Tweets and Status Updates Meet the Courtroom: How Social Media Continues to be a Challenge for E-Discovery in 2011

By Nadine R. Weiskopf

LexisNexis®

According to a survey from Arbitron Inc. released in April 2011, the percentage of Americans age 12 and older who have a profile on one or more social networking websites has reached almost half (48 percent) of the population—double the level from two years ago (24 percent in 2008). The study also revealed that consumer use of social networking sites is not just a youth phenomenon. While nearly eight in ten Americans in their teens (78 percent) have personal profile pages, almost two-thirds of 25- to 34-year-old adults (65 percent) and half of 35- to 44-year-olds (51 percent) also now have personal profile pages.

Moreover, these social media sites receive a lot of attention from users. The Arbitron® study found that 30 percent of Americans age 12 and older, who have a profile on at least one social networking website, use those sites "several times a day" as compared with only 18 percent one year ago. Simply put, social media has become a part of mainstream daily behavior.

For litigation professionals, the social media explosion is more than a cultural phenomenon; it is simultaneously creating unprecedented opportunities and challenges in the pursuit of electronic evidence. On the one hand, social media presents an exciting new tool in the arsenal of judges and lawyers seeking to acquire relevant electronic data. At the same time, the unique nature of social networking websites is frustrating the ability of lawyers and electronic discovery experts to gather information they know is crucial to their cases.

More Social Media Use Means More Electronic Evidence

There is a very simple principle fueling the increased attention from litigation professionals when it comes to social media and electronic discovery: any medium through which people interact and express themselves is a medium that may need to be reviewed for potentially relevant information in litigation discovery.

Just consider the staggering number of users of social media platforms. In July 2011, Facebook® announced they now have more than 750 million active users worldwide and Twitter® now has nearly 200 million users who send out more than 1 billion "tweets" per week. Of the Top 20 most visited U.S. websites in 2010, eight of them were social media sites.

What's more, social media is actually beginning to make in-roads as a leading avenue for business communications. A 2010 study by Burson-Marsteller found that, of the Fortune Global 100 companies, 65 percent have active Twitter® accounts, 54 percent have Facebook® fan pages, 50 percent have YouTube® video channels and 33 percent have corporate blogs. And according to the technology research firm Gartner, over the next four years, social networking services are predicted to replace email as the primary vehicle for interpersonal communications for 20% of business users.

The upshot of this trend is the erosion of the distinction between "email communication" and "social media communication" that we have come to draw in recent years, creating a much wider universe of potentially relevant communications to survey during electronic discovery.

Until recently, there has been very little guidance for litigants on how to discover potential evidence from social media websites. Moreover, the courts themselves have split dramatically on what is subject to discovery from such sites. Over the last six months, there has been an influx of cases—and even an Ethics Committee opinion—providing more guidance for litigants.

New Ethics Opinion Provides Guidance on "Friending" Jurors and Witnesses

When it comes to evolving areas of law, it can be highly unpredictable as to when and whether key cases will arise to provide direction. Ethics opinions can be highly helpful in providing guidance in such cases. On May 24, 2011, the San Diego County Bar Legal Ethics Committee issued an opinion to help parties and their attorneys navigate around the arising commonplace use of social media and its possible impact on litigation dynamics[1]. The hypothetical concerned a plaintiff's attorney in a wrongful termination action who "friends" senior employees of the defendant corporation seeking information damaging to the defendant's case. The Committee found that it is unethical for a lawyer to submit a "friend" request to a potential witness or opposing party if their goal in doing so is to get inside information for use in the litigation. For a represented party, the "friend" request is considered an ex parte communication, while for an unrepresented party it violates the "attorney's duty not to deceive." The same request to a witness is held unethical if it doesn't include a disclosure of the purpose of the request. Clear guidance like this is helpful to attorneys in navigating these uncharted waters but, as with most areas of law, much of this guidance must be pulled and pried from case law which isn't always quite as clear cut.

Authentication of Electronic Discovery Derived from Social Media Sites Does a 180° Turn

In 2010, we saw the courts becoming increasingly comfortable with technology and discovery[2]. In the first half of 2011, however, we've seen some uncertainty arise in connection with the authentication of electronic data derived from social media sites which has led to clearer authentication holdings.

On April 15, 2011, the Massachusetts Court in *Commonwealth v. Purdy*[3] demonstrated a distinct apprehension for the potential for fraud in connection with electronic communications. In *Purdy*, the defendant was convicted of running a prostitution house. The trial court allowed various emails to be admitted into evidence, including ones that clearly indicated that prostitution services were being provided. The defendant author objected to the admission of the emails, arguing that it could only be properly authenticated by him. The defendant, of course, argued that although it was his computer, he had not authored the emails. He pointed to the fact that his computer was shared as evidence that someone else would have access and could have written the emails. The court held that the emails were not properly authenticated and that there was too much of an opportunity for fraud in connection with the defendant's email. The court did not feel that the facts that the emails were on the defendant's email account, appeared on his hard drive and even contained his photo were sufficient to allow for authentication and that only the defendant could authenticate the emails in this case.

