The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 2 February 2011

Civil Justice Reform – Law Firms

E-Discovery Takes A Turn – Charting The Course To Discovery From Social Networks

Loryn P. Riggiola and Grace A. Brown

SILLS CUMMIS & GROSS P.C.

For many Americans, social networking is their primary source of connection and communication. Statistics confirm that as social networking increases, the use of individual email dramatically declines.[1] In order to conduct comprehensive discovery, information transmitted through social networking providers ("SNPs") must be uncovered. Whether the case involves a commercial dispute or a product defect – postings, pictures and messages transmitted through SNPs can be a valuable source of discovery.

According to its own statistics, Facebook alone has over 500 million users[2]. Coupled with each of the top 15 social networking sites, including MySpace, Friendster, Bebo, Twitter, and LinkedIn, the number of social networking users is estimated to exceed 880 million.[3] Not just for entertainment, many Fortune 500 companies have Facebook and Twitter profiles, including Walmart and ExxonMobil.[4] Companies are using social media[5] to secure data about people's preferences and to track consumer trends.[6] In responding to this growing trend,[7] litigators are also including discovery from SNPs as a part of their discovery protocol.[8]

Although the information transmitted through SNPs can be helpful, securing this information can be challenging. With a little tenacity, however, the skillful litigator can navigate the discovery hurdles and achieve production of all available electronically stored information ("ESI") directly from the SNP.

Procedures And Applicable Discovery Rules To Secure ESI From SNPs And Users[9]

Initially, the party seeking information should serve written discovery upon the SNP user demanding disclosure of: (1) the social networks subscribed to by the user, (2) the duration of each subscription, (3) all information and documents responsive to the discovery demands, and (4) applicable usernames and passwords.[10] Because information on social networks can be easily altered, deleted and may not be properly preserved by the user, complete discovery requires production from both the user and the SNPs.

a. New York, New Jersey and Federal Discovery Rules For ESI

Generally, under both New Jersey and the Federal Rules of Civil Procedure, a party can "obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense," or that is "reasonably calculated to lead to the discovery of admissible evidence."[11] Similarly in New York, "[t]here shall be full disclosure of all matter material and necessary in the prosecution or defense of an action."[12] Both the New Jersey and Federal Rules specifically include ESI.[13] New York recently followed suit by amending its rules (the "CPLR") to address ESI and require its disclosure.[14] Notably preservation of ESI is required, but the ESI available for production on the user's site can change with the click of a mouse. Therefore, the best procedure to ensure disclosure of all responsive ESI is to seek that information from both the user and the SNPs.

b. California Procedure for Obtaining Subpoena For Out-of-State Action

To secure disclosure from third-party SNPs, the litigator will need to obtain a subpoena from a California court. Although they are based in different venues, all SNPs are essentially based in California. The California Code of Civil Procedure was recently amended to simplify the process of obtaining a subpoena issued in an out-of-state action.[15] A foreign subpoena may be issued to the Clerk of the Court in the county in which discovery is sought, accompanied by the proper fee[16] and an application for a California subpoena with the same terms as the foreign subpoena.[17] Alternatively, upon presentation of the forms and fees required under the statute, an active California attorney may issue a foreign deposition subpoena without going to the local court.

Anticipated Objections By Users And SNPs

Once the discovery is served, the demanding party should be prepared for likely objections from opposing counsel and the SNP. Standard objections claiming requests are overly broad, vague and unduly burdensome will likely be lodged, but responses can be tailored in a manner to facilitate disclosure. Responses to objections based upon the Stored Communications Act ("SCA"),[18] however, require a more focused and detailed response.

The SCA prohibits electronic communication providers and remote computing services from "knowingly divulging the contents of their customers' electronic communications or records relating to their customers.[19] Because the SCA was enacted before the advent of social networking, case law addressing the SCA previously focused on

***Loryn P. Riggiola** is a Member of the Firm's Commercial and Construction Law Practice Group, representing clients in counseling, litigation and arbitration of disputes. **Grace A. Brown** is an Associate in the Firm's Employment and Labor Practice Group.* *The authors would like to extend their special thanks to **Bonnie Schwab,** the Firm's Managing Clerk, for her contribution and research regarding the procedures and forms for subpoenas in California.* *The views and opinions expressed in this article are those of the authors and do not necessarily reflect those of Sills Cummis & Gross P.C.*

Please email the authors at lriggiola@sillscummis.com or gbrown@sillscummis.com with questions about this article.

email providers. More recently, however, courts have addressed the parameters of the SCA with regard to social networking.

