SOCIAL MEDIA AND PRIVACY: WHEN PERSONAL POSTS INTERSECT WITH THE BUSINESS OF LITIGATION

Jeanne Kosieradzki[*]

I. INTRODUCTION

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual the right to be let alone."[1] These words, circulated over 100 years ago in a famous law review article by Samuel Warren and Louis Brandeis, still guide business interactions today.[2] The recent inventions and business methods referenced above were instantaneous photographs and the newspaper enterprise.[3] Warren and Brandeis feared that mechanical devices would invade the "sacred precincts of private and domestic life and make good the prediction that what is whispered in the closet shall be proclaimed from the housetops."[4] Recent inventions and business methods no longer require a proclamation from the housetops to quickly disseminate personal information. In fact, through a recent invention, information can be disseminated faster from the closet than from the housetops. This invention is the social network website.[5]

Sites such as Facebook and MySpace have become the forum for conversation among teens and young adults. "Nearly three quarters (73%) of online teens and an equal number of (72%) young adults use social network sites."[6] While there are many social network sites,[7] "Facebook is the most ubiquitous of them all with upwards of 500 million members and a Quantcast-estimated 135 million daily visitors" says Lee Rainie, the director of the Pew Research Center's Internet and American Life Project, which studies the web's impact on society.[8]

While teens and young adults are the heaviest users, there are users of all ages. "Over the past few years, Facebook has morphed from a closed site for college students to an online playground where barriers of age, distance, background and technological expertise have been leveled. It has become a rare space where generations can meet on neutral turf to share and interact."[9]

Despite what seems like the perfect solution for socializing in a busy and global world, social networking website postings provide opportunities for personal information to work against the poster in the business world. Judges, colleges and employers use Facebook to gather data.[10] Information shared on these sites range from discussions about illegal activities like substance

---

[*] Associate Professor of Legal Studies, Hamline University.

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[2] *Id.*

[3] *Id.* at 195.

[4] *Id.*

[5] Mark McGuiness, *The Top Ten Social Networks for Creative People,* LATERAL ACTION (November 6, 2008), http://lateralaction.com/articles/social-networks-for-creatives.

[6] Amanda Lenhart, Kristen Purcell, Aaron Smith & Kathryn Zickuhr, *Social Media and Young Adults,* PEWINTERNET.ORG (February 3, 2010), http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

[7] McGuiness, *supra* note 5.

[8] Monica Hesse, *Keeping Up With Social Networking Sites: How Much Is Enough?*, PEWINTERNET.ORG (October 19, 2010). http://www.pewinternet.org/Media-Mentions/2010/Keeping-up-with-social-networking-sites.aspx.

[9] Molly Baker, *OMG! My Grandparents R My BFF*, THE WALL STREET JOURNAL (May 9, 2011). http://online.wsj.com/article/SB10001424052748703280904576247152267875970.html.

[10] Sandra Hornberger, *Social Networking Websites: Impact On Civil Litigation and the Legal Profession in Ethics*, 27 TOURO L. REV. 284, (2011).

abuse and evading police capture to information relevant to a contract, employment or personal injury dispute. The individuals who post on these websites seem unwary and uninhibited in the information they share. Stories such as an employee posting a picture of a fish caught with the time and date of the picture stamped on the posting being the same time and date the employee was supposed to be making a delivery for his employer are common. Also common is the loss of a scholarship after a university discovers pictures of underage drinking, as well as the compromise of a lawsuit after pictures are found proving claims of injury are not genuine.[11] Information posted to a social networking site provides a potential goldmine for those seeking information useful to various types of litigation.

When, during the discovery phase of litigation, an opponent serves a discovery request seeking access to the litigant's social networking site, clients and attorneys alike are taken aback. Clients may be surprised because some believe there is an expectation of privacy in their social networking site postings. Attorneys who represent these clients are many times from a generation unaware of the endless conversations posted and recorded on social networking sites. They are also surprised at the incriminating evidence stored on the sites. They make every effort to construe the rules of discovery against production of social networking site postings.