> *"According to the technology research firm Gartner, over the next four years, social networking services are predicted to replace email as the primary vehicle for interpersonal communications for 20% of business users."*

Last winter, we discussed challenges in authenticating evidence derived from social media with a colorful case of first impression by the Maryland Court of Appeals, *Griffin v. State*[4]. In *Griffin*, the court allowed for a printout of a murder defendant's girlfriend's MySpace® page, to be authenticated by the police officer who printed it from the website. In April 28, 2011, however, the Maryland Supreme Court showed the same apprehension for fraud demonstrated by the *Purdy Court*, overruling the Court of Appeals decision and rejecting circumstantial authentication for the admission of MySpace® evidence. The Court based part of its decision on the fact that there is very little security around who can create a MySpace profile and little to no authentication takes place to ensure that the person who creates the account is the same one depicted. As a result, the brief honeymoon of being able to authenticate MySpace pages by printing a third-party's page from their website is over.

1. The San Diego Ethics Opinion is SDCBA Legal Ethics Opinion 2011-2
2. Connecticut court outlined in detail the procedures that the computer forensic specialist should follow. *Genworth Financial Wealth Management Inc. vs. McMullan*, 2010 U.S. Dist. LEXIS 53145 (D. Conn. June 1, 2010); Fourth Circuit Court of Appeals held that it "accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer," *United States v. Williams*, 2010 U.S. App. LEXIS 1347 (4th Cir Jan 21, 2010); Court provided detailed instructions on the protocol for cloned hard drives. Court held that any request for investigation of a hard drive must contain a specific protocol including, *Schreiber v Schreiber*, 2010 NY Slip Op 20271 (N.Y. Sup. Ct. 2010).
3. Commonwealth v. Purdy, 459 Mass. 442 (Mass. 2011)
4. *Griffin v. State*, 2010 Md App. LEXIS 87 (Md. Ct. Spec. App. May 27, 2010)

These two cases clearly demonstrate that, going forward, the proper course for parties to authenticate email from a shared computer or a MySpace posting is have the author of the MySpace page authenticate it.

The *Purdy Court* provided additional guidance to litigants seeking to authenticate evidence derived from MySpace pages. First, the Court noted that the purported author could be asked to testify as to whether he/she created the profile in question and/or posted the statement at issue. In addition, the litigating parties could "search the computer of the person who allegedly created the profile." Finally, the Court noted that the information could be sought directly from the social media provider. The first option is the simplest but, in the two cases cited above, was unlikely to occur. This second course is a common use of forensics services and could appropriately authenticate the evidence but is also costly and doesn't overcome the shared computer issue. Moreover, if the social media site belongs to a witness rather than a litigant, the party seeking such a search could face a challenge in getting such an intrusive discovery allowed. The final option unfortunately ignores the many obstacles that websites, such as Facebook and Twitter, have put in the path of litigants seeking information from their media sites.

Employees' Access of Social Media and Private Email Sites from their Employer-Issued Computers Continues to Split the Courts

Last year, we also looked at the impact on social media and discovery on employee lawsuits. The first such case was *EEOC v. Simply Storage Management*[5], a dispute involving two employees' sexual harassment claims, where a federal court permitted the employer to obtain discovery of an employee's social networking activity that, through privacy settings, the employee had made "private" and not available to the general public.

> *The path to discovering data from social networking sites is not clear and the admissibility of such evidence varies from coast to coast as much as the weather.*

Two other cases set the stage in 2010 on the challenges of electronic data discovery and social media in lawsuits between employers and employees although these focused more on discoverability of email. In *Stengart v. Loving Care Agency*[6], the New Jersey Supreme Court held that emails between an employee and her attorney sent from her personal email on the employer's laptop were subject to the attorney-client privilege in spite of the company's use policy providing otherwise. The Court held that company policy did not convert the employee's emails with her attorney into company property.

Similarly, in *Convertino v. United States DOJ*[7], the Court upheld the attorney-client privilege of a federal prosecutor's emails to his personal attorney that were sent on the DOJ's email system. The court noted that the Justice Department's email policy permitted personal use of its email system. Conversely in *Alamar Ranch, LLC v. County of Boise*[8], issued shortly before, the Idaho Court held that the attorney-client privilege had been waived by an employee who sent emails to her attorney through the company's email address because both had notice that the email was on the company's computer and would be accessible and stored by the company. Clearly the courts are split on the discoverability of emails either accessed on a private email account through an employer-issued computer or even sent from the employer's employee-issued email account.

In 2011, the potential for the types of claims that an employer could raise against its employee for use of social media on an employer-issued computer became of rising concern to roughly 95 percent of the employees in the United States. In *United States v. Nosal*[9] the Ninth Circuit followed the pro-employer path laid out by cases like Alamar when it held that an employee's use of a computer in violation of the employer's use policy was grounds for a criminal indictment under the Computer Fraud and Abuse Act.

