Infinity?*, L. PRAC. MAG., Jan. 2008, at 47, available at <http://www.abanet.org/lpm/magazine/articles/v34/is1/pg47.shtml> (“One important difference is the functionality of the sites’ privacy controls. For those who take the time to examine and tweak their privacy settings, Facebook makes it possible to funnel certain information only to certain parties.”).

112. “Dissembling” or “pretexting,” whatever the medium, is the practice of a lawyer or a lawyer’s subordinate either pretending to be someone he or she is not, lying, or being deceitful about his or her intentions, all for the purpose of obtaining information from an adverse party or witness. *See* Eric Cooperstein, *Facebook Ethics: It’s Not About Facebook*, LAWYERIST.COM (June 23, 2009), <http://lawyerist.com/facebook-ethics-it%E2%80%99s-not-about-facebook/>.

113. *Op.* 2009-02. In general, there is a lack of authority on these questions. *See, e.g.,* Zazzali-Hogan & Thibodaux, *supra* note 108, at 726 (noting that there is no New Jersey authority on point).

114. *Op.* 2009-02, at 1.

115. *Id.*

the pages maintained by the witness [contained] information relevant to the matter in which the witness was deposed, and could be used to impeach the witness's testimony should she testify at trial."¹¹⁶

First, the opinion states that, under Pennsylvania Rule of Professional Conduct 5.3,¹¹⁷ which is identical to Model Rule 5.3,¹¹⁸ an attorney is responsible for the conduct of a non-lawyer who "friends" the employee on the attorney's behalf. According to the opinion:

But the inquirer plainly is procuring the conduct, and, if it were undertaken, would be ratifying it with full knowledge of its propriety or lack thereof, as evidenced by the fact that he wisely is seeking guidance from this Committee. Therefore, he is responsible for the conduct under the Rules even if he is not himself engaging in the actual conduct that may violate a rule.¹¹⁹

116. *Id.*

117. PA. RULES OF PROF'L CONDUCT R. 5.3 (2010). Rule 5.3 of the Pennsylvania Rules of Professional Conduct provides, in part:

With respect to a nonlawyer employed or retained by or associated with a lawyer:

. . . .

(c) a lawyer shall be responsible for conduct of [a nonlawyer over whom the lawyer has "direct supervisory authority"] that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if: the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved;

118. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3 (2010).

119. Op. 2009-02, at 2. Another employee of the employer, such as the employee's supervisor, could already be "friends" with the plaintiff-employee, in which case the other employee could voluntarily, or be compelled to, share information with defense counsel that the plaintiff has posted on a social networking site. If the other employee is unrepresented, defense counsel cannot misrepresent that she is uninterested. *See* MODEL RULES OF PROF'L CONDUCT R. 4.3 (2010) ("In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the

The bar association does not distinguish between the activities of an investigator or paralegal and the activities of a junior lawyer who the lawyer handling the case is supervising.¹²⁰

The lawyer is not responsible under Model Rule 5.3 for the actions of an investigator hired by the client who “friended” an employee as long as the investigator was not “employed, retained, or associated with the attorney.”¹²¹ Additionally, the communication between the investigator and the employee would be communication between parties, not between an attorney and an opposing party, and it would therefore not be prohibited by Model Rule 4.2.¹²² Consequently, defense counsel in a workers’ compensation case is not acting unethically if an investigator hired by the insurance company “friends” the employee on a social networking site, as long as the lawyer does not encourage the investigator to do so and the investigator is not associated with her, and defense counsel could potentially use the information or photographs that the investigator uncovers in defending the employee’s claim.¹²³ It is not relevant to the lawyer’s culpability whether the investigator used her real identity or not: what is critical is the lack of any relationship between the lawyer and the investigator.

Second, the Philadelphia Bar Association opinion states that the attorney’s proposed conduct violates Pennsylvania

lawyer shall make reasonable efforts to correct the misunderstanding.”).

120. See Op. 2009-02; see also MODEL RULES OF PROF’L CONDUCT R. 5.1(b) (2010) (“A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.”).

121. State Bar of Mich. Standing Comm. on Prof’l & Judicial Ethics, Ethics Op. RI-153 (1993) (citing MODEL RULES OF PROF’L CONDUCT R. 5.3), available at 1993 WL 274201. In the scenarios described in the Michigan ethics opinion, insurance investigators used pretexts to film workers’ compensation claimants acting inconsistently with their claimed injuries. Because the insurance company, and not defense counsel, hired the investigators, they “[were] agents of the company, not agents of the lawyers,” and the investigators “[were] not encompassed by the professional rules applicable to lawyers.” *Id.* at 2.

122. See *id.* (citing MODEL RULES OF PROF’L CONDUCT R. 4.2).

123. See *infra* Part IV.

Rule of Professional Conduct 8.4(c),¹²⁴ the same as Model Rule 8.4(c).¹²⁵ According to the opinion, it is deceptive for a non-lawyer working on defense counsel's behalf to attempt to access an employee's profile on a social networking site while omitting a material fact—"that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness."¹²⁶ The fact that the witness might permit anyone to access her profile does not excuse deceit.¹²⁷ The Professional Guidance Committee distinguishes the inquiry before it from the ordinary surveillance context—in the latter the videographer films, photographs, or observes the employee as she presents herself to the public and does not have to ask permission to gain access to a private area.¹²⁸ The inquirer of the

124. Rule 8.4 of the Pennsylvania Rules of Professional Conduct provides, in part: "It is professional misconduct for a lawyer to: . . . (c) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation." PA. RULES OF PROF'L CONDUCT R. 8.4(c) (2010).

125. See MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2010).

126. Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02, at 3 (2009), available at

http://www.philadelphiabar.org/WebObjects/PBARReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf ("The omission would purposefully conceal that fact from the witness for the purpose of inducing the witness to allow access, when she may not do so if she knew the third person was associated with the inquirer and the true purpose of the access was to obtain information for the purpose of impeaching her testimony.").

127. *Id.* ("The possibility or even the certainty that the witness would permit access to her pages to a person not associated with the inquirer who provided no more identifying information than would be provided by the third person associated with the lawyer does not change the Committee's conclusion. Even if, by allowing virtually all would-be 'friends' onto her Facebook and MySpace pages, the witness is exposing herself to risks like that in this case, excusing the deceit on that basis would be improper. Deception is deception, regardless of the victim's wariness in her interactions on the internet and susceptibility to being deceived. The fact that access to the pages may readily be obtained by others who either are or are not deceiving the witness, and that the witness is perhaps insufficiently wary of deceit by unknown internet users, does not mean that deception at the direction of the inquirer is ethical.").

