MILLER CANFIELD

Social Media and Discovery: New Technology, but the Old Rules Still Apply

September 2012

This article was previously published in Laches (Aug. 2011) and was reprinted in the State Bar of Michigan, Labor and Employment Lawnotes, Winter 2012.

1. SOCIAL MEDIA INFORMATION IS GENERALLY DISCOVERABLE

Social media has dramatically changed how humans interact with each other and the digital footprint left by individuals on sites like Facebook, Twitter, LinkedIn, and YouTube must not be discounted when formulating discovery plans. Rather, attorneys must embrace social media as part of the "new normal." Discovery through the lens of social media should not be viewed as new and unfamiliar territory. Posts on social media are just additional ways for individuals to document their lives like diaries, letters, photo albums, or emails. An individual's posts may document things that are seemingly innocuous at the time but could literally make or break a case later. Consider how valuable a time-stamped post on Facebook documenting an individual's mood – including as expressed in pictures – may be to either buttressing or undermining that individual's claim for emotional distress damages.[1] Attorneys would be remiss to not at least probe to see whether an individual's social media site contains discoverable material or confirm that broad discovery requests – like those seeking all communications about the individual's claims – include communications via social media. Such discovery is exactly the type of discovery contemplated by Rule 2.302 of the Michigan Court Rules and Rule 34 of the Federal Rules of Civil Procedure, both of which expressly include "electronically stored information" in the scope of permissible discovery.[2]

A. Content Must be Relevant

Whereas courts[3] and attorneys[4] are just now grappling with social media, it is clear that courts are applying traditional discovery rules to social media content. One of the leading cases in this developing area of the law is *EEOC v. Simply Storage Management LLC*.[5] In *Simply Storage*, the EEOC filed a sexual harassment complaint against the employer and the employer's attorneys served document requests seeking the content of the complaining employees' social networking sites to obtain information about the employees' emotional health. They requested:

Request No. 1: All photographs or videos posted by [employee] or anyone on her behalf on Facebook or MySpace from April 23, 2007 to the present

Request No. 2: Electronic copies of [employee]'s complete profile on Facebook and MySpace (including all updates, changes, or modifications to [employee]'s profile) and all status updates, messages, wall comments, causes joined, activity streams, blog entries, details, blurbs, comments, and applications . . . .

The EEOC objected, and upon the employer's motion to compel, the court rejected the idea that discovery of social media or other electronically stored information is unique. "Rather," the court stated, "the challenge is to define appropriately broad limits – but limits nevertheless – on the discoverability of social communications in light of a subject as amorphous as emotional and mental health . . . ."[6] The court detailed some general guiding principles before discussing the specific requests at issue.

Continued

First, the court rejected the argument that since the social media profiles were "locked" or "private," they were not discoverable due to privacy concerns as such concerns could be "addressed by an appropriate protective order . . . ."[7] Additionally, privacy arguments by those attempting to prevent the discoverability of social media are undermined "by the fact that the production . . . would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through postings."[8] The very purpose of social media undercuts such an argument: "Facebook is not used as a means by which account holders carry on monologues with themselves."[9]

Second, the court emphasized that the material requested must be relevant to a claim or defense in the case. The employer had requested access to the employees' entire Facebook and MySpace accounts, but according to the court did not show why such broad access was relevant to the employees' claims for emotional damages. "[T]he simple fact that a claimant has *had* social communications is not necessarily probative of the particular mental and emotional health matters at issue in this case."[10]

Third, when an employee makes claims for emotional damages, "[i]t is reasonable to expect severe emotional or mental injury to manifest itself in some [social media] content, and an examination of that content might reveal whether onset occurred, when, and the degree of distress. Further, information that evidences other stressors that could have produced the alleged emotional distress is also relevant."[11] The discoverability of social media information should be broader, according to the court, than just "communications that directly reference the matters alleged in the complaint" as argued by EEOC.[12]

Turning to the case at hand, the court narrowed the employers' requests, while still allowing significant social media discovery:

[T]he court determines that the appropriate scope of relevance is any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and [social media] applications for [the employees] . . . 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.[13]

As for the employer's request for pictures on social media pages:

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.[14]

Such a holding provides the framework for litigators who seek to discover (or prevent the discovery of) social media information. "The court's determination of relevant material is crafted to capture all arguably relevant materials, in accord with the liberal discovery standard of Rule 26. In carrying out this Order, the EEOC should err in favor of production."[15]