5. *EEOC v. Simply Storage Mgmt.*, 270 F.R.D. 430 (S.D. Ind. 2010)
6. *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (N.J. 2010)
7. *Convertino v. United States* DOJ, 674 F. Supp. 2d 97 (D.D.C. 2009)
8. *Alamar Ranch, LLC v. County of Boise*, 2009 U.S. Dist. LEXIS 101866 (D. Idaho Nov. 2, 2009)
9. *United States v. Nosal*, 642 F.3d 781 (9th Cir. Cal. 2011)

In contrast, the District Court in Florida held the direct opposite in *Lee vs. PMSI*[10], issued in May 2011. In *Lee*, the employee sued her employer, PMSI, for pregnancy discrimination. PMSI counterclaimed under the Computer Fraud and Abuse Act, alleging that the employee partook in excessive use of the Internet by visiting social networking websites such as Facebook and by sending numerous personal emails through her Verizon® email account. The *Lee Court* recognized that there would be few employees who would not be liable under such a strict application of the Computer Fraud and Abuse Act. While directly contrary to Nosal, the court never cited the case, causing the same split between the coasts and inevitable "forum shopping" that we've seen spurred in 2010 by *Crispin vs. Christian Audigier, Inc. and Romano v. Steelcase Inc*[11] split.

This Year's Sanctions Case Carefully Watched by Litigants

Underlying the need to properly address arising issues in e-discovery—such as the discovery of social media—are the annual sanctions cases that have historically reached jaw-dropping proportions. This year's leading sanctions case in the e-discovery arena was filed on June 2, 2011, by J-M Manufacturing Company against McDermott Will & Emery, claiming that the firm failed to adequately review the work of its contract attorneys provided by Stratify, which resulted in the production of 3,900 privileged documents.

The use of contract attorneys provided by vendors to review vast numbers of documents is a common practice that appeared shortly after the birth of e-discovery. This case demonstrates that all parts of the e-discovery process are still under scrutiny and subject to review and possible redefinition by the courts. As a result, it is expected to have far-reaching impact on e-discovery practices regardless of the outcome.

Conclusion

As the use of social networking services continues to accelerate, it's inevitable that litigation professionals will need to become better equipped when it comes to conducting electronic discovery in social media. In general, there are two legal options for how to gather electronic information from a social networking site: (1) Obtain consent to produce the requested data; or (2) File a motion to compel with the court, demanding the production of data.

Also keep in mind that the major social networking services, much like the courts, generally encourage litigants to resolve their discovery issues on their own and to issue their requests for account information directly to the opposing party in a dispute. Moreover, the site operators are quick to emphasize the seriousness of the SCA, which effectively prohibits them from disclosing the contents of an individual account to any non-governmental entity.

So, if a litigant believes that certain information from a social network is indispensable and is not within the possession of either party in the dispute, they must serve a subpoena on the service. This can be an expensive proposition, depending on the company involved. Facebook, for example, charges "a mandatory, non-refundable processing fee" of $500 per production request, an additional $100 fee for notarized declarations and an extra $200 fee for expedited responses.

The path to discovering data from social networking sites is not clear and the admissibility of such evidence varies from coast to coast as much as the weather. In an area of law known for its tremendous sanctions, clear guidance from the courts is absolutely required before law firms and their clients can safely wade through these shark-infested waters. In the interim, the best path for litigants to follow is to keep a careful eye on the emerging case law and ethics opinions.

10. *Lee v. PMSI, Inc.*, 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011)
11. In *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010) the defendant subpoenaed Facebook and other social networking services, seeking all communications between Crispin and a third party. The Court quashed the portions of the subpoenas that related to private messaging, finding that those postings on social media sites "can constitute ['electronic communications services']" under the Stored Communications Act. Conversely, in *Romano v Steelcase Inc.*, 2010 NY Slip Op 20388, 2 (N.Y. Sup. Ct. 2010) the Court held that precluding defendant from accessing the plaintiff's private postings on Facebook and MySpace "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."

About the author

Nadine Weiskopf is director of strategic planning for litigation software at LexisNexis, where she is responsible for developing and executing strategic plans for various service and software lines. Prior to joining LexisNexis in 2006, she was a litigator at Jeffer, Mangels, Butler & Marmaro, and other West Coast law firms. Weiskopf earned her law degree from the Seattle University School of Law and her undergraduate degree from the University of Washington. She can be contacted at nadine.weiskopf@lexisnexis.com.

This document is for educational purposes only and should not be construed as legal advice. For legal advice applicable to the facts of your particular situation, you should obtain the services of a qualified attorney licensed to practice in your state. LexisNexis does not warrant this document is complete or error-free and does not guarantee the functionality or features of any LexisNexis products that may be identified. If written by a third party, the opinions may not represent the opinions of LexisNexis.

LexisNexis, Lexis, Nexis, and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.
Other products or services may be trademarks or registered trademarks of their respective companies. © 2011 LexisNexis. All rights reserved. BLT00184-0 0811