



HOME

In This Issue

- This Week's Feature
- Legal News
- DRI History
- DRI News
- And The Defense Wins!
- Legislative Tracking
- Quote of the Week
- DRI Cares
- DRI CLE Calendar

Links

- About DRI
- Annual Meeting
- Membership
- Membership Directory
- News and Events
- CLE Seminars and Events
- Publications
- The Alliance
- DRI Europe
- Archive

This Week's Feature

Discovery of Social Networks: Getting It, Getting the Most Out of It, and Getting It into Evidence
By Stephen M. Brooks and Matthew E. Brown
Nelson Mullins Riley & Scarborough, LLP, Atlanta, Georgia

You are working on a case in which the plaintiff is alleging that your client's product caused development of a severe and permanent neurological disability from manganese poisoning. As a defense lawyer, you need evidence that is going to show the judge and jury that the claim is bogus. Would pictures of the plaintiff racing motor boats help? This is exactly what happened in *In re: Welding Fume Prods. Liab. Litig., Ernest Ray v. Lincoln Elec.*, No. 1:04-cv-18252, MDL 1535, No. 03-17000, (N.D. Ohio), and shortly after the defendants found the pictures, the plaintiff's claims were dismissed. These pictures came to light only because the defendants found them on plaintiff's Facebook page.

Comprehensive discovery of social networks like Facebook, MySpace, and Twitter is imperative in litigation in the 21st century. Social networks have taken hold in our culture, and they continue to grow. Over 400 million people maintain active Facebook accounts. <http://www.facebook.com/press/info.php?statistics>. They upload over 3 billion photos every month. *Id.* MySpace boasts 100 million active members. <http://www.myspace.com/pressroom?url=/fact+sheet/>. Twitter has over 6 million active members, <http://siteanalytics.compete.com/twitter.com/>, and will likely continue to grow as internet traffic on the site multiplies. *See id.* (noting that the number of monthly visitors to Twitter climbed from approximately 6 million people in January 2009 to approximately 23 million people in January 2010). Indeed, almost three-quarters of people active online in the United States are involved with social networking sites. *ComScore Media Metrix Ranks Top 50 U.S. Web Properties for April 2009*, comscore.com (May 14, 2009), available at http://www.comscore.com/Press_Events/Press_Releases/.

Defense lawyers should no longer ask if they need discovery of social networks. They should ask how to get it, how to get the most impact out of it, and how to get it admitted into evidence. Here is a recommended approach:

Obtaining social-network profiles without going through the formal discovery process can be an enormous advantage because defendants can surprise plaintiffs and witnesses with postings and/or pictures at deposition or trial. After learning about

a claim, go online immediately to see if the plaintiff or any other identifiable witness maintains a social-network profile that is publicly accessible. See, e.g., *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1130 (Ct. App. 2009) (finding that a posting on an unrestricted MySpace page "opened it to the public eye," and that plaintiff had no reasonable expectation of privacy.). If so, print or download the information immediately before plaintiff/witnesses have an opportunity to delete anything. Consider using an IT professional to make a copy of the web pages. Note, however, that access to social-network profiles depends on the security settings that the plaintiff/witnesses selected, and fewer people maintain purely public profiles than in the past, a trend that will likely continue in the future.

Routine checks of the profiles should be performed to stay abreast of new posts, and new searches should be conducted immediately upon learning of any new witnesses. Copies of everything will not only provide defendants with deposition exhibits, but they will also lay the groundwork for admissibility of the material at trial.

Because anyone can open social network accounts under pseudonyms or the names of other people, establishing that a witness' social network account is, in fact, the witness' account is a precondition to admissibility that courts will scrutinize closely. *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 543 (D. Md. 2007) (noting that courts are examining foundational requirements more carefully for electronically stored information than hard-copy material); *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773 (S.D. Tex. 1999) (noting that "the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time."). Authentication of the account requires sufficient evidence for a reasonable jury to find that the exhibit is what the proponent claims. Fed. R. Evid. 901 (a); *Lorraine*, 241 F.R.D. at 542. Getting the witness to admit that the account at issue is his or her account is obviously preferable. If the witness will not authenticate the account, however, defendants should either serve requests for admission or obtain testimony or an affidavit from the person who copied the webpage about how and when the webpage was copied and that the copy of the webpage is accurate. See *Lorraine*, 241 F.R.D. at 555-56.

If plaintiff's/witnesses' social network profiles are not publicly available, one approach to consider is service of a subpoena on the social network site. Currently, this approach is not likely to lead to production of actual profile content because social networks will oppose subpoenas that call for production of private information as a violation of the Stored Wire and Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et seq.*, (ECPA). The ECPA provides that electronic communication services may not disclose the contents of its subscribers' communications absent several narrowly defined exceptions, none of which includes civil litigation. *Id.* § 2702(b). Note that the ECPA was passed in 1986, and congressional hearings have recently been held to consider how to update the Act to address the technological advances of the past twenty-five years. As the ECPA currently stands, however, the electronic communication services may produce "customer records" to civil litigants, which

excludes the content of their profiles, such as postings and pictures. *Id.* § 2702(c). The most information that defendants can expect in response to a subpoena is basic subscriber information and IP logs for a user's account, which are helpful to establish when the plaintiff/witnesses posted specific content on the social-network account. See *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 545-49, 555-57 (D. Md. 2007) (discussing proof of authorship by admission, stipulation, testimony of a witness who observed the entry of the posting, or by connecting the plaintiff/witnesses to the postings either directly or circumstantially). While defense counsel is not likely to obtain substantive content because of the ECPA, subpoenas to the social networks should create preservation obligations, which will reduce the risk of spoliation when defendants request the contents of the account through formal discovery to the plaintiff/witnesses.