Continued

Also applicable is the case of *Mackelprang v. Fidelity National Title Agency of Nevada, Inc.*[16] In *Mackelprang*, the plaintiff alleged sexual harassment and other claims against her employer. At issue was the employer's motion to compel private communications on plaintiff's MySpace page after subpoenas to MySpace resulted in the production of only public information. The employer claimed that such communications would show that the plaintiff "was a willing participant who condoned and actively encouraged the alleged sexual communications . . . and sexual conduct" at the basis of her claims. Rejecting this argument, the court found that the employer was "engaging in a fishing expedition since . . . it has nothing more than suspicion or speculation as to what information might be contained in the private messages."[17] It did so, relying upon Federal Rule of Evidence 412(a), because there was not "a sufficiently relevant connection between . . . plaintiff's non-work related sexual activity and the allegation that . . . she was subjected to unwelcome and offensive sexual advancements in the workplace."[18] Even if such evidence were relevant, the court continued, "its probative value as to either liability or damages is not substantial enough to outweigh the unfair prejudice that its admission would cause."[19]

The employer in *Mackelprang* also argued that plaintiff should produce all of her email communications via MySpace in order to review for plaintiff's admissions or for impeachment purposes. While the court rejected this argument on similar relevance and overbreadth concerns,[20] it did not preclude the employer from obtaining *some* of the private messages. Instead, it suggested that the employer "serve upon [p]laintiff properly limited requests for production of *relevant* email communications."[21] The court stressed that it was not preventing the employer from "serving such discovery requests on [p]laintiff to produce her Myspace.com private messages that contain information regarding her sexual harassment allegations . . . or which discuss her alleged emotional distress and the cause(s) thereof."[22]

In sum, the *Simply Storage* and *Mackelprang* decisions find a balance between producing *all* social media information and *no* social media information. Instead, they dictate that social media information is discoverable when adequately tailored to satisfy the relevance standard.[23]

B. <u>May a Social Media User Limit Discovery Based Upon a Privacy Objection?</u>

As noted in *Simply Storage*, it is difficult for an objecting party to successfully object to producing social media information on privacy grounds. Social media users affirmatively place information about themselves on sites to be shared with other users. A few recent state courts outside of Michigan have found individuals have no privacy protections even when individuals take affirmative steps to limit who can view their social media sites. *Romano v. Steelcase Inc*, for example, is a personal injury case with the plaintiff claiming "permanent injuries" resulting from the defendant's conduct.[24] After portions of the plaintiff's publicly available social media site revealed plaintiff still maintained an active lifestyle and traveled during the relevant time period, the defendant served discovery requests accordingly. The court rejected the plaintiff's argument that the defendant's attempt to secure access to the "non-public" portions of her site, stating "[t]o deny [d]efendant an opportunity [to] access . . . these sites not only would go against the liberal discovery policies of New York favoring pre-trial disclosure, but would condone [p]laintiff's attempt to hide relevant information behind self-regulated privacy settings."[25] Further, the very fact that the social media sites at issue – Facebook and MySpace – remind users that postings are not private when plaintiff signed up are evidence that "she consented to the fact that her personal information would be shared with others, *not withstanding her privacy settings.*"[26] Even assuming plaintiff had a privacy interest in her "non-public" site, the court concluded that such an interest was outweighed by the defendant's need for the information.[27]

A similar holding occurred in *McMillen v. Hummingbird Speedway Inc.*, another personal injury case with the defendants seeking information to disprove plaintiff's injuries.[28] In *McMillen*, the defendants sought and successfully obtained plaintiff's login and password information. The court specifically relied upon the terms of use for Facebook and MySpace to dismiss plaintiff's privacy objections: "[R]eading their terms and privacy policies should dispel any notion that information one chooses to share, even if only with one friend, will not be disclosed to anybody else." This is because both sites reserve the right to collect and disclose information. Regardless of the steps users take to limit the information flow on social media sites, "their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion." The court then ordered plaintiff to provide his login and password information to the defendants for their review.[29]

2 SUBPOENAS TO SOCIAL MEDIA SITES LIKELY WILL NOT WORK

In addition to seeking discovery from party participants, may a party seek to enforce third party subpoenas to social media sites? Facebook, for instance, will not disclose "user content (such as messages, Wall posts, photos, etc.) in response to a civil subpoena."[30] Instead, it will only provide "basic subscriber information . . . 'where: 1) the requested information is indispensable to the case and not within the party's possession; and 2) you personally serve a valid California or federal subpoena on Facebook. Out-of-state civil subpoenas must be domesticated in California and personally served on Facebook's registered agent."'[31]

A recent decision from a California federal court supports Facebook's policy that subpoenas to social media sites are generally not enforceable to the extent they seek private user content. In *Crispin v. Christian Audigier, Inc*, an artist sued several licensees and the defendants subpoenaed several social media sites seeking plaintiff's "basic subscriber information" as well as a communications, in part, about the defendants.[32] The plaintiff filed a motion to quash arguing, in part, that the Stored Communications Act ("SCA") [33] prohibited such disclosure. Generally, the SCA prohibits the disclosure of "private communications to certain entities and individuals." The court quashed the subpoenas on SCA grounds.