This article will establish that a litigant cannot avoid the production of social networking site postings through an expectation of privacy assertion. Secondly, it will consider to what extent the potentially revealing information contained in those postings will be discoverable in a lawsuit. Recent cases addressing social networking postings indicate that discovery will be allowed but suggest two schools of thought on the extent of discoverability.[12] One line of cases suggests a liberal approach allowing complete access to everything on the site.[13] Another line of cases offers a more workable format and sets parameters only allowing discovery of limited information.[14] These two lines of cases will be compared and contrasted. Finally, this article will discuss the unethical behavior that results if a lawyer's litigation practice entails befriending a person on a social networking site for the purpose of finding potentially incriminating information useful in litigation.[15]

---

[11] Janet Kornblum & Mary Beth Marklein, *What You Say Online Could Haunt You.* USA TODAY (March 8, 2006). http://www.usatoday.com/tech/news/internetprivacy/ 2006-03-08-facebook-myspace_x.htm.
[12] *See generally,* Romano v. Steelcase, 907 N.Y.S.2d 650, 651 (N.Y. Sup. 2010).
[13] Liberal Approach Case, See Romano v. Steelcase, 907 N.Y.S.2d 650, 651 (N.Y. Sup. 2010).
[14] Limited Approach Case, *See EEOC v. Simply Storage Mgmt., LLC,* 270 F.R.D. 430, 432 (S.D. Ind. 2010).
[15] Phila. Bar Ass'n Prof'l Guidance Comm. Op. 2009-2 (2009) *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

II. RIGHT TO PRIVACY IN SOCIAL NETWORKING SITE POSTINGS

A. Reality of Social Website Postings and Whether Such Postings are Protected by One's Right to Privacy

Evaluating whether litigation compels production of information posted on a social networking site such as MySpace or Facebook, begins with a consideration of the poster's right to privacy. Some people believe that a right to privacy exists in information posted to a social networking site, particularly when they have taken the time to set all of their "privacy" settings to limit the availability of the information to a particular audience, or when they send a message to only a few select friends. Whether people are justified in their expectation of privacy in social networking site postings turns on an analysis that involves considerations beyond their individual belief. While the law currently is developing with respect to privacy and the use of technology, [16] hiding behind a right to privacy argument during litigation will not prevent court-ordered production of social networking site postings.[17]

When considering privacy claims in social networking site postings, there are two primary areas of law to consider. There is the constitutional right to privacy and there is the common law tort of invasion of privacy.[18] When courts balance the discoverability of social networking site posting with a litigant's privacy objections they seem to draw from both bodies of law.[19] "Constitutional privacy jurisprudence has tremendously influenced judges confronted with invasion of privacy claims derived from other legal sources, such as state constitutions, state common law, and state statutory law."[20]

As stated in the introduction to this article, both the right to privacy and the resulting invasion of privacy tort were advocated for as early as 1890 in an article written by Warren and Brandeis entitled *The Right to Privacy*.[21] In this law review, the authors indicated that the right to privacy included the right to be left alone. [22] The Fourth Amendment to the United States Constitution, and similar state constitutional provisions, support the right to be left alone in certain situations.[23] Though the constitutional right to privacy is not specifically stated in the

---

[16] City of Ontario v. Quon, ___ U.S. ___, 130 S.Ct. 2619, 2630 (2010) (noting that states have recently passed statutes requiring employers to notify employees when monitoring their electronic communications).

[17] *See* Woodrow Hartzog, *Website Design as a Contract*, 60 AM. U. L. REV. 1635, 1653 (2011) (advocating for an alternative view suggesting that, even though courts rely primarily on the terms of service and privacy policy of a social networking site in determining a reasonable expectation of privacy, website features and designs such as privacy settings should be considered part of the privacy agreement between the user and the social networking site).

[18] Constitutional Right To Privacy Cases, *see* Griswold v. Conneticut, 381 U.S. 479 (1965); Roe v. Wade, 410 U.S. 113, 152 (1973); Katz v. United States, 389 U.S. 347, 373 (1967). Common Law Tort of Invasion of Privacy case, see Rumbauskas v. Cantor, 138 N.J. 173, 179, 649 A. 2d 853 (quoting William L. Prosser, The Law of Torts § 112 (3d ed. 1964).

[19] *See* Romano v. Steelcase, 907 N.Y.S.2d 650 (N.Y. Sup. 2010).

[20] *See* Alexander Rodriguez, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace***,** 47 EMORY L.J. 1439 (1998).

