New York Law Journal

A NEW YORK LAW JOURNAL SPECIAL SECTION

An ALM Publication

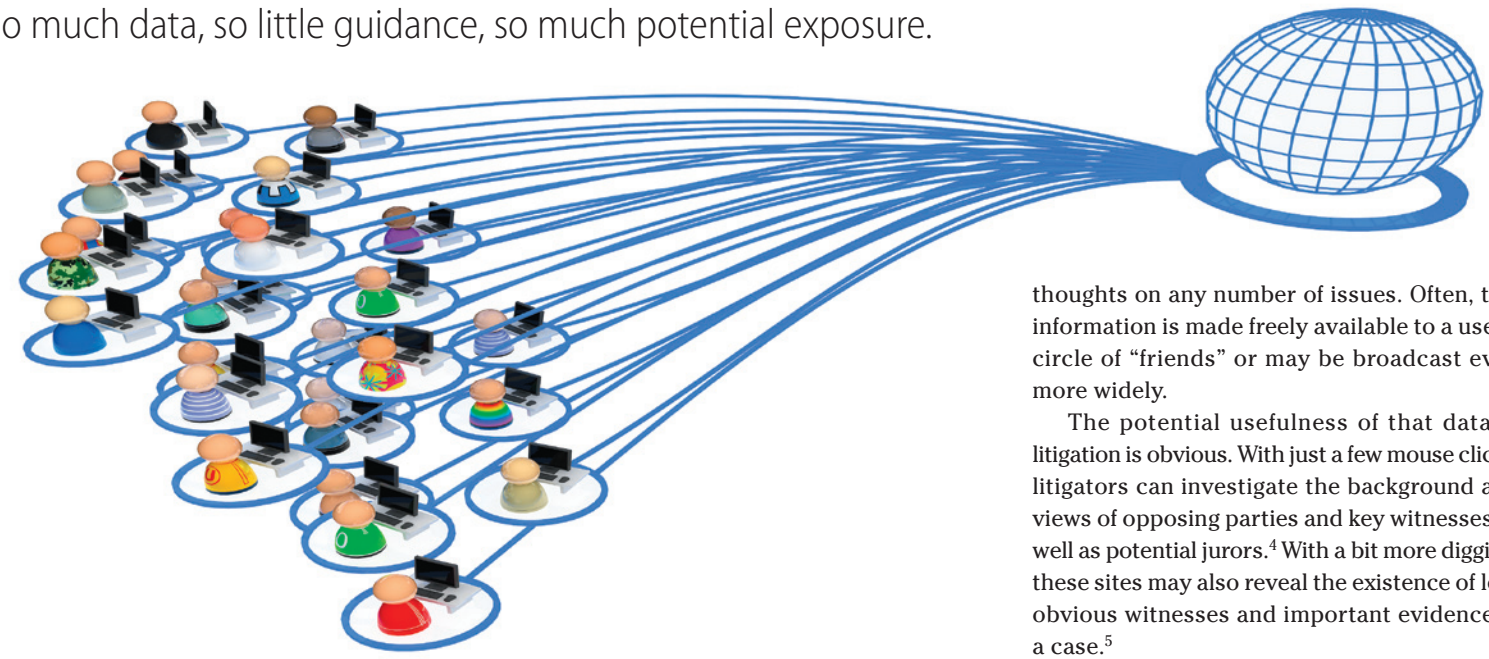
Litigation

WWW.NYLJ.COM

MONDAY, NOVEMBER 15, 2010

Social **Networking**

So much data, so little guidance, so much potential exposure.



© BIGSTOCK

BY STEPHEN M. PRIGNANO AND ANDREW P. FISHKIN

THE RECENT EXPLOSION of social networking represents a paradigm shift in online communications. According to the latest statistics, individuals now spend more time interacting through social networking sites than they do through traditional e-mail.[1] Facebook alone now boasts more than 500 million active members,[2] larger than the entire population of the United States.[3] MySpace, Twitter, LinkedIn and other sites have seen similar growth.

STEPHEN M. PRIGNANO, *a partner in the Providence, R.I. office of Edwards Angell Palmer & Dodge, is the chair of the firm's mass torts practice group.* ANDREW P. FISHKIN, *a New York partner, co-chairs the firm's litigation department.* ZOE COOPER, *a litigation associate, assisted in the preparation of this article.*

This new mode of communication is not simply confined to personal use. Businesses have discovered social networking's marketing potential and have set up their own social networking pages to attract customers and promote their products or services. Many employees also use social networking on company time, and with company computers, for both personal and business use.