Crispin has several significant holdings. First, the plaintiff had standing to quash the subpoenas.[34] The court reasoned that "an individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and bank records."[35] Second, the court found that the social media providers at issue – including Facebook and MySpace – constituted electronic communication service ("ECS") providers under the SCA.[36] Under the SCA, ECS providers are prohibited from disclosing information contained in "electronic storage."[37]

Most significantly, the court determined that the information sought by the defendants was "electronic storage" and thus quashed the subpoenas to the extent that they sought "private messaging" not readily accessible to the public.[38]

While *Crispin* is likely not the last word on whether the SCA prohibits subpoenas directed at third-party providers like Facebook and MySpace,[39] its lesson appears to be that parties should alternatively craft appropriate discovery requests within the parameters discussed in the prior section.[40] Indeed, Facebook suggests as much:

Parties to civil litigation may satisfy discovery requirements relating to their Facebook accounts by producing and authenticating contents of their accounts and by using Facebook's "Download Your Information" tool, which is accessible through the "Account Settings" drop down menu.

If a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request.[41]

3. DUTY TO PRESERVE

There is currently no published court decision discussing the duty to preserve evidence maintained on social media sites.[42] Given the possible relevance of material contained within social media websites and an individual user's ability to control information on social media – including altering, restricting, or deleting information[43] – this area is likely to be confronted by the courts in short order. That said, it appears logical and fairly straightforward that a party has an affirmative duty to maintain data stored on social media given recent e-discovery decisions.[44] At the very least, employers have an obligation to maintain documentation about the process and information obtained in making employment decisions and this would presumably include, for example, solicitations for and applications received via social media.

4. CONCLUSION

One of the unique aspects of social media posts is its potential permanence, given that it can be stored indefinitely somewhere on the Internet, regardless of the initial site on which it was posted and the user's intent. Take for example the well-publicized "tweet" that was sent from Chrysler's official Twitter account by an employee of a social media agency: "I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to (expletive) drive." Chrysler deleted the tweet almost immediately, but it remains forever available on the Internet as it was re-tweeted several times before being deleted.

Regardless of whether one is propounding or receiving discovery requests, such permanence, combined with the exponential growth of social media across all demographics, makes discovery of social media information inevitable. While courts have provided limited guidance so far, all indications are that courts do not view social media discovery any differently than traditional discovery. At the end of the day, information contained on social media sites is likely discoverable assuming it passes the relevancy threshold.

Adam S. Forman
313.496.7654

David G. King
313.496.7585

---

[1] *Cf. Zimmerman v Weis Markets,* No. CV-09-1535 (Pa Ct Com Pl May 19, 2011) (ordering Plaintiff to provide "passwords, user names and log in names for any and all MySpace and Facebook accounts to Defendant" where pictures on Plaintiff's publicly available MySpace and Facebook pages contradicted his deposition testimony); *BM v DM*, No. 50333/2007, 2011 WL 1420917, at *5 (NY Sup Ct April 7, 2007) (postings made by wife in a divorce action reflecting her belly dancing activities "contradict[ed] her claims that she is unable to work due to injuries sustained in the Accident, rarely leaves home, and socializes only once per month").

Continued

[2] MCR 2.302 and Fed R Civ P 34.

[3] One example of how courts are struggling with social media is the case of *Barnes v CUS Nashville, LLC*. No. 3:09-cv-00764, 2010 WL 2265668 (MD Tenn June 3, 2010). There the magistrate judge offered to expedite the discovery dispute by creating a Facebook account and then "friending" two individuals "for the sole purpose of reviewing photographs and related comments *in camera* . . . ." *Id.* at *1. He then would "properly review and disseminate any relevant information to the parties . . . [and would] then close this Facebook account." *Id. See also Offenback v LM Bowman, Inc.*, No. 1:10-CV-1789, 2011 WL 2491371 (MD Pa June 22, 2011) (similar); *Anderson v. MG Trucking, Inc*, 11-000165-NI (Mich App Dec. 14, 2011) (vacating the lower court's order that plaintiff's social media information was irrelevant and remanding to allow trial court to further consider the issue as the record was unclear as to why the lower court denied access to plaintiff's records and instructing the court to "list the information provided by plaintiff in general terms such as those described in *Offenback v. LM Bowman, Inc.*").