[21] Warren & Brandeis, *supra* note 1, at 193.

[22] Warren & Brandeis, *supra* note 1, at 193.

[23] U.S. CONST. amend. IV.

Fourth Amendment, it has come to be recognized as a basic human right through well-known Supreme Court decisions.[24]

The 1967 United States Supreme Court decision in *Katz v. United States* provides guidance on what it means to have a right to privacy.[25] Though *Katz* involves a criminal case, the *Katz* "reasonableness" test is essentially the same approach used by state courts to analyze the common-law tort of invasion of privacy.[26]

The *Katz* Court indicates that the fourth amendment only protects against searches that violate a reasonable expectation of privacy. [27] A reasonable expectation of privacy exists when (1) privacy is expected and (2) when the reasonable person would have an expectation of privacy.[28] What a person knowingly exposes to the public, even if transmitted from the home or office, is not subject to the Fourth Amendment's protection.[29] Similarly, any reasonable expectation of privacy in information is lost if it is voluntarily turned over to third parties.[30] This was the situation in *United States v. Miller* wherein the Supreme Court held that a bank depositor had no reasonable expectation of privacy in information voluntarily provided to bank employees in the typical course of business.[31]

Parties subjected to a discovery request seeking social networking postings may argue that they should not have to produce postings because they expect privacy in the postings. They may argue that the social networking site is a medium of discovery far more invasive into private realms than traditional discovery devices and that with traditional discovery devices, the litigants are asked a question to which they respond with potential production. They do not have to provide a key to their home so that their adversary can look for evidence of any potential thought that might be helpful during litigation. While this view may present social networking sites as more important in people's lives than they actually are, one court has stated that "cell phones and text message communications are so pervasive that some persons may consider them essential means or necessary instruments for self-expression, even self-identification."[32] The same can be said of social networking site postings. However, whether the party that has been asked to respond to discovery believes they are entitled to privacy is irrelevant, because the expectation of privacy analysis turns on whether the reasonable person would have an expectation of privacy in such postings. [33]

In analyzing whether the reasonable person expects privacy in information posted to MySpace or Facebook, *Smith v. Maryland* provides guidance. [34] In *Smith*, the telephone

---

[24] *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965); Roe v. Wade, 410 U.S. 113, 152 (1973); Katz v. United States, 389 U.S. 347, 373 (1967).
[25] Katz, 389 U.S. at 351.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *United States v. Miller*, 425 U.S. 435, 442 (1975).
[31] *Id.*
[32] *City of Ontario*, ___ U.S. ___, 130 S.Ct. at 2630.
[33] See Bryce Clayton Newell, *Rethinking reasonable expectations of privacy in online social networks*, 17 RICH. J.L. & TECH 12 (2011) (recognizing that few courts respect an expectation of privacy in online posts and urging courts to accept contemporary conceptions of what constitutes reasonable expectations of privacy and consider expanding the reasonable expectations of privacy in online social networks).
[34] See Smith v. Maryland, 442 U.S. 735 (1979).

company installed a device known as a pen register at the request of the police department.[35] A pen register records the numbers dialed from the petitioner's home.[36] In determining there was no expectation of privacy in this information, the Smith court held:

"Petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not 'legitimate.' First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes…. Even if petitioner did harbor some subjective expectation of privacy, this expectation was not one that society is prepared to recognize as 'reasonable.' When petitioner voluntarily conveyed numerical information to the phone company and 'exposed' that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police."[37]

The view expressed in *Katz*, *Miller* and *Smith* continues to be the view even though much of the information transmitted today is shared electronically.[38] In fact, any expectation of privacy decreases with online transmissions because the person who shared information is unable to prevent the recipient of the communication from forwarding the message to third parties.[39]

Ironically, Facebook's own privacy policy indicates similar procedures.[40] Section 2 of Facebook's privacy policy contains a section entitled "information from other users." It states: "We may collect information about you from other Facebook users, such as when a friend tags you in a photo, video, or place, provides friend details, or indicates a relationship with you."[41] The section also states: "We keep track of some of the actions you take on Facebook, such as adding connections (including joining a group or adding a friend), creating a photo album, sending a gift, poking another user, indicating you "like" a post, attending an event, or connecting with an application. In some cases you are also taking an action when you provide information or content to us. For example, if you share a video, in addition to storing the actual content you upload, we might log the fact that you shared it."[42]