In the case of *Crispin v. Christian Audigier, Inc.*,[20] a court analyzed whether private communications sent through social networking sites are protected by the SCA. Defendants issued third-party subpoenas to Facebook and MySpace, among others, to obtain all messages and wall postings that referred to the defendants. The California federal district court in *Crispin* held that private messages sent via Facebook and MySpace were protected by the SCA. The *Crispin* court drew a distinction, however, between plaintiff's private messages and wall postings, because wall postings are generally public, unless specifically protected by the user. Accordingly, the *Crispin* court remanded for a determination of whether the plaintiff's privacy settings rendered these wall postings unprotected by the SCA.

Although *Crispin* suggests that a user's efforts to make communications on social networking sites private is a key factor in determining whether a user's communications are protected by the SCA, some courts have still required parties to provide access to this purportedly private information. For instance, in *Romano v. Steelcase*[21] a New York State court ordered a plaintiff to execute a consent and authorization form providing defendants access to information on the social networking sites she utilized. The *Romano* court held that in light of public information, such as the smiling profile picture, there was a reasonable likelihood that other information on the social networking sites could contain evidence relevant to her damage claim regarding her enjoyment of life.[22]

The judge's approach in *Romano* is consistent with exceptions in the SCA that permit disclosure of a user's information with lawful consent.[23] Courts may, however, be resistant to compel a party to disclose social networking information in order to prevent a fishing expedition into a party's personal information.[24] Nonetheless, where the information is discoverable, a court may very likely require the party to execute an authorization.[25]

Conclusion

Social networks are a relatively untapped discovery source that can contain a wealth of useful information. Because unsophisticated users of social networks will likely have difficulty preserving such data, the best source for discovery is to seek the production directly from the SNPs subscribed to by the user. For compliance with the SCA, counsel will be required to secure consent from the user, which can be compelled by a court. With the service of a subpoena and authorization from the user, counsel can begin the process of obtaining production from the SNPs.

Although some users have successfully argued that the privacy settings should dictate what information is discoverable, such an analysis defies the historically broad scope of discoverable information. For example, the fact that a party sends written correspondence to another in a sealed envelope, even marked confidential, does not render it undiscoverable. The same is arguably true for ESI, whether it is email or communications through social networks, regardless of whether the user designated the information as private.

Although somewhat challenging, securing discovery from SNPs is achievable. Indeed, in many instances it is the only source from which counsel can achieve the complete historical information from a users' social networking sites. As such, it is a discovery source that should be explored.

---

[1] Nielson.com, "*What Americans Do Online: Social Media And Games Dominate Activity*," Aug. 2, 2010, http://blog.nielsen.com/nielsen wire/online_mobile/what-americans-do-online-social-media.

[2] *Facebook – Statistics*, http://www.facebook.com/press/info.php?statistics, Facebook.com, (last accessed December 28, 2010).

[3] EBiz/MBA, "*Top 15 Most Popular Social Networking Websites*," December 2010, http://www.ebizmba.com/articles/social-networking-websites.

[4] As of November 2009, each of the top ten Fortune 500 companies had Twitter and Facebook profiles - Exxon Mobil, Wal-Mart Stores, ConocoPhillips, General Electric, General Motors, Ford Motor, AT&T, Hewlett-Packard and Valero Energy. *See* Websudasa,*"Can Facebook Beat Twitter in Fortune 500 Companies,"* Websudasa Blog, November 30, 2009, http://www.websudasa.com/blog/2009/11/can-facebook-beat-twitter-in-fortune-500-companies/.

[5] Burson-Marsteller, "*Fortune Global 100 Social Media Study*," Burson-Marsteller.com, February 23, 2010, http://www.burson-marsteller.com/Innovation_and_insights/blogs_and_podcasts/BM_Blog/

Lists/Posts/Post.aspx?ID=160.

[6] Miguel Helft, "*Facebook Seeps Onto Other Websites*," N.Y. Times, April 18, 2010, http://www.nytimes.com/2010/04/19/technology/19facebook.html?_r=1.

[7] *See* Karen L. Stevenson, "*What's On Your Witness's MySpace Page?*," March 2008, http://www.abanet.org/litigation/litigationnews/2008/march/0308_article_myspace.html.

[8] *See* Tiffany M. Williams, "*Social Networking Sites Carry Ethics Traps and Reminders*," August 27, 2009, http://www.abanet.org/litigation/litigationnews/top_stories/social-networking-ethics.html.