[4] *See Piccolo v Paterson*, No. 2009-04979 (Pa Ct Com Pl May 5, 2011) (denying defendant's motion to compel plaintiff to accept a "neutral friend request" from defense counsel in order to review the Facebook postings she testified about during her deposition).

[5] 270 FRD 430 (SD Ind 2010).

[6] *Id.* at 434.

[7] *Id.*

[8] *Id.* at 437.

[9] *Id.* (citations omitted).

[10] *Id.* at 435.

[11] *Id.*

[12] *Id.* at 435-36.

[13] *Id.* at 436.

[14] *Id.*

[15] *Id.*

[16] No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149 (D Nev Jan 9, 2007).

[17] *Id.* at *2.

[18] *Id.* at *6.

[19] *Id.*

[20] *Id.* at *6-7.

[21] *Id.* at *8.

[22] *Id.*

[23] *See also Held v Ferrellgas, Inc*, No. 10-2393-EFM, 2011 WL 3896513 (D Kan Aug 31, 2011) (granting employer's motion to compel information from Plaintiff's Facebook page in employment discrimination case, stating "Defendant is attempting to mitigate Plaintiff's privacy concerns by allowing Plaintiff to download and produce the information himself, rather than providing login information. Indeed, Defendant itself notes that it is not seeking unfettered or unlimited access to Plaintiff's Facebook, but rather limited access during the relevant time frame"); *Debord v Mercy Health Sys of Kan*, No. 5:10-cv-04055-WEB-KMH (D Kan Aug 8, 2011) (employer's request for post-termination Facebook postings were not related to basis of employee's termination and thus not relevant); *Muniz v United Parcel Serv, Inc.*, No. C-09-01987-CW (DMR), 2011 WL 311374, at *9 (ND Cal Jan 28, 2011) (defendant's request for postings on social media sites by plaintiff's attorneys relating to "work" and "effort" for use in determining attorneys' fees was "not appropriately geared toward revealing information relevant to the fee dispute . . . ."); *Bass ex rel Bass v Miss Porter's Sch*, 3:08cv1807 (JBA), 2009 WL 3724968, at *1 (D Conn Oct 27, 2009) (employer's document request for information on Facebook related to plaintiff's complaint was relevant as it "depicts a snapshot of the user's relationship and state of mind at the time of the content's posting."); *Arcq v Fields*, No. 2008-2430 (Pa Ct Com Pl Dec 7, 2011) (denying defendant's motion to compel access to Plaintiff's social networking website profiles because defendant "has not alleged any basis for believing that Plaintiff's profiles contain any information relevant to the pending matter. . . . While it is not an absolute necessity that a plaintiff have a public profile before a defendant can be given access to the private portion, it is necessary that the defendant have *some* good faith belief that the private profile may contain information."); *Patterson v Turner Constr*, 88 AD3d 617 (NY App Div 2011) (remanding lower court's granting of motion to compel an authorization for all of plaintiff's Facebook records "for more specific identification of plaintiff's Facebook information that is relevant, in that it contradicts or conflicts with plaintiff's alleged restrictions, disabilities, and losses, and other claims"); *McCann v Harleysville Ins Co of New York*, 78 AD3d 1524 (NY App Div 2010) (denying defendant's motion to compel plaintiff to turn over "authorization for plaintiff's Facebook account information . . . [because] defendant essentially sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence"); *but see Gallion v Gallion*, FA114116955S (Conn Super Ct Sept. 30, 2011) (court ordered counsel in a divorce action dealing with custody issues to "exchange the password(s) of their clients' Facebook and dating website passwords" and that "[t]he parties themselves shall not be given the passwords of the other"); *Largent v Reed*, 2011 WL 5632688 (Pa Ct Com Pl Nov 8, 2011) (requiring plaintiff in personal injury action to turn over her Facebook login information to defense counsel finding that access to her Facebook account would not cause "unreasonable embarrassment" or "unreasonable annoyance" to plaintiff because "Facebook posts are not truly private and there is litte harm in disclosing that information in discovery.").

[24] 907 NYS2d 650, 653 (NY App Div 2010).

[25] *Id.* at 655. *See also Beye v Horizon Blue Cross Blue Shield of New Jersey*, No. 06-5337 (FSH), 2007 WL 7393489, at *2 n.3 (DNJ Dec 14, 2007) ("The Court will require production of entries on webpages such as 'MySpace' or 'Facebook' that the beneficiaries shared with others. The privacy concerns are far less where the beneficiary herself chose to disclose the information."); *Dexter v. Dexter*, 2007 WL 1532084, at *6 (Ohio Ct App May 25, 2007) (rejecting a claim of

privacy to MySpace postings where "appellant admitted in open court that she wrote these on-line blogs and that these writings were open to the public to view").