In addition, the Federal Trade Commission (FTC) maintains a presence on the Facebook site and warns users that: "By using Facebook and its application providers, you may be providing non-government third parties access to your personal information, which can be used to distinguish or trace your identity. In addition, Facebook and its application providers may use persistent tracking technology throughout their sites.[43]

MySpace provides similar cautionary language to that provided by Facebook. MySpace's cautionary language states that:

---

[35] *Id*. at 737.
[36] *Id*.
[37] *Id.* at 735.
[38] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).
[39] *Id.*
[40] *Data Use Policy*, FACEBOOK.COM, http://www.facebook.com/about/privacy/ (last visited, January 23, 2012.).
[41] *Id.*
[42] *Id.*
[43] www.facebook.com/federaltradecommission?v=app_4949752878.

> There may be instances when MySpace may access or disclose pii (personally identifiable information), Profile Information or non-pii without providing you a choice in order to: (i) protect or defend the legal rights or property of MySpace, our Affiliated Companies or their employees, agents and contractors (including enforcement of our agreements); (ii) protect the safety and security of Users of the MySpace Services or members of the public including acting in urgent circumstances; (iii) protect against fraud or for risk management purposes; or (iv) comply with the law or legal process. In addition, if MySpace sells all or part of its business or makes a sale or transfer of all or a material part of its assets or is otherwise involved in a merger or transfer of all or a material part of its business, MySpace may transfer your pii to the party or parties involved in the transaction as part of that transaction.[44]

Courts are likely to view Facebook and MySpace postings in a similar fashion to the way the Supreme Court in *Smith v. Maryland* viewed information transmitted to the telephone company. That is, any reasonable expectation of privacy in information is lost if it is voluntarily turned over to third parties.[45] This includes information transmitted electronically.[46] As stated previously, any expectation of privacy decreases with on-line transmissions.[47]

B. Does Increasing Privacy Settings Make Postings Private?

Some litigants may argue that choosing an increased privacy setting or "locking" information posted to a social networking site will create a reasonable expectation of privacy, but this is an argument not judicially favored.[48] In *Romano v. Steelcase*, *Inc.,* where the plaintiff sought damages for personal injury, a New York trial court recently stated: "It is reasonable to infer from the limited postings on plaintiff's public Facebook and MySpace profile pages that her private pages may contain material and information that are relevant to her claims or that may lead to the disclosure of admissible evidence. To deny defendant an opportunity to access these sites not only would go against the liberal discovery policies of New York favoring pretrial disclosure, but would condone plaintiff's attempt to hide relevant information behind self-regulated privacy settings."[49]

The right to privacy is the right of the people of the United States that is embedded in the constitution and interpretative Supreme Court decisions.[50] The right to privacy does not protect information when there is an unreasonable expectation of privacy and this includes information transmitted to third parties.[51] Social networking site postings are transmitted to third parties and are not likely to provide a reasonable or legitimate expectation of privacy regardless of whether they limit their privacy settings or not.[52]

---

[44] www.myspace.com/index.cfm?fuseaction=misc.privacy.
[45] *Smith v. Maryland,* 442 U.S. 735, 735 (1979).
[46] *Guest,* 255 F.3d at 333.
[47] *Id.*
[48] Romano v. Steelcase, 907 N.Y.S.2d 650, 658 (N.Y. Sup. 2010).
[49] *Id*. at 659.
[50] *See Griswold,* 381 U.S. at 485 (1965); *Roe,* 410 U.S. at 152); *Katz*, 389 U.S. at 373.
[51] See Smith v. Maryland, 442 U.S. 735 (1979).
[52] See Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS L.J. 1131

III. ARE SOCIAL NETWORKING SITE POSTINGS DISCOVERABLE?

Since courts are unlikely to prevent discovery of social networking site postings, it is important to consider the extent of discovery courts are willing to allow. It is illegal under many circumstances, including discovery, for an electronic communication service provider to provide access to social networking site postings to anybody who requests access.[53] The Stored Communications Act prohibits an entity such as Facebook or MySpace from disclosing information posted by a site owner.[54] Section 2702 of this act states:

> 2702 Voluntary disclosure of customer communications or records.
>
> 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 to any person or entity the contents of a communication while in electronic storage by that service.
>
> Exceptions for disclosure of communications. -- A provider described in subsection (a) may divulge the contents of a communication
>
> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) as otherwise authorized in section 2703 of this title.
>
> (3) With the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
>
> (4) To a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> (5) As may be necessarily incident to the service or to the protection of the rights or property of the provider of that service;
>
> (6) To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;
>
> (7) To a law enforcement agency.[55]

(2011) (discussing a comprehensive history and analysis of reasonable expectation of privacy from *Katz* to *Quon*).