[9] A quick reference chart that sets forth the necessary steps to initiate discovery from SNPs can be easily accessed at www.metrocorpcounsel.com.

[10] It is unlikely that an SNP user will voluntarily provide his password in response to discovery requests. Importantly, once the litigator makes discovery requests the user will likely delete relevant information. SNPs are able to access information even after a user has deleted it, making it critical to subpoena the SNP directly and not simply rely on information the user provides.

[11] Fed. R. Civ. P. 26(b).

[12] CPLR 3101.

[13] *See* Fed. R. Civ. P. 26(b)(2); Fed. R. Civ. P. 34(a); N.J. Ct. R. 4:10-2(a).

[14] CPLR 3119; The Joint Committee On Electronic Discovery proposed several amendments to address the changing discovery landscape and effective January 1, 2011, the CPLR has been amended to specifically address the duty and scope of preservation of ESI. Association of the Bar of the City of New York Joint Committee on Electronic Discovery, "*Explosion of Electronic Discovery in All Areas of Litigation Necessitates Changes in CPLR*," p.1-3, August 2009, http://www.nycbar.org/ pdf/report/uploads/20071732-ExplosionofElectronicDiscovery.pdf.

[15] Cal Code Civ Proc § 2029.300.

[16] Cal. Evid. Code § 1563(b)(6).

[17] Additionally, the litigator will need to obtain a deposition agent in California to secure document production from the SNP. *See* Cal Code Civ Proc § 2020.430 and Cal. Evid. Code § 1560. Note that the foreign subpoena should provide that records are to be produced by the date and time on the subpoena, but no sooner than 20 days after issuance or 15 days from service.

[18] Title II of the *Electronic Communications Privacy Act*, 18 U.S.C. § 2510 *et seq.*

[19] 18 U.S.C. § 2702(a)(1) 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)(2)(same prohibition for a person or entity providing a remote computing service). The SCA was enacted as part of the Electronic Communications in Privacy Act of 1986 and predates the use of social networks. *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008)(citations omitted), *Abrogated in part by Flagg v. City of Detroit*, 252 F.R.D. 346, 2008 U.S. Dist. LEXIS 64735 (E.D. Mich. 2008).

[20] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[21] *Romano v. Steelcase, Inc.*, No. 2006-2233, 2010 N.Y. Misc. LEXIS 4538, *7 (Sept. 21, 2010).

[22] *Id.* at *3-4.

[23] *See* Section 2702(b)(3) of the SCA states that a provider "may divulge the contents of a communication…(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service". Section 2702(c)(2) of the SCA states that a provider "may divulge a record or other information pertaining to a subscriber to or customer of such service…(2) with the lawful consent of the customer or subscriber."

[24] *Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc.*, No. 2:06-cv-00788, 2007 U.S. Dist. LEXIS 2379 (D. Nev. Jan. 9, 2007)(refusing to order plaintiff to execute provide consent to obtain information from MySpace to prevent a fishing expedition); Ronald J. Levine and Susan L. Swatski-Lebson, "*Are Social Networking Sites Discoverable?*," November 13, 2008, http://www.law.com/jsp/ lawtechnologynews/ PubArticleLTN.jsp?id=1202425974937 (November 13, 2008)(citing, *T.V. v. Union Township Board of Education*, No. UNN-L-4479-04 (N.J. Super. filed Dec. 22, 2004)(finding that due to privacy concerns plaintiff's personal social networking pages is discoverable only if there is a particularized showing that the information is relevant)); *Cf Beye v. Horizon Blue Cross Blue Shield*, 568 F. Supp. 2d 556, 564 (D.N.J. 2008)(ordering plaintiffs to produce information posted on their daughters' Facebook and MySpace pages); *Ledbetter v. Wal-Mart Stores Inc.*, No. 06-cv-01958, 2009 U.S. Dist. LEXIS 113117 (D. Colo. Apr. 21, 2009) (denying plaintiffs' motion for protective order regarding their Facebook, MySpace and Meetup.Com content and permitting Wal-Mart's subpoenas).

[25] Once produced, courts appear to liberally permit admissibility of information secured from social networks applying the traditional rules of evidence. *See* Robert C. Rodriguez, "*Decisions Reflect Importance, Limitations of Evidence Obtained from Internet*," February 3, 2010, http://www.abanet.org/litigation/litigationnews/top_stories/020310-evidence-admissibility-social-networking-saadi-dockery.html.