Requests for production to the plaintiff and/or subpoenas directed to third-party witnesses will yield more substantive content than subpoenas to the social network sites. Moreover, requiring that the witness produce the social-network material in response to document requests or a subpoena will facilitate authentication of the material for admissibility purposes. See, e.g., *Perfect 10 v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (presuming that a party's production of print-offs from its website were authentic); *Indianapolis Minority Contractors Ass'n.*, 94-1175-C-T/G, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998). Defendants also should remind plaintiff/witnesses that they must preserve their online content in the event that their preservation subpoenas on the social networks are ineffective.

In addition to the actual content of the plaintiff's/witnesses' social-network profile, defendants should also consider formal discovery seeking plaintiff's/witnesses' IP addresses, which, together with the IP logs that the social networks should produce, will help establish authorship of material posted to the network. Defendants should consider conducting a forensic examination of the plaintiff's/witnesses' web cache files, which may reveal evidence of plaintiff's/witnesses' social-network activity. Discovery should aim to prove authorship of the social-network material by the witness' admission, stipulation, testimony of a witness who observed the entry of the posting, or by connecting the witness to the postings either directly or circumstantially. See *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 545-49, 555-57 (D. Md. 2007).

Defendants will likely face objections, however, as to the scope of the requests for social-network material, as well as objections on privacy grounds. Objections as to scope will not generally be sustained if the requests are narrowly tailored. See, e.g., *Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc.*, No. 06-788, 2007 U.S. Dist. LEXIS 2379, at **25-26 (D. Nev. Jan. 9, 2007) (noting that, in a s*xual-harassment lawsuit, requests to produce MySpace private messages containing information regarding s*xual harassment and emotional distress allegations would be sufficiently tailored). Defendants can overcome privacy objections by agreeing that all private information will be produced subject to a protective order. Moreover, courts generally have not been persuaded by privacy arguments when

information has been shared on social networks, regardless of the privacy settings that the person selected for his or her account. See, e.g., *Ledbetter v. Wal-Mart Stores, Inc.*, 06-cv-01958, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (finding that the stipulated protective order sufficiently protected plaintiffs' privacy interests in their Facebook, MySpace, and Meetup accounts); *Mackelprang*, 2007 U.S. Dist. LEXIS 2379, at **25-26 (overruling privacy objection and finding that defendant was entitled to discover the private MySpace messages if the categories of documents requested were appropriately tailored to comport with Rule 34).

Moreover, people participating on social network websites agree to the privacy policies of the networks, all of which include provisions that the information posted may be disclosed to third parties. The average social network user also has a diminished expectation of privacy (the average Facebook user, for instance, has 130 friends and is a member of 13 networks, some of which include hundreds of thousands of people, <http://www.facebook.com/press/info.php?statistics>, such that even if a person has only a few friends and a few networks, potentially hundreds of thousands of people or more can view the account). Despite the tendency of courts to allow discovery of private, social-network information upon properly tailored discovery requests, the law is not settled.

Although there is little guidance from case law or ethics opinions addressing discovery of social networks, a few additional considerations for defense counsel are:

- If social-network profiles are private, accessing them can risk invasion-of-privacy lawsuits. See *Pietrylo v. Hillstone Restaurant Group*, 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 25, 2008) (finding that a jury question was created as to whether an employer accessing an employee's private MySpace page constituted an invasion of privacy).
- Attempting to "friend" a plaintiff/witness or hiring a private investigator for this purpose may violate various state ethics rules, including Rule 4.2 (Communication with Person Represented by Counsel), 4.3 (Dealing with Unrepresented Person), Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants), 8.4 (Misconduct), and potentially 4.1 (Truthfulness in Statements to Others) and 5.1 (Responsibilities of Partners, Managers and Supervisory Lawyers). See The Philadelphia Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (Mar. 2009).

The dearth of case law and ethics opinions regarding social networks leaves many questions unanswered. May defense counsel change the location settings on his or her own account to view the witnesses' otherwise-private pages if the witnesses are part of local networks (for example, a city network)? May defense counsel hire local counsel to join the witnesses' local networks? Finally, may defense counsel view the public pages of the witnesses' friend, and link into the witnesses' otherwise private pages (depending on the witnesses' privacy settings)?

Because of these unanswered questions, the risk of invasion-of-

privacy suits, and potentially running afoul of state ethics rules, defense counsel should exercise caution when searching for information on social networks, particularly if the information is not readily publicly available.

Conclusion

Information from social networks can be invaluable to civil defendants, and the ubiquity of social networks requires that they be routinely explored during discovery. Although the law surrounding the discoverability of social networks is still developing, defendants can discover this material, use it effectively, and get it admitted into evidence if they develop a strategy early in the litigation and execute on it.

Stephen M. Brooks (stephen.brooks@nelsonmullins.com)

Matthew E. Brown (matt.brown@nelsonmullins.com)

Nelson Mullins Riley & Scarborough, LLP

Atlanta, Georgia

Published by DRI

Powered by IMN™