All of this online social interaction has created mountains of personal information about users that, prior to the advent of social networking, would have been regarded as private and difficult to obtain. A typical user's "profile page" may include information about the individual's location and background, videos and photographs posted by the user and his or her friends, real time updates tracing the user's every move and mood, and groups that reflect the user's interests and views. So-called micro-blogging sites like Twitter provide up-to-the-minute information on a user's musings and thoughts on any number of issues. Often, this information is made freely available to a user's circle of "friends" or may be broadcast even more widely.

The potential usefulness of that data in litigation is obvious. With just a few mouse clicks, litigators can investigate the background and views of opposing parties and key witnesses as well as potential jurors.[4] With a bit more digging, these sites may also reveal the existence of less obvious witnesses and important evidence in a case.[5]

Social networking sites have already proven their worth to plaintiffs' lawyers in mass tort and consumer cases by revealing consumer complaints about products, and as a means of recruiting and interacting with potential clients.

The prevalence of social networking data raises novel issues with respect to the use of this information in litigation. Preservation, privacy and admissibility issues frequently arise in this context, as do many others. Unfortunately, the law has significantly lagged behind social networking. Some of the more problematic issues are only now being addressed, while others continue to await much needed guidance from the courts.

Access and Preservation Challenges

Litigants seeking social networking data face considerable challenges with respect to both access and preservation of potential evidence.

A user's online pages are usually password protected and their contents can be deleted with just a few strokes of the keyboard. Social networking pages are also dynamic, with new content frequently added or changed. A user's social network page, therefore, may be significantly different from day to day, or even hour to hour.

These characteristics make it difficult to access and isolate the contents of social networking pages at any given point in time. Indeed, the individual's own computer may not provide a "picture" or "snapshot" of the page as it appeared at a time relevant to the litigation. As will be seen, privacy and authentication issues present real obstacles for parties attempting to use social networking data in litigation.

For litigants, including businesses, that may be the target of discovery requests seeking social networking data, the problems of access and preservation are likewise complex. Parties generally have a duty to preserve any potentially relevant evidence once litigation is "reasonably anticipated."[6] And courts have imposed significant penalties on parties who fail to preserve electronically stored information.

To the extent that businesses maintain social networking pages, a duty to preserve that data may arise if relevant to anticipated or actual litigation. That data will also need to be captured as part of a litigation hold. While many businesses have protocols and document preservation policies directed at traditional e-mail and electronic computer files, few have procedures that touch upon or concern social networking data. These businesses will be ill-prepared to meet their preservation obligations with respect to that data.

Even more problematic for businesses, employees may use company computers to post messages to their personal social networking accounts that will be relevant to litigation. This information may, in fact, be accessible in the form of "cached" Web pages on a company's computer servers. The company, however, may not even be aware that an employee's personal social networking postings are available on its system, and that information is unlikely to be captured by a traditional litigation hold.

In these circumstances, there is a considerable risk that relevant data will be lost or destroyed, with potentially serious consequences for both the party seeking the information, as well as the party who has a duty to preserve it. Unfortunately, little guidance has been provided by the courts regarding a company's obligations in these circumstances, and a number of unanswered questions remain. Businesses are therefore well advised to develop internal policies governing the use and preservation of social networking data, and should make those policies well known to their employees.

Privacy

The retrieval and use of information on social networking sites can pose Fourth Amendment and privacy concerns, and there are a number of factors that may affect the level of protection a court is willing to grant these communications. First, the Stored Communications Act, 18 U.S.C. §2702, presents a threshold challenge to litigants seeking to obtain an individual's social networking data directly from a third party social networking Web site.

Few businesses have protocols and preservation policies that touch upon or concern social networking data and will be **ill-prepared** to meet their **preservation obligations** with respect to that data.

