Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
April 2010 Issue

By Iris Weinmann

DON'T invade MySpace

Responding to employers' attempts to discover information from social network sites

A stadium operations worker who criticized his employer via a post on his personal Facebook page was terminated days later. (*ESPN.com News Services* (March 9, 2009).) An insurance company cut off benefits to a woman on sick leave for depression after her agent found pictures of her on Facebook showing her on vacation, at a bar and at a party. (*PCmag.com* (November 24, 2009).) A police officer in Georgia alleges that he was terminated for posting information about his job on Facebook. (*MyFoxAtlanta.com* (December 10, 2009).)

The Internet is replete with examples of employees whose jobs or benefits have been affected because of a posting seen by their employers on social network sites. The proliferation of social network sites presents new challenges as employers find new ways to monitor their employees and investigate applicants for employment. These sites also provide a whole new area of interest to defendants in wrongful termination and other employment lawsuits. Increasingly, employers are demanding copies of postings in requests for production and are attempting to subpoena information about plaintiff-employees from social network sites. How much information is a former employer entitled to? What can be done by plaintiffs' counsel to minimize the invasions to their clients' privacy? This article seeks to assist plaintiff's counsel in addressing these questions.

What is a social network site?

Social network sites are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections

See Weinmann, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
April 2010 Issue

may vary from site to site." (Boyd, D. M., & Ellison, N. B. *Social network sites: Definition, history, and scholarship* (2007) Journal of Computer-Mediated Communication, 13(1), article 11.)

Some of the more popular social network sites include Facebook, MySpace, LinkedIn and Twitter. It is likely that most potential clients who walk through the employment practitioner's door seeking legal representation have had some activity on social network sites. It is important to recognize this immediately, as part of normal case intake and be prepared to deal with its implications to the lawsuit.

Before the lawsuit

When first interviewing a potential client, the attorney must ask whether the client has participated in social network sites, and explain that, even where the client believes his or her posts were completely private, they may not remain so once litigation starts. Depending on the type of lawsuit contemplated, questions to ask might be whether the employee posted comments about his or her employer on the site, either positive or negative; whether the employee participated on such sites during working hours; and whether there are photos of the employee that might harm a sexual harassment case or negate claims of severe depression following termination. There are a whole host of issues that could arise. Ideally, the attorney should access and view the client's entire site as part of the initial intake or shortly thereafter in order to assess what potentially damaging evidence may exist.

Counsel should also consider advising clients to shut down their social network sites altogether during the pendency of the lawsuit. As careful as the plaintiff might be about what he or she says or posts, others on the network may nevertheless make harmful comments or tag the plaintiff in photos which could prove damaging. A posting intended as a joke could be interpreted in different ways. The level of risk may vary, depending on the type of lawsuit. There will be different implications in a suit merely alleging overtime violations than in a suit alleging sexual harassment by a supervisor. This may be a tough sell to some clients, who may view their social network activities as a way to try to find new employment or who simply rely on these networks for social support. In such cases, counsel should consider providing the client with a written disclosure advising that social network activity be ceased during the pendency of the lawsuit, and advising of the risks of continuing to maintain such networks.

Can employer subpoena the plaintiff's records from social network sites?

The employer may try to subpoena the plaintiff's records from social network sites, claiming that postings made by the employee related to his or employment, the amount of time spent by the employee on such sites during working hours, and postings that may relate to the level of the plaintiff's alleged distress are relevant. Further, in sexual harassment cases, the defendant may argue that photos of the plaintiff may impact the plaintiff's claim that the plaintiff was subjectively offended by the harasser's conduct. (*Fisher v. San Pedro Peninsula Hospital* (1989) 214 Cal.App.3d 590, 609-610 [262 Cal.Rptr. 842]; *Beyda v. City of Los Angeles* (1998) 65 Cal.App.4th 511, 517 [76 Cal.Rptr.2d 547].)

The defense to this type of request is twofold. First, messages or postings that the plaintiff may have sent to friends on a social network site and messages posted by others to or about the plaintiff are statutorily protected from disclosure by the Stored Communications Act, 18 U.S.C. section 2701, a chapter contained in the Electronic Communications Privacy Act, 18 U.S.C. section 2510, et seq. Second, such a subpoena is invasive of plaintiff's rights to privacy, as well as the right to privacy of individuals with whom the plaintiff may have communicated on such sites.

Protection of communications posted on a social network

Messages or postings that the plaintiff may have sent to friends on a social network site and messages posted by others to or about the plaintiff are governed by the Stored Communications Act, 18 U.S.C. section 2701, a chapter contained in the Electronic Communications Privacy Act, 18 U.S.C. section 2510, et seq.

The Stored Communications Act "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." (*Theofel v. Farey-Jones* (9th Cir. 2003) 341 F.3d 978, 982.) The statute "protects individuals' privacy" and "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." (*Id.* at p. 982.) The Stored Communications Act provides that "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…" (18 U.S.C. § 2702(a)(1).)