128. See *id.*; see also Zazzali-Hogan & Thibodaux, *supra* note 108, at 726 ("The waters are muddied, however, when an attorney's concealment of the facts becomes a variable in the equation. The hypothetical we present is problematic because the paralegal attempting to 'friend' the subject would not disclose his relationship with the attorney and his true intentions. The

Philadelphia Bar Association opinion proposed that his agent use a truthful identify;¹²⁹ one issue that arises is whether the lawyer's conduct runs more unquestionably afoul of Rule 8.4(c) if the lawyer instructs an agent to use a false identity in trying to "friend" an employee. While there is no authority on this latter point, it certainly appears that such conduct is "deceitful."

Last, the opinion states that a non-lawyer who friends an adverse witness at the direction of an attorney violates Pennsylvania Rules of Professional Conduct 4.1¹³⁰ and 8.4(a)¹³¹

paralegal's conduct is more invasive than simple surveillance but more importantly, it would occur under false pretenses. An analogy outside of the cyberspace context is if the paralegal knocked on the party's door; the party, without questioning the visitor's background or motives, allowed him to come inside; and, they engaged in a discussion that included information relevant to the lawsuit. While the party's voluntary act of allowing the paralegal to enter her home—like the party's voluntary acceptance of an online invitation to become 'friends'—may mitigate invasion of privacy concerns and call into question the party's discretion, the element of deception still exists. Until a New Jersey court or ethics committee makes a clear pronouncement, all attorneys should exercise caution before becoming 'friendly' with adverse witnesses or parties on social networking sites."); Clifford F. Shnier, *Friend or Foe?: Social Networking and E-Discovery*, INSIDE COUNS. (Feb. 16, 2010), <http://www.insidecounsel.com/Issues/2010/February-2010/Pages/Friend-or-Foe--Social-networking-and-EDiscovery.aspx?page=1> ("If a personal injury defense attorney hires an investigator to take videos of a plaintiff who claims he is incapacitated due to injury, and the investigator catches that plaintiff playing basketball, few courts would disallow that evidence and none would see any reason to discipline the defense attorney. However, if that same defense attorney asks his assistant to 'friend' the plaintiff on Facebook, so as to obtain information that the plaintiff doesn't make available on his page to nonfriends, that crosses the ethical line.").

129. Op. 2009-02, at 1.

130. PA. RULES OF PROF'L CONDUCT R. 4.1(a) (2010) ("In the course of representing a client, a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person"); *see also* MODEL RULES OF PROF'L CONDUCT R. 4.1(a) (2010); Browning, *supra* note 105 ("In instances where it is not readily available, beware the ethical pitfalls that lie in attempting to obtain access to such non-public material. Misrepresenting who you are in order to become a 'friend' and gain access could be considered a violation of Rule 4.01 of the Professional Rules of Conduct.").

131. PA. RULES OF PROF'L CONDUCT R. 8.4(a) (2010) ("It is professional misconduct for a lawyer to (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another"); *see* MODEL RULES OF PROF'L CONDUCT R. 8.4(a) (2010); *see also In re Luther*, 374 N.W.2d 720, 720 (1985) (reprimanding lawyer for violating DR-102(A)(4) and (6) in using false

as well.¹³² The opinion notes that states differ on whether lawyers and their agents can engage in deception in certain types of investigations.¹³³ Even in states such as Oregon, that

identity to gain information about debtors to initiate debt collection suits on behalf of his creditor-client).

132. Op. 2009-02, at 4.

133. See *id.* at 4-6. Compare IOWA RULES OF PROF'L CONDUCT R. 32:8.4 cmt. 6 (2010) ("It is not professional misconduct for a lawyer to advise clients or others about or to supervise or participate in lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights or in lawful intelligence-gathering activity, provided the lawyer's conduct is otherwise in compliance with these rules."); N.Y. City Lawyers' Ass'n Comm. on Prof'l Ethics, Formal Op. 737 (2007), available at http://www.nycla.org/siteFiles/Publications/Publications519_0.pdf (distinguishing "dissemblance" from "dishonesty, fraud, misrepresentation, and deceit" and allowing lawyers to use deceit in investigations of intellectual property and civil rights violations where no rights of third parties are involved, the risk of harm is imminent, no other means exists to obtain the necessary evidence, and the lawyer's and investigator's conduct do not otherwise violate the ethical rules, including the no-contact rule); OR. RULES OF PROF'L CONDUCT R. 8.4(b) (2010) ("Notwithstanding paragraphs (a)(1), (3) and (4) and Rule 3.3(a)(1), it shall not be professional misconduct for a lawyer to advise clients or others about or to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, provided the lawyer's conduct is otherwise in compliance with these Rules of Professional Conduct. 'Covert activity,' as used in this rule, means an effort to obtain information on unlawful activity through the use of misrepresentations or other subterfuge."); *Apple Corps Ltd. v. Int'l Collectors Soc'y*, 15 F. Supp. 2d 456, 475 (D.N.J. 1998) ("However, RPC 8.4(c) does not apply to misrepresentations solely as to identity or purpose and solely for evidence-gathering purposes. . . . The prevailing understanding in the legal profession is that a public or private lawyer's use of an undercover investigator to detect ongoing violations of the law is not ethically proscribed, especially when it would be difficult to discover the violations by other means."), with *In re Pautler*, 47 P.3d 1175, 1176 (Colo. 2002) ("In this proceeding, we reaffirm that members of our profession must adhere to the highest moral and ethical standards. Those standards apply regardless of motive. Purposeful deception by an attorney licensed in our state is intolerable, even when it is undertaken as a part of attempting to secure the surrender of a murder suspect."). Perhaps, in a jurisdiction such as Iowa or Oregon, it does not violate the Model Rules for a defense lawyer to supervise a third party who "friends" an employee to gain access to her social networking site if the lawyer believes that the employee is engaging in unlawful activity, such as prosecuting a fraudulent workers' compensation claim. For more on deception in undercover investigations under the professional responsibility rules, see generally Barry R. Temkin, *Deception in Undercover Investigations: Conduct-Based v. Status-Based Ethical Analysis*, 32 SEATTLE U. L. REV. 123 (2008); Douglas R. Richmond, *Deceptive Lawyering*, 74 U. CIN. L. REV. 577 (2005); and David B. Isbell & Lucantonio N. Salvi, *Ethical Responsibility of Lawyers for Deception by Undercover*

have an exception for a lawyer to use deceit in investigations, the lawyer probably cannot use deceit when there is no violation of law, as is often the case with no-fault workers' compensation claims.¹³⁴ In some states, a situation where this Philadelphia Bar Association opinion might be applicable in the workers' compensation context, in addition to the case of a fraudulent claim, is where a non-lawyer "friends" an employee who has a profile on a social networking site that advertises a business to the public.¹³⁵