In *Crispin v. Christian Audigier Inc.*,[7] the U.S. District Court for the Central District of California examined whether messages and "wall posts" from social networking Web sites can be subpoenaed in a civil case. Plaintiff in that case brought an action for the misuse and non-consensual use of his artwork.[8] Defendants served subpoenas on Facebook and MySpace, seeking all of plaintiff's communications related to a relevant license agreement.[9]

In its ruling on plaintiff's motion to quash, the court held that the Stored Communications Act prevents providers of communication services from divulging private communications to certain parties and creates a Fourth Amendment-like privacy protection by statute.[10] The court therefore extended protection to private messages on social networking sites since they "are not readily accessible to the general public."[11] At the same time, the court implied that wall postings and comments on these sites are not protected where they are readily available to a wider audience.[12]

For parties seeking to prevent disclosure of social networking data on privacy grounds, a "reasonable expectation of privacy under the circumstances" must be demonstrated.[13] As the author of a profile or social networking communication, a user has the primary responsibility to limit access to information that the user believes is private.

Based on Web site privacy preferences chosen by the user, a profile page or other communication may be available to the general public or only those authorized to access it. Where the user elects to make information available more generally, the courts have held that there is a lower expectation of privacy and, consequently, such information will receive less protection from disclosure.[14]

Other factors may also undermine a user's expectation of privacy in social network postings. For example, in the employment setting, social networking data created or accessed by an employee on the employer's computer may be subject to company policies in effect at the time. Those policies may very well provide that an employee has no expectation of privacy with respect to communications using company computer systems.

Indeed, even "privacy policies" established by social networking Web sites may weaken a user's privacy claim. Many of these policies make clear that information provided by the user is generally intended to be shared with others.[15]

Similarly, the function and/or purpose of a social networking site may also be important in determining whether a user has a reasonable expectation of privacy. Some such sites may be geared toward more limited, professional networking, while others may strive to spread a user's postings far and wide.[16]

Likewise, the type of social networking data requested may also be a factor in determining privacy protection. For example, users of social networking sites will likely have a stronger privacy interest in webmail and private messages sent through those sites and directed at a particular recipient, as opposed to comments posted on profile pages that may be available to others more generally.[17]

Admissibility

Assuming that access, preservation and privacy issues can all be overcome in a bid to use social networking evidence in litigation, a final challenge awaits. Ultimately, the data must be admitted into evidence and all of the rules for admissibility that apply to other forms of evidence apply to social networking data.[18] Particularly problematic in this regard is the foundational requirement of authenticity.

Information found on social networking sites is especially susceptible to fraud and

manipulation.[19] And the problem of viruses or spam e-mails from "friends" as a result of Internet hacking is prevalent in social networking communications.[20] Moreover, as mentioned earlier, there is the problem of obtaining an accurate snapshot of a social networking page at any given point in time. For these reasons, courts are especially cautious when admitting social networking data and other electronically stored information.[21]

As the court observed in *Lorraine v. Markel Am. Insur. Co.*, "[a]pplication of the Federal Rules of Evidence to electronic information… is not well settled and courts vary in how they weigh whether evidence is sufficient to support a finding of authenticity."[22] The court, however, observed that Rule 901(b)(4) is most frequently used to authenticate electronically stored information, including the content of Web sites.[23]

Ultimately, the data must be **admitted into evidence** and all of the **rules for admissibility** that apply to other forms of evidence apply to social networking data. **Particularly problematic** in this regard is the foundational requirement of **authenticity**.

Under that rule, authentication may be accomplished by circumstantial evidence.[24] Importantly, the creation of electronic data may itself produce certain information that can be used as circumstantial evidence to identify the author of the posting.[25] The court in *Lorraine* described the use of "hash marks" (numerical identifiers assigned to a file) and "metadata" (information describing the history, tracking, or management of an electronic document) as potentially useful in authenticating electronic data.[26]

This same information might also prove useful in identifying the contents of a user's social network page at a certain point in time. For these reasons, litigants are well advised to seek metadata and other identifying information in discovery.

The Future

With the number of online social network users growing each year,[27] such data will undoubtedly expand as an important litigation tool. And as social networking data takes greater prominence in litigation, issues beyond those mentioned in this article will certainly arise.

Unfortunately, the law is far behind this new form of communication. Just as occurred with the advent of e-mail, however, the courts need to address the challenges and complexities raised by social networking and provide meaningful guidance to litigants.