Since the plaintiff in an employment lawsuit is a person, and the social network sites provide an electronic communication service to the public, the provisions of the Stored Communications Act are applicable to civil subpoenas issued by defendant employers seeking the contents of communications stored by the social network sites.

Contents of communications stored by an electronic communication service may not be compelled, *even by a civil subpoena*. (*O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, 1447 [44 Cal.Rptr.3d 72].) In *O'Grady*, Apple Computer issued a civil subpoena to publishers of a Web site on which alleged trade secret information was posted, in an attempt to determine who had misappropriated and revealed the trade secret information. Apple argued that even though the Stored Communications Act specifically prohibits an electronic service provider from divulging the contents of a communication while in storage by the service, there were exceptions to the general rule. The court examined each of

See Weinmann, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
April 2010 Issue

the Stored Communication Act's exceptions, and found none for civil discovery subpoenas. (*Id.* at p. 1443.) The court refused to recognize "an implicit exception for civil discovery subpoenas," concluding that if Congress had intended to include an exception for civil discovery subpoenas, it would have done so. (*Id.* at p. 1443-1444.) The *O'Grady* court concluded that enforcement of a civil subpoena issued to an electronic communications facility is inconsistent with the plain terms of the Stored Communications Act. (*Ibid.*)

Other courts facing this issue have come to the same conclusion. (See *Federal Trade Comm'n v. Netscape Communications Corp.* (N.D. Cal. 2000) 196 F.R.D. 559, 561 ["There is no reason for the court to believe that Congress could not have specifically included discovery subpoenas in the statute [as an exception to the rule of nondisclosure] had it meant to"]; *In re Subpoena Duces Tecum to AOL, LLC* (E.D. Va. 2008) 550 F. Supp. 2d 606, 611 ["Agreeing with the reasoning in *O'Grady*, the court holds that State Farm's subpoena may not be enforced consistent with the plain language of the Privacy Act because the exceptions enumerated in § 2702(b) do not include civil discovery subpoenas"].)

Thus, subpoenas seeking the contents of communications posted by a plaintiff on social network sites are not enforceable.

However, not all information is protected from disclosure by the Stored Communications Act. An electronic communication service "may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))…to any person other than a governmental entity." (18 U.S.C. § 2702(c)(6).) Thus, if the employer seeks IP log-in information or subscriber information, that would not be prohibited by the Stored Communications Act, although it would still be subject to the privacy and relevance considerations discussed in the next section.

Records from social network sites are protected by the right to privacy

A very broad subpoena would potentially encompass credit card records, passwords, log-in information, and other personal identifying information, which are protected by the right to privacy. Requests for postings made by or about the plaintiff are invasive of not only the plaintiff's right to privacy, but the right to privacy of every individual with whom the plaintiff may have corresponded over Internet sites or who may have posted a message to or about the plaintiff, at least with respect to sites in which the plaintiff has limited his or her communications to "friends" in the network, rather than to the general public.

Article I, section 1 of the California Constitution guarantees all individuals a right to privacy:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, *and pursuing and obtaining* safety, happiness, and *privacy*.

(Cal.Const., art. I, §1 (emphasis added).) The privacy clause of article I, section 1 of the California Constitution protects against invasions of privacy by private citizens, as well as the state. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 20 [26 Cal.Rptr.2d 834]; *Jeffrey H. v. Imai, Tadlock & Keeney* (2000) 85 Cal.App.4th 345, 353 [101 Cal.Rptr.2d 916].)

That there is a privacy interest in information maintained on social network sites is confirmed by the Electronic Communications Privacy Act, of which the Stored Communications Act is a part. (18 U.S.C. § 2510, et seq; See *Theofel v. Farey-Jones*, *supra,* 341 F.3d at 982.) Because such documents are within the zone of privacy, the defendant has a high burden to meet before being able to compel their production.

Where a party seeks to discover documents subject to the constitutional right to privacy, that party bears the burden of establishing a *compelling need* for the discovery. (*Davis v. Superior Court* (1992) 7 Cal.App.4th 1008, 1014 [9 Cal.Rptr.2d 331]; *Lantz v. Superior Court* (1994) 28 Cal.App.4th 1839, 1853 [34 Cal.Rptr.2d 358].) This burden is significant and not easily overcome. To meet this burden, the party seeking discovery must first establish that each of the records sought is *directly relevant to the action* and *essential to its fair resolution.* (*Lantz, supra,* 28 Cal.App.4th at 1854; See also, *Britt v. Superior Court* (1978) 20 Cal.3d 844, 859 [143 Cal.Rptr. 695].)