[53] 18 U.S.C. § 2702 and § 2703.

[54] 18 U.S.C. §§ 2701-2712 (2006).

[55] 18 U.S.C. § 2702 (2006).

Anybody familiar with social networking sites, and the lack of inhibition some people show who post to these sites, realizes that incriminating information may await if those sites can be accessed. Since litigation attorneys know they are unlikely to obtain access through the site administrators, they must turn to other means. These other means include discovery requests.

Since access to social networking sites is not likely to survive a privacy argument, it is important for those engaged in the business of litigation to become familiar with potential discovery requests and applicable discovery rules. Discovery requests, as found in recent cases, may include requests for production such as:

> (1) All photographs or videos posted by plaintiff or anyone on her behalf on Facebook or MySpace from April 23, 2007 to the present.
>
> (2) Electronic copies of plaintiff's complete profile on Facebook and MySpace (including all updates, changes, or modifications to plaintiff'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.[56]

The extent to which a judge agrees that requested discovery be allowed varies from court to court.[57] Determining what will be ordered discoverable begins with an analysis of the Rules of Civil Procedure from the jurisdiction in which the dispute arises.[58] Since many state rules of procedure are patterned after the federal rules, the federal rules are considered here.

The Federal Rules of Civil Procedure define the scope of discovery broadly as: "any non-privileged matter that is relevant to any party's claim or defense."[59] The rule further explains that the information "need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.[60]

While Rule 26 provides for liberal discovery, discovery is not unlimited and Fed. R. Civ. P. 26 (C)(1) indicates that "the court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense."[61] Before a court issues a protective order pursuant to Rule 26, however, the court has to be satisfied that the objecting party has "shown specifically, despite the broad and liberal construction afforded the federal discovery rules, how each interrogatory is not relevant or how each question is overly broad, burdensome or oppressive by submitting affidavits or offering evidence revealing the nature of the burden."[62]

---

[56] EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 432 (S.D. Ind. 2010).
[57] See *Romano,* 907 N. Y. S. 2d at 650; EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010).
[58] *Id*., McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. Lexis 270, (Pa. Cnty. Ct. Sept. 9, 2010), Romano v. Steelcase, 907 N.Y.S. 2d 650 (N.Y. Sup. 2010) and EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. 2010).
[59] FED. R. CIV. P. 26(b)(1).
[60] *Id.*
[61] FED R. CIV. P. 26(c)(1).
[62] Campagnie Francaise D'Assurance Pour Le Commerce Exterieur v. Phillips Petroleum Co., 105 F.R.D. 16, 42 (D.C.N.Y 1984).

A. Liberal Discovery of Social Network Postings

Some courts have allowed the discovery of social networking postings under liberal discovery rules. In *Romano v. Steelcase*, the defendant sought authorization from the plaintiff to view information posted on MySpace and Facebook.[63] In allowing the discovery, the court noted the liberal discovery rules in New York, and that the private pages of the plaintiff's social networking site may contain relevant information.[64] The court further noted that when creating her social networking sites, the plaintiff "consented to sharing personal information with others in spite of her privacy settings as that is the very nature of these sites or they would cease to exist."[65] In this finding, the court referenced the fact that neither Facebook nor MySpace guarantees complete privacy and plaintiff therefore could not have a legitimate expectation of privacy.[66]

The *Romano* Court found support for this position in the social networking sites themselves when it noted: "MySpace warns users not to forget that their profiles and MySpace forums are public spaces, and Facebook's privacy policy set forth, inter alia, that 'you post User Content…on the site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable.[67]