Whatever the ethics rules in a particular state, workers' compensation judges would have some discretion in whether they find the efforts of defense counsel and their agents to gain access to an employee's restricted social networking profile

Investigators and Discrimination Testers: An Analysis of the Provisions Prohibiting Misrepresentation Under the Model Rules of Professional Conduct, 8 GEO. J. LEGAL ETHICS 791 (1995). For a criticism of the narrowness of the exception for deceit in lawyer-supervised investigations in New York, see Gerald B. Lefcourt, *Fighting Fire with Fire: Private Attorneys Using the Same Investigative Techniques as Government Attorneys: The Ethical and Legal Considerations for Attorneys Conducting Investigations*, 36 HOFSTRA L. REV. 397, 398-403 (2007). For a critique of lawyers hiring investigators to engage in deceit, see Michael Bonsignore, Note, *Rules Exist for a Reason: A Commentary on Lawyers Hiring Investigators to Partake in Deceptive Tactics*, 21 GEO. J. LEGAL ETHICS 655 (2008).

134. Or. State Bar Ass'n, Ethics Op. 2005-173 (2005), available at 2005 WL 5679600. In the case where the attorney suspects the plaintiff of breaching a duty, for example by filing a fraudulent claim, the lawyer can "advise" or "supervise" covert behavior but not directly participate in it. "[A]ny lawyer involvement in activity that includes the lawyer's direct misrepresentation or deception runs counter to the fundamental tenet of lawyer 'honesty and personal integrity.'" *Id.* (quoting *In re Gatti*, 8 P.3d 966, 977 (Or. 2000)).

135. *Cf.* *Baumann v. Joyner Silver & Electroplating*, 47 W.C.D. 611, 1992 MN Wrk. Comp. LEXIS 622, at *15 n.3 (Minn. Work. Comp. Ct. App. Sept. 1, 1992) ("Among other objections, the employee objected to the surveillance evidence based, apparently, on the claim the activities of investigators posing as potential customers for employee's self-employed business constituted improper direct communications between an attorney's agent and a represented opposing party. Although we do not here reach this contention, we note that the surveillance evidence to which employee objects is not in the record before us. Since, in our view, surveillance contact in which investigators seek to elicit only information which the employee would normally provide to the public in the course of his or her public activities is not proscribed conduct, we would in any event have needed to review the specifics of the contact during the investigation to determine the presence or absence of impropriety.").

deceitful.¹³⁶ Evidence can, however, be admissible in a workers' compensation case even if an attorney violates the rules of professional responsibility in obtaining it.¹³⁷ But in certain cases, a court might impose sanctions and not admit into evidence what a lawyer obtains in violation of the Model Rules.¹³⁸

136. *Cf., e.g.,* Rhoades v. Nabisco, Inc., 1985 WL 47399, at *3 (Minn. Work. Comp. Ct. App. May 14, 1985) (Gard, J., concurring) (“I would affirm the findings of the Compensation Judge because of the review standard presently applicable to the Workers’ Compensation Court of Appeals. I feel it necessary to comment, however, upon the method used to investigate the case and the contacts made with the employee after the attorney-client relationship had been established and published. The majority has concluded that the employers and insurers are entitled to reasonable investigative and surveillance procedures and, undoubtedly, there are no limitations on the investigative and surveillance procedures contained in the Workers’ Compensation Law. There is the allegation of the use of a hidden camera, a hidden microphone, a meeting established on pretense or pretext, and the allegation of fraud and deceit. This Court is certainly aware that the method of investigation and surveillance in workers’ compensation cases has occasionally involved such pretext and actual misrepresentation as to the real intention of the party conducting the surveillance or investigation. It would seem that, in the absence of legislation dealing with such conduct, that there be considerable discretion in the trial judge with regard to the introduction of evidence gathered by such means. I do not believe that the analogy of entrapment is in any way applicable, since the law with regard to entrapment in a criminal proceeding would not only not here be applicable, but the conduct here does not constitute entrapment in any event.”); Clemente-Volpe v. Workmen’s Compensation Appeal Bd., 624 A.2d 666, 672 (Pa. Commw. Ct. 1993) (refusing to disturb referee’s finding that surveillance film was credible even though employee was “tricked by the investigators into performing tasks that required lifting and bending”); Isadore v. Workers’ Compensation Appeal Bd., 465 A.2d 1096, 1099 (Pa. Commw. Ct. 1983) (finding motion pictures admissible even though investigator tricked employee into performing acts inconsistent with alleged medical condition).

137. *See* Keiser v. Dick Lind Heating Co., 1996 WL 705445, at *4 (Minn. Work. Comp. Ct. App. Nov. 22, 1996) (“This court may not construe or apply non-workers’ compensation statutes or rules to determine whether there has been a violation of those statutes or rules. Furthermore, nothing in the statute or rule cited by the employee [Minnesota Rule of Professional Conduct 4.2] requires that evidence obtained in contravention of either the statute or the rule be excluded from admission in a civil proceeding.” (footnote omitted)); State Bar of Mich. Standing Comm. on Prof’l & Judicial Ethics, Ethics Op. RI-153 (1993), *available at* 1993 WL 274201 (“The admissibility of the surveillance results is a question of law, not ethics, and therefore will not be further considered.”).

138. *See, e.g.,* Midwest Motor Sports v. Arctic Sales, Inc., 347 F.3d 693, 699-70 (8th Cir. 2003) (upholding evidentiary sanctions—the exclusion from evidence of conversations obtained in violation of the Model Rules—against

The witness whose social networking profiles the lawyer inquired about accessing in the Philadelphia Bar Association opinion was not represented by counsel; if an employee is represented by counsel, then there is risk of the lawyer, or a third party acting under the supervision of the lawyer, violating Model Rule 4.2 in “friending” the employee. Model Rule 4.2 states, “In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized do so by law or court order.”¹³⁹ Pursuant to Model Rule 5.3, the lawyer cannot direct a non-lawyer to contact, or “friend,” the employee on the lawyer’s behalf.¹⁴⁰ This is no different than the physical surveillance context where an attorney who represents the employer and the insurance carrier potentially violates Model Rule 4.2 if an investigator, who is the attorney’s agent, engages the employee in conversation during the course of the investigator’s surveillance.¹⁴¹

The same exceptions to the prohibitions in Rule 8.4 that apply in cases where deception is authorized in particular states would also likely apply here. But little in this area is certain, because as the technologies develop, so does the application of the ethics rules. What is certain, however, is that Rules 4.2 and 5.3, in addition to the Philadelphia Bar Association opinion, suggest, at minimum, that defense counsel

attorney who, in violation of Model Rules 4.2 and 8.4(c), supervised an investigation where investigators deceitfully posed as customers of the plaintiff and secretly tape recorded conversations).