[26] *Romano*, 907 NYS2d at 657 (emphasis added).

[27] *Id.* An interesting side note to the court's order – the court granted access to plaintiff's *entire* Facebook and MySpace pages without engaging in the detailed relevance analysis conducted by the *Simply Storage* court. *Id.*

[28] No. 113-2010 CD (Pa Ct Com Pl Sept 9, 2010).

[29] *See also Zimmerman v. Weis Markets*, No. CV-09-1535 (Pa Ct Com Pl May 19, 2011) (ordering Plaintiff to provide "passwords, user names and log-in names for any and all MySpace and Facebook accounts to Defendant" where pictures on Plaintiff's publicly available MySpace and Facebook pages contradicted his deposition testimony); *Largent*, 2011 WL 5632688 ("There is no reasonable expectation of privacy in material posted of Facebook. Almost all information on Facebook is shared with third parties, and there is no reasonable privacy expectation in such information.").

[30] May I obtain contents of a user's account from Facebook using a civil subpoena?, http://www.facebook.com/help/?faq=17158 (last visited Jan 11, 2012).

[31] May I obtain any information about a user's account using a civil subpoena?, http://www.facebook.com/help/?faq=17159 (last visited Jan 11, 2012).

[32] 717 F Supp 2d 965, 968-69 (CD Cal 2010).

[33] *See* 18 USC 2701 *et seq.*

[34] *Id.* at 976. *See also Mancuso v Fla Metro Univ*, No. 09-61984-CIV, 2011 WL 310726, at *1-2 (SD Fla Jan 28, 2011) (plaintiff in FLSA action had standing to quash subpoena directed to social media sites, but refusing to do so on jurisdictional grounds).

[35] *Id.* at 974.

[36] *Id.* at 980. The court did so in large part by analogizing to private electronic bulletin board services due to the private messaging capabilities of the social media sites, including the ability to restrict access to only certain users.

[37] 18 U.S.C. § 2701(a).

[38] *Crispin*, 717 F Supp 2d at 987-88, 991. The court also found on alternative grounds that "Facebook and MySpace are RCS providers" for the purposes of "wall postings and comments" because individuals may limit accessibility to select users. *Id.* at 990.

[39] *See also O'Grady v Superior Court*, 139 Cal App 4th 1423, 1447 (2006) (third-party subpoenas require consent from owner of information, not the transmitter's or service provider's).

Continued

[40] *But see Ledbetter v Wal-Mart Stores, Inc*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *2 (D Colo April 21, 2009) (enforcing subpoena to Facebook, MySpace, and Meetup.com, without discussing the SCA); *Largent,* 2011 WL 5632688 (holding that the SCA did not apply to plaintiff because she was "not an entity regulated by the SCA" and thus the SCA did "not protect her Facebook profile from discovery.").

[41] May I obtain contents of a user's account from Facebook using a civil subpoena?, http://www.facebook.com/help/?faq=17158 (last visited Jan 11, 2012).

[42] Part of the Order in *Zimmerman v. Weis Markets, Inc*, *supra*, stated that "Plaintiff shall not take steps to delete or alter existing information and posts of his MySpace or Facebook accounts." No. CV-09-1535.

[43] Consider the recent spoliation case from a Virginia state court. In *Lester v Allied Concrete Company*, the plaintiff brought a wrongful death case against his wife's former employer. Case Nos. CL08-150, CL09-223 (Va Cir Ct). Defendants sought discovery regarding plaintiff's Facebook page upon discovering a picture of the allegedly distressed widower holding a beer can while wearing a t-shirt emblazoned with "I hot moms." Plaintiff's attorney then instructed plaintiff through his paralegal to "clean up" his Facebook and MySpace pages prior to responding to defendant's discovery requests because "we don't want blowups of this stuff at trial" and plaintiff deleted sixteen pictures from his Facebook page. He also, at his attorney's request, deactivated his Facebook page. After trial, the court sanctioned plaintiff and his attorney for this spoliation, requiring them to pay a total of $722,000 in fees. *See also Patel v. Havana Bar, Rest and Catering*, 2011 WL 6029983 (ED Pa Dec 5, 2011) (allowing an adverse inference instruction, the redeposition of several witnesses at plaintiff's cost, and awarding attorneys fees and costs where plaintiff failed to produce witness statements made on Facebook).

[44] *See, eg, Zubulake v UBS Warburg LLC*, 220 FRD 212, 217-18 (SDNY 2003) ("Zubulake IV").