Another court to employ liberal discovery rules in finding social networking site postings discoverable and "reasonably calculated to lead to the discovery of admissible evidence" is *Ledbetter v. Wal-Mart Stores.*[68] In *Ledbetter,* the court denied plaintiff's request for an *in camera* review of Facebook postings due to physician-patient as well as spousal privilege.[69] The court determined that the plaintiff waived her physician-patient privilege when she put her medical condition at issue in the lawsuit and similarly that she waived the spousal privilege when plaintiff's wife made the spousal relationship an issue by bringing a loss of consortium claim.[70] Numerous other courts have not been persuaded by privacy arguments with respect to social networking site postings.[71]

---

[63] *Romano,* 907 N.Y.S.2d at 651.
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] Ledbetter v. Wal-Mart Stores, Inc., No. 06 Civ. 01958 (D. Colo. April 21, 2009).
[69] *Id.*
[70] *Id.*
[71] *See* Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125 (2009) (explaining that no reasonable person would feel an expectation of privacy is found once info is posted on MySpace); McMillen v. Hummingbird Speedway, Inc., 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, (Pa. Cnty. Ct. Sept. 9, 2010) (clarifying that in denying a "social network site privilege" the court indicated expectation that Facebook postings would be confidential is not realistic); Leduc v. Roman, [2009] CanLII 6838 (ON S.C.) (court notes that it is beyond controversy that a person's Facebook pages may contain relevant documents); Murphy v. Perger, [2007] O.J. No. 5511 (S.C.J.) (allowing access to private part of Facebook does not constitute a fishing expedition); Bishop v. Minichiello, [2009] B. C. J. No. 692 (Sup. Ct.)(holding that a hard drive produced for limited purpose of ascertaining amount of time spent on Facebook each night was valid for purpose of evaluating fatigue claim); Kent v. Laverdiere, [2009] CanLll (ON S.C) (ordering, despite objection, that review of social network site by producing party for a determination of relevance would take a minimum of 75 hours, court inclined to allow access to social networking site information when boiler plate pleading alleges claim for loss of enjoyment of life as there is likely to be relevant information on site but not inclined to allow access when claim is for loss of care, comfort, guidance, support and companionship as there is not likely to be information posted that are relevant to those

B. Less Liberal Discovery of Social Network Postings

In some jurisdictions, a less liberal approach to discovery has been adopted.[72] In *EEOC v. Simply Storage Mgmt.*, the EEOC filed a complaint on behalf of two claimants who alleged that the defendant businesses were liable for sexual harassment by a supervisor.[73] During the discovery phase, the defendant sought**, "***all* photographs or videos posted by plaintiff or anyone on her behalf on Facebook or MySpace from date of incident to the present… Electronic copies of plaintiffs *complete* profile on Facebook and MySpace."[74]

In denying complete access to the social networking sites, the court in *Simply Storage* found:

> (1) Social networking site content was not shielded from discovery simply because it was "locked" or "private."
>
> (2) Anything that a person says or does might in some theoretical sense be reflective of her emotional state. But that is hardly justification for requiring the production of every thought plaintiff may have reduced to writing or, indeed, the deposition of everyone she may have talked to.[75]

The court then provided guidance on the scope of permissible discovery in the case before them. This guidance makes clear that the court would not favor unrestricted access:

> Claimant's Verbal Communications: The appropriate scope of relevancy is any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and SNS applications for claimants for the period from April 23, 2007, through the present that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events *that could reasonably be expected to produce a significant emotion, feeling or mental state*.
>
> Third-party Communications: Third-party communications to claimants must be produced if they place these claimants' own communication in context.

---

claims); Kourtesis v. Joris, [2007] Can Lll 39367 (holding that photos on social networking sites were relevant and subject to review to evaluate claims for loss of enjoyment of life).

[72] 270 F.R.D. 430, 430 (S.D. Ind. 2010).

[73] *Id.*

[74] *Id.* at 432.

[75] *Id.* at 435.