139. MODEL RULES OF PROF'L CONDUCT R. 4.2 (2010).

140. *See supra* note 119 and accompanying text.

141. *See* State Bar of N.C., 2003 Formal Ethics Op. 4, *available at* <http://www.ncbar.com/ethics/ethics.asp?page=332&keywords=6>. Whether the information obtained through the prohibited contact is admissible is a separate question. *See id.* (“The Ethics Committee declines to opine on the admissibility of evidence. However, to discourage unauthorized communications by an agent of a lawyer and to protect the client-lawyer relationship, the lawyer may not proffer the evidence of the communication with the represented person, even if the lawyer made a reasonable effort to prevent the contact, unless the lawyer makes full disclosure of the source of the information to opposing counsel and to the court prior to the proffer of the evidence.”); *see also infra* Part IV.

should proceed with considerable caution before having an agent “friend” an employee.¹⁴²

IV. Using Evidence Obtained from Social Networking Sites in Litigation

Despite the prevalence of social networking, there are few published cases discussing the use of social networking evidence in litigation, and an absence of workers’ compensation cases on the use of social networking evidence. This Part applies workers’ compensation law, as well as pertinent state and federal court cases discussing the admissibility of social networking evidence and other forms of ESI, to offer guidance on when social networking evidence should be admissible and how judges should weigh it in workers’ compensation litigation.

A. *Admissibility of Evidence*

Workers’ compensation judges have broad discretion in light of liberal rules of evidence, including rules as to hearsay and authentication. Despite that discretion, compensation judges may not disregard all traditional principles of evidence applied by state and federal courts in deciding whether social networking evidence is admissible.

1. Maintaining Relevancy Despite Relaxed Admissibility Standards

In state court, when ESI is offered as evidence, judges consider these types of questions:

(1) is the **ESI relevant** as determined by [Federal] Rule [of Evidence] 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less

142. *But cf.* State Bar of Mich. Standing Comm. on Prof'l & Judicial Ethics, Ethics Op. RI-153 (1993), available at 1993 WL 274201 (advising that the lawyer does not violate Model Rule 4.2 when the client, and not the lawyer, hires and supervises the investigator).

probable than it otherwise would be); (2) if relevant under 401, is it **authentic** as required by *Rule 901(a)* (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it **hearsay** as defined by *Rule 801*, and if so, is it covered by an applicable exception (*Rules 803, 804 and 807*); (4) is the form of the ESI that is being offered as evidence an **original** or **duplicate** under the original writing rule, of [sic] if not, is there admissible secondary evidence to prove the content of the ESI (*Rules 1001–1008*); and (5) is the probative value of the ESI substantially outweighed by the danger of **unfair prejudice** or one of the other factors identified by *Rule 403*, such that it should be excluded despite its relevance.¹⁴³

As use of the Internet has become widespread, state courts are becoming more accustomed to answering these types of questions with regard to ESI, such as information from social networking sites, and more liberal in admitting ESI into evidence.¹⁴⁴

Workers' compensation judges generally have broad discretion¹⁴⁵ and are not bound by state or federal rules of

143. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 538 (D. Md. 2007); see also THOMAS BUCKLES, LAWS OF EVIDENCE 13 (2003). After enactment of the Federal Rules of Evidence in 1975, the Uniform Rules of Evidence, originally providing a framework for the Federal Rules, were amended to match the Federal Rules. *Id.* The majority of states currently have adopted the Uniform Rules of Evidence or use them as a model. *Id.*; see also *Uniform Rules of Evidence Locator*, CORNELL UNIV. L. SCH. LEGAL INFO. INST. (Mar. 5, 2003), <http://www.law.cornell.edu/uniform/evidence.html>.

144. See Robert C. Rodriguez, *Decisions Reflect Importance, Limitations of Evidence Obtained from Internet*, LITIG. NEWS (Feb. 3, 2010), http://www.abanet.org/litigation/litigationnews/top_stories/020310-evidence-admissibility-social-networking-saadi-dockery.html ("Courts are becoming more comfortable with Internet evidence and perhaps more liberal in allowing such information into evidence.").

145. See, e.g., MINN. STAT. § 176.411, subdiv. 1 (2008); *Bey v. Oxford Props., Inc.*, 481 N.W.2d 40, 42 (Minn. 1992) ("In view of the well recognized principles that . . . the compensation judge is not bound by rules of evidence or by technical or formal rules of pleading or procedure . . ."). However,

evidence, and therefore social networking evidence may be admitted even more liberally in workers' compensation courts than in state or federal court.¹⁴⁶ Relaxed rules of evidence provide for informal and faster resolution of claims, consistent with workers' compensation's underlying goal of efficiency.¹⁴⁷

For example, one major obstacle to the admissibility of social networking evidence in state or federal court is the hearsay rule.¹⁴⁸ Hearsay evidence that is inadmissible in state

workers' compensation courts generally cannot adopt rules of evidence that are more restrictive than the state court rules of evidence. *See, e.g.*, *Fite v. Ammco Tools, Inc.*, 258 N.W.2d 922, 926 (Neb. 1977) (“[T]he compensation court is empowered to admit evidence not admissible in the trial courts of this state. It does not, as we understand it, grant to the compensation court the right to establish rules of evidence which are more restrictive than the rules applicable to the trial courts of this state.”).