Businesses likewise need to recognize that social networking data has the potential to create significant exposure to companies both in terms of liability and in the cost of complying with electronic discovery. For these reasons, the development of comprehensive internal policies will be a key to managing the business risks created by online social networking.

1. Nielson.com, "What Americans Do Online: Social Media and Games Dominate Activity," Aug. 2, 2010, http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+%28Nielsen+Wire%29.
2. Facebook Press Room: Statistics, http://www.facebook.com/press/info.php?statistics (last visited Oct. 19, 2010).
3. Robert Schlesinger, "U.S. Population, 2010: 308 Million and Growing," U.S. News.com, Dec. 30, 2009, http://politics.usnews.com/opinion/blogs/robert-schlesinger/2009/12/30/us-population-2010-308-million-and-growing.
4. Molly McDonough, "Trial Consultants Add Facebook/MySpace to Juror Research Toolbox," A.B.A. J., Sept. 29, 2008; Karen L. Stevenson, "What's on Your Witness' MySpace Page?," ABAnet.org, March 2008, http://www.abanet.org/litigation/litigationnews/2008/march/0308_article_myspace.html.
5. See, e.g. *Mackelprang v. Fidelity Nat'l Title Agency*, No. 2:06-cv-00788-JCM-GWF, 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007) (where defendant sought to admit content on plaintiff's social networking page to counter plaintiff's sexual harassment claim).
6. *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, No. 05 Civ. 9016, 2010 U.S. Dist. LEXIS 4546, at *14-15 (S.D.N.Y. Jan. 15, 2010).
7. No. CV 09-09509 MMM, 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010).
8. Id. at *2.
9. Id. at *4-5.
10. Id. at *12.
11. Id. at *77.
12. Id. at *78-79.
13. *Moreno v. Hanford Sentinel Inc.*, 91 Cal. Rptr. 3d 858, 862 (Cal. Ct. App. 2009).
14. See *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001) (holding that public postings lack a legitimate expectation of privacy); see also *Moreno*, 91 Cal. Rptr. 3d at 862 (holding that since plaintiff posted her article on MySpace, "no reasonable person would have had an expectation of privacy regarding the published material.")
15. See Twitter Privacy Policy, http://twitter.com/privacy (last visited Oct. 19, 2010) ("Our Services are primarily designed to help you share information with the world. Most of the information you provide to us is information you are asking us to make public.")
16. Compare Twitter "About Us," http://twitter.com/about (last visited Oct. 19, 2010) ("Twitter asks 'what's happening' and makes the answer spread across the globe to millions, immediately.") with LinkedIn "About Us," http://press.linkedin.com/about (last visited Oct. 19, 2010) ("LinkedIn exists to help you make better use of your professional network…").
17. See *Crispin*, 2010 U.S. Dist. LEXIS at *77 ("[w]ith respect to webmail and private messaging, the court is satisfied that those forms of communications media are inherently private such that stored messages are not readily accessible to the general public."); see also *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996) (indicating that general e-mail messages are afforded more privacy than "chat room" postings).
18. See *Lorraine v. Markel Am. Insur. Co.*, No. PWG-06-1893, 2007 U.S. Dist. LEXIS 33020, at *15 (D. Md. May 4, 2007) (indicating that the rules of evidence must be considered whenever electronically stored information is offered as evidence).
19. Vasanth Sridharan, "How to Hack Facebook in 51 Seconds," Business Insider.com, March 28, 2008, http://www.businessinsider.com/2008/3/facebook-hacking-it-can-take-less-than-1-minute.
20. Claire Suddath, "The Downside of Friends: Facebook's Hacking Problem," TIME.com, May 5, 2009, http://www.time.com/time/business/article/0,8599,1895740,00.html.
21. See *Lorraine*, 2007 U.S. Dist. LEXIS at *33 ("courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication of 'hard copy' documents.")
22. Ronald J. Levine and Susan L. Swatski-Lebson, "Are Social Networking Websites Discoverable?," Law.com, Nov. 13, 2008, http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202425974937; see *Lorraine*, 2007 U.S. Dist. LEXIS at *36 ("there is no 'one size fits all' approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges.")
23. *Lorraine*, 2007 U.S. Dist. LEXIS at *44-45.
24. Id. at *44.
25. See, e.g. id. at *50 ("metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it.")
26. Id. at *46-49.
27. Nielson.com, supra note 1.