> Photographs and Videos: The same test set forth above can be used to determine whether particular pictures should be produced. For example, pictures of the claimant taken during the relevant time period and posted on a claimant's profile will generally be discoverable because the context of the picture and the claimant's appearance may reveal the claimant's emotional or mental status. On the other hand, a picture posted on a third party's profile in which a claimant is merely "tagged" is less likely to be relevant. In general, a picture or video depicting someone other than the claimant is unlikely to fall within the definition set out above. These are general guidelines provided for the parties' reference and not final determinations of what pictures must be produced consistent with the guidelines above.[76]

The court set specific parameters around the information that the defendant was allowed access to.[77] As indicated in the above language, the parameters allowed access to information relating to the claimants emotional or mental status.[78] Interestingly, the court referenced the decision in *Bass v. Miss Porter's Sch.* where the defendant did not ask for complete MySpace and Facebook profiles but for documents related to the plaintiff's alleged "teasing and taunting" suffered at Miss Porter's School and those representing or relating to communications between the plaintiff and anyone else related to the allegations in the amended complaint. [79] The plaintiff objected that the request sought information that is "irrelevant and immaterial, and not reasonably calculated to lead to the discovery of admissible evidence."[80] The court ordered that the plaintiff provide copies in compliance with defendant's request. The court also ordered that the plaintiff produce to the court for *in camera* review a complete copy of Facebook documents along with a copy of the set of documents produced to the defendant.[81] Upon comparison of the complete copy of Facebook documents with those produced to the defendant, the court felt that the plaintiff's response to the request was under-inclusive.[82] The court's review of the unproduced portion of the Facebook production revealed a number of communications to and from plaintiff that were clearly relevant to the action.[83] Plaintiff's undifferentiated objection was therefore overruled.[84]

The *Bass* court was not willing to allow complete access to plaintiff's Facebook at the time of the discovery request but rather gave the plaintiff the opportunity to comply with the

---

[76] *Id*. at 436 (emphasis added).
[77] *Id.*
[78] *Id.*
[79] Bass v. Miss Porter's School, No. 3:08cv1807, 2009 WL 3724968 (D. Conn. Oct. 27, 2009).
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] Bass v. Miss Porter's School, No. 3:08cv1807, 2009 WL 3724968 (D. Conn. Oct. 27, 2009).
[84] *Id.*

defendant's discovery request before ordering complete access.[85] Other courts have denied unrestricted access to social networking site postings as well.[86]

More than likely, a court will allow some sort of discovery of social network site postings. The extent to which discovery will be allowed will vary from jurisdiction to jurisdiction.[87]

IV. ACCESS OBTAINED THROUGH BEFRIENDING A LITIGANT ON FACEBOOK

If in the business of litigation, the attorney is not able to get access to social network site information through the service provider or through the discovery process, it is important to remain free of temptation to get access to information through unethical means. Access to a person's social networking site can be obtained through sending a "friend" request to that person, which, if accepted, provides significant access to personal information. This is a tempting way to obtain information useful to a lawsuit, but it is not appropriate in the litigation setting, where the rules of professional conduct control. Because many state rules of professional conduct are modeled after the American Bar Association's Model Rules of Professional Conduct, those rules will be considered in this section.

In considering accessing social network site postings four rules of professional conduct are particularly relevant. Those rules are Model Rules of Professional Conduct R. 8.4, R. 5.3, R. 4.1 and R. 8.3.[88]

> Model Rule of Professional Conduct Rule 8.4 states, in pertinent part, that, "It is professional misconduct for a lawyer to… (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation." [89]

Model Rule of Professional Conduct R. 5.3 states:

---

[85] *Id.*

[86] McCann v. Harleysville Ins.Co., 78 A.D.3d 1524, 910 N.Y.S.2d 614 (N.Y. App. Div. 2010) (holding that the production of Facebook posts were denied as a fishing expedition since defendant had not demonstrated the relevance of the disputed posts to the facts disputed in the case); Rozell v. Ross-Holst, No. 05 Civ. 2936, 2006 WL 163143 (S.D.N.Y Jan. 20, 2006) (explaining that in denying defendant's motion to compel production of all non-intercepted emails the court noted that the defendant is correct that an interested party cannot be the "final arbiter" of relevance but that counsel for the producing party is judge of relevance in the first interest); Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149 (D. Nev. Jan. 9, 2007)(reasoning that in a sexual harassment action, the court could decline defendants request for access to private messages on plaintiff's MySpace as fishing expedition since defendant had nothing more than a suspicion that plaintiff was using MySpace to facilitate the same kinds of relationships she has characterized as sexual harassment and that such access would cast too wide a net since defendant could also obtain irrelevant information. Defendant could serve properly limited requests for production of relevant email communications).