146. *See, e.g.*, MINN. STAT. § 176.411, subdiv. 1 (“[T]he compensation judge is bound neither by the common law or statutory rules of evidence nor by technical or formal rules of pleading or procedure.”); *In re Wilson*, 911 P.2d 754, 758 (Idaho 1996) (“[I]n those areas where the Commission possesses particular expertise, it has the discretionary power to consider reliable, trustworthy evidence having probative value in reaching its decisions . . . even if such evidence would not be ordinarily admissible in a court of law.” (quoting *Thom v. Callhan*, 540 P.2d 1330, 1333 (Idaho 1975))); *Roberts v. J.C. Penney Co.*, 949 P.2d 613, 621 (Kan. 1997) (“We are not unaware of the decisions holding that ‘[t]he rules of evidence . . . are not applicable in workers’ compensations proceedings. . . . The admissibility of evidence is more liberal in compensation cases, not more restrictive.’” (quoting *Rodriguez v. Henkle Drilling & Supply Co.*, 828 P.2d 1335, 1341 (Kan. Ct. App. 1992)) (internal quotations omitted)); *Adkins v. R & S Body Co.*, 58 S.W.3d 428, 430 (Ky. 2001) (“[T]he principles that control the admissibility of evidence in a personal injury action . . . do not apply to workers’ compensation proceedings.”). A few states, however, follow a contrary rule binding workers’ compensation courts to the state rules of evidence. *See, e.g.*, *Paganelis v. Indus. Comm’n*, 548 N.E.2d 1033, 1038 (Ill. 1989) (“Except when the [Workers’ Compensation] Act provides otherwise, the rules of evidence apply to Industrial Commission proceedings, including those conducted before the arbitrator.”).

147. *See* Kenneth M. Berman, *The Current State of Workers’ Compensation Law and Practice*, 584 PLI/LIT 327, 330-31 (1998) (“The Acts are typically administered by a Workers Compensation Commission . . . that employ relaxed rules of evidence designed to provide for informal and rapid resolution of claims.”).

148. *See, e.g.*, MINN. STAT. § 176.411, subdiv. 1 (“Hearsay evidence which is reliable is admissible.”). Hearsay is generally defined as an out-of-court statement offered in court to prove the truth of the matter asserted. *See* FED. R. EVID. 801(c). Even when judges are bound by hearsay rules, social networking evidence is often admissible due to the hearsay exception for an admission by a party opponent under Federal Rule of Evidence 801(d)(2).

or federal court is often admissible in workers' compensation courts.¹⁴⁹ As the finder of fact, workers' compensation judges have discretion to determine if hearsay evidence should be excluded as "worthless rumor or gossip" or admitted as persuasive and reliable evidence.¹⁵⁰

Judges, however, may not entirely abandon the state court rules of evidence.¹⁵¹ Workers' compensation courts are the "gatekeepers" of what evidence to admit at trial,¹⁵² and, in doing so, they are bound by a standard of relevance.¹⁵³ Though formulations vary, evidence is "relevant" if it "tends to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence."¹⁵⁴

However, workers' compensation judges often admit hearsay evidence directly. *See, e.g.,* *Cargill, Inc. v. Conley*, 620 N.W.2d 496, 502 (Iowa 2000) (admitting hearsay evidence when the information is within the knowledge of the employer); *Chaisson v. Cajun Bag & Supply Co.*, 708 So. 2d 375, 382 (La. 1998) (providing that the "general rule" in workers' compensation courts "is to allow hearsay evidence"); *Lunde v. State ex rel. Wyo. Workers' Compensation Div.*, 6 P.3d 1256, 1260 (Wyo. 2000) (stating that "a broad range of informal evidence, including hearsay, is admissible in workers' compensation" courts).

149. *See, e.g.,* *Keiser v. Dick Lind Heating Co.*, 1996 WL 705445, at *4-5 (Minn. Work. Comp. Ct. App. Nov. 22, 1996) (admitting parts of investigative reports that the employee alleged were hearsay).

150. *Reynolds Metals Co. v. Indus. Comm'n*, 402 P.2d 414, 417 (Ariz. 1965) ("Much hearsay is worthless rumor or gossip, but there is also such a thing as 'persuasive hearsay' and the fact-finding commission may be given credit for the ability to distinguish the one from the other.").

151. *See, e.g.,* *Hudson v. Horseshoe Club Operating Co.*, 916 P.2d 786, 788-91 (Nev. 1996) (applying a relevancy standard for admissibility of evidence in a workers' compensation matter); *City of Pittsburgh v. Workmen's Compensation Appeal Bd.*, 315 A.2d 901, 903 (Pa. Commw. Ct. 1974) ("However, it has been held that section 422, and similar enactments applicable to administrative and quasi-judicial bodies, are not authority for denying parties in adversary proceedings fundamental rights embraced by some rules of evidence.").

152. *Rodriguez, supra* note 144 ("Lawyers should also keep in mind that courts are essentially the "gatekeepers" of what evidence comes in at trial . . .").

153. *See* MINN. STAT. § 176.411, subdiv. 1 (2008) (providing that "findings of fact shall be based upon relevant and material evidence only"); 1 PA. CODE § 35.161 (1989) ("relevant and material evidence shall be admissible"), *available at* <http://www.pacode.com/secure/data/001/chapter35/chap35toc.html>.

154. FED. R. EVID. 401.

State and federal courts apply the same relevancy standard to ESI as to any other form of evidence.¹⁵⁵ For example, a Texas court admitted evidence from a mother's MySpace profile in a family law matter. In terminating the mother's parental rights, the Texas Court of Appeals admitted—and relied upon—two MySpace pictures that “were captioned, ‘At Ashley House Drinking it Up [sic],’ and ‘Me Helping Ashley Stand Up, Were Both Drunk [sic],’” as well as several photographs from a MySpace page showing the mother at a bar.¹⁵⁶

Similarly, workers' compensation courts should apply their liberal evidentiary rules to admit social networking evidence that is relevant, just as they do with traditional forms of surveillance evidence. “[T]he admission of [surveillance] evidence is within the discretion of the Workers' Compensation Court.”¹⁵⁷ In *Keiser v. Dick Lind Heating Co.*, an employee injured his low back at work.¹⁵⁸ Surveillance by the defense found that the employee was exaggerating his limp, and later surveillance, on video, showed the employee installing heating ducts.¹⁵⁹ The employee was receiving temporary total disability benefits at this time and defense counsel filed a “notice of intent to discontinue temporary total disability benefits” based on the fact that the employee was working.¹⁶⁰ Defense counsel offered reports at hearing prepared by an investigation firm the insurer hired to perform surveillance of the employee's activities.¹⁶¹ The employee objected on the basis of hearsay, arguing that the reports included statements made “by unidentified third parties” to investigators, and that the

155. *See, e.g., In re F.P.*, 878 A.2d 91, 96 (Pa. Super. Ct. 2005) (“We see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.”).

156. *Mann v. Dep't of Family & Protective Servs.*, No. 01-08-01004-CV, 2009 WL 2961396, at *10 (Tex. App. Sept. 17, 2009).

157. *Aken v. Neb. Methodist Hosp.*, 511 N.W.2d 762, 768 (Neb. 1994).

158. *Keiser v. Dick Lind Heating Co.*, 1996 WL 705445, at *2 (Minn. Work. Comp. Ct. App. Nov. 22, 1996).