The employer may set forth several arguments supporting its attempts to discover the content of an individual's social network site. For example, the employer may assert that any comments made by the employee about the employer are reasonably calculated to lead to the discovery of relevant or admissible evidence. Without a specific showing that something about the employer was, in fact, posted and its link to the issues in the lawsuit, this should be insufficient to establish *direct relevance.* The normal standard for discovery set forth in Code of Civil Procedure section 2017.010 – i.e., that the information sought need only be reasonably calculated to lead to the discovery of relevant or admissible evidence – is inapplicable to discovery of items protected by a constitutional right to privacy. Rather, in such cases, the items sought must be *directly relevant*. (*Britt, supra,* 20 Cal.3d at 859; *Tylo v. Superior Court* (1997) 55 Cal.App.4th 1379, 1387 [64 Cal.Rptr.2d 731].)

Likewise, the employer may argue in a sexual harassment case that racy photos of the employee may be relevant to help establish that the employee was not offended by an alleged harasser's conduct. (See *Fisher, supra,* 214 Cal.App.3d at 609-610; *Beyda, supra,* 65 Cal.App.4th at 517 [one of the elements of a hostile environment claim is that the employee was actually offended by the allegedly harassing conduct].) Again, without some information about a specific photo or incident, the employer is simply engaging in a fishing expedition, which is

See Weinmann, Next Page

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
April 2010 Issue

improper where the constitutional right to privacy is implicated. Mere speculation as to the possibility that some portion of the records *might* be relevant to some substantive issues does not suffice. (*Davis, supra,* 7 Cal.App.4th at page 1017; *Mendez v. Superior Court* (1988) 206 Cal.App.3d 557, 570-571 [253 Cal.Rptr. 731] [mere conjecture about what might be found is an insufficient basis for discovery of matters protected by the constitutional right to privacy]; *Huelter v. Superior Court* (1978) 87 Cal.App.3d 544, 549 [151 Cal.Rptr.138] ["mere speculation…does not justify the discovery of privileged matter"].)

Recognizing that the Stored Communications Act prohibits employers from subpoenaing the content of an individual's social network activity, the employer may try to limit its subpoena to seek the plaintiff's log-in information to determine whether the plaintiff was accessing such sites during working hours. Absent a claim that the plaintiff was terminated for accessing social network sites during working hours, this also constitutes an improper fishing expedition, which is not permitted when the constitutional right to privacy is at issue.

It is impossible to list here every possible argument that an employer may assert to try to obtain access to a plaintiff's social network activities. Plaintiff's counsel should analyze each argument raised by the employer to determine whether the employer is seeking information that is directly relevant and essential to a just resolution of the lawsuit, or is simply engaging in a fishing expedition.

Even if in a particular case an employer can establish direct relevance and essentiality of messages posted on social network sites, the court must still carefully balance the need for production against the fundamental right to privacy. (*Lantz, supra,* 28 Cal.App.4th at 1854.) Moreover, any intrusion on the right to privacy "should be the minimum intrusion necessary to achieve its objective." (*Id.* at p. 1855.) Thus, the employer should not be permitted to view every discussion between the plaintiff and every person with whom the plaintiff has communicated via online social networks. Rather, any request must be very narrowly tailored to only encompass information directly relevant to the lawsuit, and perhaps redacting the names of third parties with whom communications took place.

The foregoing discussion about privacy rights assumes that the plaintiff has a reasonable expectation of privacy in his or her social network activities. Some sites allow an individual to limit the persons who can access the plaintiff's communications to "friends" identified by the plaintiff. To the extent the plaintiff is using a site which has no built-in privacy protections and is open to view by the general public, it may be harder to convince a court that the privacy protections discussed above apply. In fact, in such cases, the employer may be able to access the information directly, without having to employ any discovery tool.

The employer may demand production of postings on social network sites directly to plaintiff

When the employer does not subpoena the third-party providers, such as Facebook or MySpace, but instead issues a request for production of documents directly to the plaintiff seeking the plaintiff's postings from social network sites, the Stored Communications Act does not apply. However, the same privacy arguments articulated above are applicable. The plaintiff should object to these requests on privacy grounds, and either file a motion for protective order or be prepared to oppose a motion to compel.

Conclusion

The mode in which individuals communicate information about themselves has changed rapidly over the past decade, and the law has not necessarily kept up with the changes. Until more legal precedent has been established by the courts, counsel must rely on analogous cases dealing with privacy and emphasize to the courts the implications these types of broad requests by defendant-employers will have. However, regardless of how the courts rule, the safest bet is to always assume the employer can see everything posted on these sites and be prepared to deal with any damaging or improper information via motion in limine or at trial before the jury.

Iris Weinmann is a partner in Greenberg & Weinmann, *located in Santa Monica. Ms. Weinmann has concentrated her practice on the representation of employees in civil rights and other employment related litigation since 1994. Together with her partner, Paul Greenberg, she has successfully tried multiple employment cases to verdict. She has also argued several appeals before the Court of Appeal for the State of California. Ms. Weinmann is a frequent contributor to the* Advocate*'s annual Employment Law issue.*