[87] See *Romano,* 907 N. Y. S. 2d at 650 and *Simply Storage Mgmt.,* 270 F.R.D. at 430.

[88] MODEL RULES OF PROF'L CONDUCT R. 4.1, MODEL RULES OF PROF'L CONDUCT R. 5.3, MODEL RULES OF PROF'L CONDUCT R. 8.3, MODEL RULES OF PROF'L CONDUCT R. 8.4.

[89] MODEL RULES OF PROF'L CONDUCT R. 8.4.

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) a partner, and a lawyer who individually or together with other lawyers possess comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take remedial action.[90]

Analyzing these two rules together establishes that attempting to pose as a "friend" on a social network site for the purposes of viewing personal information is unethical.[91] The lawyer or non-lawyer assistant is attempting to access this information of an adversary through a friend request for no reason other than to fish for information that might be incriminating in a forthcoming or pending lawsuit. This is dishonest and deceitful and in violation of the Rules of Professional Conduct.[92] Behavior of this type is deceitful because: "It omits a highly material fact, namely, 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. The omission would purposefully conceal the 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."[93]

Even if the adversary reveals in their friend request that they are associated with a party in opposition to the litigant, this may still be viewed as "conduct involving dishonesty, fraud, deceit or misrepresentation" because the litigant may not be familiar enough with the litigation process to know that accepting the friend request is not in their best interest.[94]

---

[90] MODEL RULES OF PROF'L CONDUCT R. 5.3.
[91] MODEL RULES OF PROF'L CONDUCT R. 5.3; MODEL RULES OF PROF'L CONDUCT R. 8.4.
[92] *Id.*
[93] Phila. Bar Ass'n Prof'l Guidance Comm. Op. 2009-2 (2009) *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.
[94] *Id.,* MODEL RULES OF PROF'L CONDUCT R. 4.1.

Model Rule Professional Conduct 4.1 also merits consideration. It states that, "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."[95]

Posing as a "friend" on a person's Facebook page for the purpose of gaining access to information potentially detrimental to that person is a false statement of material fact in violation of Model Rule Professional Conduct R. 4.1.[96] Not only is it unethical for a lawyer or non-lawyer assistant to attempt to get social networking site postings by posing as a "friend" on Facebook, a lawyer who discovers that another lawyer has violated one of the rules above is obligated to inform the appropriate professional authority of such violation.[97]

V. CONCLUSION

While Warren & Brandeis were justified in their belief that "there is a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons," the sharing of social network postings do not fall into the category of an unauthorized circulation, notwithstanding the fact that a "privacy" setting has been selected.[98] It must be understood that social transmission of network postings is not categorically considered an unauthorized circulation. When setting up a social media account, the providers inform the user of limited rights to privacy via the policies of the site. Further, the information is provided in an environment that allows and encourages sharing of information between a vast network of individuals, not affiliated with the original poster.

The real issue lies in determining to what extent the posting can be discovered. In that regard there is no final answer. Lawyers engaged in the business of litigation will be entitled to discover at least some information posted to a social networking site if not complete access. Success will depend on which court the lawyer is appearing before. Some courts allow for liberal discovery, while others are more cautious. Either way, it is important to understand that the information within the sites may fall into the hands of the opposing attorney.

When considering the method of obtaining this information, it is clear that "befriending" a litigant will be considered unethical and unwarranted.[99] This conduct is dishonest and deceitful and requires the lawyer who is aware of such conduct to inform the appropriate professional authority.

Privacy rights and discovery in the world of social media is a rapidly evolving area of law. Every attorney must understand the ramifications and possibilities of what can happen upon the discovery of information contained on social media sites. Whether a court applies liberal or limited discovery, the ramifications of the obtained information can be profound.

---

[95] MODEL RULES OF PROF'L CONDUCT R. 4.1.
[96] Phila. Bar Ass'n Prof'l Guidance Comm. Op. 2009-2 (2009) *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.
[97] MODEL RULES OF PROF'L CONDUCT R. 8.3.
[98] Warren & Brandeis, *supra* note 1, at 195.
[99] Phila. Bar Ass'n Prof'l Guidance Comm. Op. 2009-2 (2009) *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.