159. *Id.* at *2.

160. *Id.* at *3.

161. *Id.* at *4.

surveillance reports failed to identify which of several investigators prepared which parts of the reports.¹⁶² The defense argued that it had disclosed its intent to use the investigative reports months prior and had given plaintiff's counsel copies of the reports at that time.¹⁶³ In addition, all but one of the investigators attended the hearing and the plaintiff was free to call them for cross-examination.¹⁶⁴

The compensation judge excluded portions of the investigative reports containing statements made by unidentified non-parties, but admitted the rest of the reports into evidence because the testimony of the supervising investigator provided their foundation.¹⁶⁵ On appeal, the employee argued that the reports should be excluded because they were unreliable hearsay due to the investigators' misrepresentations during their investigation, making the investigators unreliable witnesses.¹⁶⁶ The workers' compensation court of appeals found that the trial judge did not abuse his discretion in admitting the evidence.¹⁶⁷ Similarly, workers' compensation judges have discretion to admit social networking evidence, in some cases even if acquired deceptively,¹⁶⁸ as gathering evidence from a social networking site is a form of surveillance.¹⁶⁹ To the extent such information is relevant to an employee's injuries or employment abilities, and has the proper foundation and authentication, the court should admit it into evidence.

2. Foundation and Authentication

Whether evidence is offered in electronic or paper form, state and federal courts can admit the proffered evidence only if, in addition to being relevant, it is properly authenticated. Authentication "is satisfied by evidence sufficient to support a

162. *Id.*

163. *Id.*

164. *Id.*

165. *Id.*

166. *Id.*

167. *Id.* at *4-5.

168. *See supra* note 136 and accompanying text.

169. *See supra* note 20.

finding that the matter in question is what its proponent claims.”¹⁷⁰ The proffering party has to establish that there is a reasonable basis for the court to draw this finding.¹⁷¹ As in *Keiser v. Dick Lind Heating Co.*, where the workers’ compensation judge permitted surveillance evidence based on the testimony of one of the investigating officers who was available to the plaintiff for cross-examination,¹⁷² foundation for authentication of social networking evidence can be established by the investigator, attorney, or paralegal who found the information about the employee on the social networking site.¹⁷³

Even with workers’ compensation’s relaxed evidentiary rules, defense counsel has to establish that any information from an employee’s social networking account was posted by the employee, because individuals can open social networking accounts under the names of other people.¹⁷⁴ It is important for

170. FED. R. EVID. 901(a). The party offering the evidence must lay a foundation for the judge to find the evidence authentic. *See, e.g.*, *Ruiz v. Virginia*, No. 1915-07-4, 2008 Va. App. LEXIS 566, at *12, *16 (Ct. App. Dec. 23, 2008) (“Foundation is a more general term for what the proponent of evidence must establish before the evidence can be admitted. . . . [T]he proponent of a document having the characteristics of a business record establishes the proper evidentiary foundation for the introduction of the document into evidence by establishing that the document is authentic.”). Although workers’ compensation judges are not bound by the federal or state rules of evidence, this standard for authentication provides a starting point.

171. *See, e.g.*, *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 542, 544 (D. Md. 2007) (“A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. . . . The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer processing.”).

172. *Keiser*, 1996 WL 705445, at *4.

173. Unlike surveillance evidence that is obtained through informal discovery, social networking evidence may be obtained through formal discovery as well. *See supra* Part II.A.3. When social networking evidence is provided by the plaintiff in discovery, foundation and authentication are not in issue, as the plaintiff does not dispute the authenticity of the evidence. In cases where information from a plaintiff’s social networking profile is obtained by informal discovery, however, defense counsel has to authenticate the evidence she seeks to introduce.

174. *Cf. Lorraine*, 241 F.R.D. at 542-43 (indicating that courts examine foundational requirements more carefully for electronically stored information than for hard-copy documents); *St. Clair v. Johnny’s Oyster &*

the person who downloaded the information from the employee's social networking account to be available to testify as to when and how it was obtained and to confirm that the copy is accurate.¹⁷⁵ Defense counsel also has to offer proof that the owner of the social networking account (the employee) actually wrote what counsel is introducing. The normal methods of proving authorship of social networking material include the admission of the author or testimony of a witness who observed the material's authorship.¹⁷⁶ Another way to authenticate such material is to demonstrate the writing matches the plaintiff's distinctive style.¹⁷⁷ If the plaintiff denies that the information on the social networking profile is hers despite a reasonable showing by defense counsel, the workers' compensation court can admit the evidence and evaluate the employee's credibility in deciding how much weight to assign to it.

3. The Notice Requirement

Although there are no workers' compensation rules specific

Shrimp, Inc., 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999) (“[T]he Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time.”); *see also* Keiser, 1996 WL 705445, at *4 (excluding surveillance evidence from unidentified third parties). One major difference between video surveillance and information gathered from social networking sites is that, with electronically stored evidence, there is an issue as to the source of the information, an issue raised in *St. Clair*. The *Keiser* court indicates that defense counsel's inability to identify a source of information is grounds for exclusion in workers' compensation cases. *Keiser*, 1996 WL 705445, at *4-5.

175. *See* Levine & Swatski-Lebson, *supra* note 14, at 3.

176. *See id.*

177. *See Lorraine*, 241 F.R.D. at 544 (“Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished. It states: ‘(b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule: . . . (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.’”). Prior postings or other writings by the plaintiff indicating a particular writing pattern, style, or other identifiable characteristics may therefore be used to authenticate social networking evidence.

to notice or disclosure of social networking evidence obtained through informal discovery, rules regulating the disclosure of surveillance evidence should apply. In at least some states, in a workers' compensation case, parties are required to make pretrial disclosure of surveillance evidence to opposing parties, to prevent unfair surprise or prejudice, or else they risk preclusion from offering the evidence at the hearing or trial.¹⁷⁸ To the extent that states do not have specific rules governing notice or disclosure of surveillance evidence, ordinary rules of notice and disclosure under the workers' compensation laws should apply.

In giving notice of social networking evidence, defense attorneys must provide copies to opposing counsel of what they intend to introduce at hearing or trial.¹⁷⁹ However, workers' compensation judges likely have the discretion to permit a party to withhold disclosure of social networking and other surveillance evidence until after the time of an employee's deposition.¹⁸⁰

178. *See, e.g.*, MINN. R. 1420.2200, subpt. 8(A) (2006) ("A party possessing relevant surveillance evidence must disclose the existence of said evidence to opposing parties . . . no later than 30 days prior to the hearing date."); 34 PA. CODE § 131.61(a) (2002), *amended by* 32 PA. BULL. 6043 (Dec. 7, 2002) ("Parties shall exchange all items and information, including medical documents, reports, records, employment records, wage information, affidavits, tapes, films and photographs, lists of witnesses, CD ROMs, diskettes and other digital recordings, to be used in or obtained for the purpose of prosecuting or defending a case, unless the foregoing are otherwise privileged or unavailable, whether or not intended to be used as evidence or exhibits."); 34 PA. CODE § 131.68(a)(9) (2002), *amended by* 32 PA. BULL. 6043 ("The deposition may be used to locate, authenticate and obtain copies of records which are material and relevant to the proceeding, including: . . . (9) Surveillance."); *Mietelski v. Banks*, 854 A.2d 579, 580 (Pa. Super. Ct. 2004) (finding that the trial court did not err in "excluding from the jury videotape surveillance evidence of Appellee, Ireneusz 'Eric' Mietelski, due to unfair surprise and prejudice caused by late production of the tape"). Surveillance evidence in workers' compensation matters could include "any photographic, video, digital, motion picture, or other electronic recording or depiction of a party surreptitiously taken or obtained without the party's expressed permission or knowledge." MINN. R. 1420.2200, subpt. 8(A). That definition encompasses information, communications, and photographs from a social networking site.

179. *See, e.g.*, MINN. R. 1420.2200, subpt. 8(A).

180. *See, e.g.*, MISS. CODE ANN. § 71-3-61(1) (West 1990); *Congleton v. Shellfish Culture, Inc.*, 807 So. 2d 492, 496 (Miss. Ct. App. 2002) ("The power to control when evidence is presented is well within the administrative law

B. *Credibility and Weight of the Evidence*

Although there is a liberal standard for the admissibility of evidence, including hearsay, in workers' compensation courts, evidence must be probative, trustworthy, and credible.¹⁸¹ As administrative agencies, these courts have the power to evaluate and weigh the credibility of evidence.¹⁸² Courts may accept all or part of the testimony of any witness.¹⁸³ In determining credibility, workers' compensation judges often pay close attention to evidence impeaching or contradicting an employee's credibility,¹⁸⁴ and this can include surveillance evidence.

In *Aken v. Nebraska Methodist Hospital*, the Supreme Court of Nebraska overturned the workers' compensation court of appeals and upheld the compensation judge who relied on the defense's video evidence to find that the plaintiff lacked credibility.¹⁸⁵ The plaintiff in *Aken* worked as a nurse.¹⁸⁶ She

judge's statutory power.”).

181. See *Story v. Wyo. State Bd. of Med. Exam'rs*, 721 P.2d 1013, 1018 (Wyo. 1986) (“Where hearsay evidence is by statute admissible in administrative proceedings, it is often held that it must be probative, trustworthy and credible; and, although it may not be the sole basis for establishing an essential fact and is insufficient to support an administrative decision, it may be considered as corroborative of facts otherwise established.”).

182. See *Kloepfer v. Lumbermen's Mut. Cas. Co.*, 916 P.2d 1310, 1312 (Mont. 1996) (“The Workers' Compensation Court, as the finder of fact, is in the best position to assess witnesses' credibility and testimony.”); *Wagaman v. Sioux Falls Constr.*, 576 N.W.2d 237, 242 (S.D. 1998) (“Department is allowed to weigh the evidence and determine the credibility of the witnesses.”).

183. See *Jordan v. Workmen's Compensation Appeal Bd.*, 704 A.2d 1063, 1066 (Pa. Commw. Ct. 1997) (“[T]he factfinder in a workers' compensation proceeding may accept the testimony of any witness in whole or in part.”).

184. See *McGee v. J.D. Lumber*, 17 P.3d 272, 278 (Idaho 2000) (“Evidence impeaching a claimant's credibility need not be ignored”); *Schneider v. S.D. Dep't of Transp.*, 628 N.W.2d 725, 729-30 (S.D. 2001) (“The Department, after hearing numerous inconsistent statements made by Schneider, found Schneider to be not credible. ‘Where there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous.’” (internal citation omitted)).

185. 511 N.W.2d 762, 768-69 (Neb. 1994).

186. *Id.* at 765.

argued that she was unable to perform her job duties as a result of a work injury and called witnesses at her hearing to testify to that effect.¹⁸⁷ Evidence presented by both the plaintiff and defendant at trial revealed conflicting diagnoses from doctors.¹⁸⁸ At the time of rehearing, the defense offered a report by a private investigator that “described surreptitious visual and videotaped surveillance” and the court admitted a surveillance videotape of the employee.¹⁸⁹

The plaintiff testified that, even on a “good” day, she “limped noticeably” and “a layman could see the limp.”¹⁹⁰ The surveillance tape, however, showed the plaintiff doing activities such as walking, carrying a child, carrying boxes, and moving furniture with ease and without any noticeable limping.¹⁹¹ The court admitted the surveillance evidence and relied on it heavily in terminating the employee’s workers’ compensation benefits.¹⁹² The type of analysis and reasoning in *Aken* in which the court admitted video surveillance evidence and subsequently used it to weigh the plaintiff’s credibility is likely applicable to social networking evidence showing or discussing an employee’s participation in physical activities.¹⁹³ If a workers’ compensation judge finds an abundance of evidentiary inconsistencies, preventing a determination that the plaintiff’s injury is compensable, the employee has failed to meet her burden of proof necessary to win the case.¹⁹⁴

187. *Id.* at 766.

188. *Id.* at 765-66.

189. *Id.* at 766.

190. *Id.*

191. *Id.*

192. *Id.* at 768-69.

193. There are no published workers’ compensation cases directly discussing the credibility of social networking evidence. The Texas Court of Appeals, however, considered the credibility of evidence from MySpace.com. *In re J.W.*, No. 10-09-00127-CV, 2009 WL 5155784, at *4 (Tex. App. Dec. 30, 2009) (“[T]he trial judge said that he would ‘consider the credibility of the source’—MySpace.”).

194. *See Aken*, 511 N.W.2d at 766 (“The evidence presents a question of credibility. The Court received Exhibits 1-23 which included two videotapes showing plaintiff walking briskly and carrying boxes. This evidence is wholly inconsistent with plaintiff’s assertions that she must walk on the sides of her feet to avoid pain and must avoid all carrying of groceries and that her pain has completely incapacitated her.” (quoting the compensation court panel)); *see also In re Corman*, 909 P.2d 966, 971-72 (Wyo. 1996) (“Inconsistencies in

A final evidentiary issue present in workers' compensation cases is for the compensation judge to balance the probative value of the evidence against the potential for unfair prejudice.¹⁹⁵ There is, again, an absence of workers' compensation cases addressing this particular issue with regard to social networking evidence, but two federal court cases are instructive. In *United States v. Drummond*,¹⁹⁶ a federal criminal case, the court discussed the admissibility of pictures from a MySpace account, weighing the probative value versus the danger of unfair prejudice.¹⁹⁷ The court found the photographs provide probative value as to whether the defendant committed the crime at issue.¹⁹⁸ The court went on to discuss the possibility of the evidence being prejudicial to the defendant.¹⁹⁹ Ultimately, the court found that, depending on the testimony presented at trial, the probative value of the photographs may outweigh any danger of unfair prejudice.²⁰⁰ The court deferred on making a ruling, finding that it must wait until the time of trial to rule based on whether the testimony regarding the alleged crime and the defendant's source of income is disputed at trial.²⁰¹

the evidence that prevent the finder of fact from determining whether the injury is compensable mean that the claimant has failed to meet his burden of proof. A claimant cannot prevail if factors necessary to prove his claim are left to conjecture.”).

195. This standard is based on Federal Rule of Evidence 403 but is also a universal standard used by workers' compensation judges. *See, e.g.*, Dixon Prop. Co. v. Shaw, 2 P.3d 330, 332 n.4 (Okla. 1999).

196. No. 1:09-CR-00159, 2010 WL 1329059 (M.D. Pa. Mar. 29, 2010).

197. *Id.* at *2.

198. *Id.* The MySpace photographs from Drummond depicted the defendant holding wads of money and a gun. *Id.* at *1 (“The photos depict Defendant counting, showing-off, and throwing large wads of cash while wearing a hat and sunglasses. . . . Additionally, one photo depicts Defendant either pretending to point a gun at the camera or pointing a gun at the camera.”).

199. *Id.* at *2.

200. *Id.*

201. *Id.* (“[I]f testimony presents evidence that Defendant had no known source of income and yet often had significant quantities of cash on-hand, but Defendant disputes having possessed large amounts cash, it is possible that the relevance of the photos could outweigh any unfair prejudice. . . . As the Government suggests, possession of a firearm may be relevant to a charge of drug trafficking because firearms are known to be ‘tools of the trade’ of drug trafficking. . . . However, the Government has not stated that testimony in

An insurance law case addressing the admissibility of ESI provides a closer comparison to workers' compensation for evaluating the danger of unfair prejudice and its potential consequences for both plaintiff and defendant. In *Lorraine v. Markel American Insurance Co.*, a boat insured by Markel American Insurance was damaged by lightning.²⁰² Magistrate Judge Grimm raised and analyzed the issue of balancing the danger of unfair prejudice against the probative value of e-mails, computer animations and simulations, and digital photographs although neither the plaintiff nor defendant directly raised this issue.²⁰³ In evaluating this final hurdle to admissibility, Magistrate Judge Grimm stated that it is generally better to admit evidence if there is any doubt about the danger of unfair prejudice.²⁰⁴

Lorraine suggests that, in addressing the admissibility of ESI, courts will play particular attention to the danger of unfair prejudice outweighing the probative value of electronic evidence when "the evidence would contain offensive or highly derogatory language that may provoke an emotional response."²⁰⁵ Relevant social networking evidence should be admissible in workers' compensation cases because it involves an employee's physical capabilities and is unlikely to contain offensive or derogatory language or depictions. Also, judges in workers' compensations courts can control for emotional persuasion in a way that judges sending cases to juries cannot, reducing the risk of prejudice. Yet, workers' compensation

this case will support the assertion that Defendant or the members of his conspiracy used firearms in furtherance of their drug-trafficking endeavors. Therefore, it is unclear to the Court that, in this case, possession of a firearm is intrinsic to the drug trafficking or conspiracy charged.").

202. 241 F.R.D. 534, 534 (D. Md. 2007).

203. *Id.* at 584.

204. *Id.* ("Generally, '[i]f there is doubt about the existence of unfair prejudice, confusion of issues, misleading, undue delay, or waste of time, it is generally better practice to admit the evidence, taking necessary precautions of contemporaneous instructions to the jury followed by additional admonitions in the charge.'" (quoting JACK B. WEINSTEIN & MARGARET A. BERGER, *WEINSTEIN'S FEDERAL EVIDENCE* § 403.02(2)(c) (Joseph M. McLaughlin 2d ed. 1997))). Obviously, providing proper instructions to the jury is not applicable to workers' compensation matters where decisions are made by judges and not juries.

205. *Id.*

attorneys do need to consider whether information from an employee's social networking profile would "unfairly prejudice the party against whom it is offered" or "unduly delay the trial of the case."²⁰⁶

Courts or legislators should not adopt rigid rules adopting or banning evidence from social networking sites in workers' compensation cases. Rather, workers' compensation judges should hear the evidence and decide whether to give it weight and, if so, how much. Judges are gatekeepers of social networking evidence, and they need to understand and evaluate this form of technology in particular cases.

V. Conclusion

The lawyers, judges, insurance companies, and parties within workers' compensation systems will increasingly confront the discovery, privacy, professional responsibility, and evidentiary issues that arise at the crossroads of workers' compensation law and social networking. In the absence of case law and ethics opinions that discuss these exact issues, this Article starts with the rules that govern workers' compensation cases, and discusses how they might apply to lawyers gathering, producing, and introducing evidence from social networking sites. But this Article is only a starting point. As workers' compensation systems are built on efficiency, flexibility, and discretion, workers' compensation is an ideal area of law for lawyers and judges to experiment with how to address some of the unique challenges and opportunities that social networking poses in litigation.

While there is a lack of legal authority on these issues, that should not cloud the reality that many employees are using social networking in their daily lives. One thing of which we are certain is that lawyers who practice in the workers'

206. *Id.* ("Thus, when a lawyer analyzes the admissibility of electronic evidence, he or she should consider whether it would unfairly prejudice the party against whom it is offered, . . . unduly delay the trial of the case, or interject collateral matters into the case."). The issue of undue delay plays heightened importance in balancing probative value versus the danger of unfair prejudice in workers' compensation cases because of workers' compensation's underlying emphasis on efficiency.

compensation field need to be able to navigate around social networking sites, such as Facebook, LinkedIn, and MySpace, and know how they work. Social networking is no longer a new technology, and ignorance should not be an excuse to the applicability of evidence from social networking sites in litigation.