

Obtaining Records From Facebook, LinkedIn, Google and Other Social Networking Websites and Internet Service Providers.

The defense employment bar is becoming increasingly aware of the potential to uncover valuable information from social networking sites like Facebook, LinkedIn, MySpace, etc., as well as email services such as gmail. An ever increasing number of employees are joining one or more of these networking sites. For example, Facebook, which claimed 250 million “active users” as of July 2009, reached 400 million active users as of February 2010!¹ And they do mean “active.” According to Facebook, “50% of our active users log on to Facebook in any given day” and “People spend over 500 billion minutes per month on Facebook.”² Facebook states that the “Average user creates 70 pieces of content each month” and “More than 25 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month”!³

The demographic of the typical user of these sites has also been changing: from teenagers and college students, to young adults in their twenties, to people of all ages.⁴ My 90 year-old mother-in-law “Facebooks” regularly! Of course, some sites – LinkedIn, for example – are designed and intended to attract older, more experienced, more senior and more professional members.

What sorts of evidence might one find if given access to a plaintiff employee’s information on one of these sites. Was the employee using them during work hours? Using them for hours at a time? Has he posted information (written posts, photos, video, even audio files) containing useful admissions? Do they reveal previously unknown misconduct which would support an after-acquired evidence defense? Do they reveal that the allegedly offensive harassing conduct was in fact welcome, or at least not likely to have been offensive to the plaintiff? Can they provide dates and times of activity useful in defending a wage and hour lawsuit? The list is really endless. However, it appears that users of social network sites often “let their hair down” in a way that surpasses even the thoughtless statements that all too often appear in email.

In a pending wage and hour case, I recently issued subpoenas to Facebook, LinkedIn and Google (on a gmail account), for posts by the plaintiff on Facebook and LinkedIn and, separately, for dates and times of any activity initiated by the account holder.

I split out the “dates and times” category because, contrary to popular belief, it is not possible simply to subpoena user records containing any “content” from an internet email or social networking site. Electronic communications holders (“EC holders”) like Facebook, LinkedIn and Google refuse to produce records containing the content of electronic communications based on the Stored Communications Act, 18 U.S.C. § 2701, et. seq. (the “SCA”).

¹ <http://www.facebook.com/press/info.php?timeline>

² <http://www.facebook.com/press/info.php?timeline#!/press/info.php?statistics>

³ <http://www.facebook.com/press/info.php?timeline#!/press/info.php?statistics>

⁴ See statistics at <http://www.insidefacebook.com/2010/01/04/december-data-on-facebook%E2%80%99s-us-growth-by-age-and-gender-beyond-100-million/>

The SCA generally prohibits -- subject to certain exceptions -- a "person or entity providing an electronic communication service to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). It further prohibits -- again, subject to certain exceptions -- a "person or entity providing remote computing service to the public" from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service." 18 U.S.C. § 2702(a)(2). Disclosure in violation of the SCA can expose the record holder to civil liability. (*Theofel v Farey-Jones* 359 F.3d 1066 (2004, CA9 Cal), cert den 160 L Ed 2d 17, 125 S Ct 48 (2004) (Because corporation and attorney procured consent by exploiting mistake of which they had constructive knowledge of subpoena's invalidity, district court erred when it dismissed officers' claim for violation of SCA based on such consent.))

The SCA enumerates several exceptions to the rule that service providers may not disclose the contents of stored messages. Among the disclosures authorized are those that are incidental to the provision of the intended service (see 18 U.S.C. § 2702(b)(1), (4), (5)); incidental to the protection of the rights or property of the service provider (18 U.S.C. § 2702(b)(5)); made with the consent of a party to the communication or, in some cases, the consent of the subscriber (see 18 U.S.C. § 2702(b)(3)); related to child abuse (18 U.S.C. § 2702(b)(6)); made to public agents or entities under certain conditions (18 U.S.C. § 2702(b)(7), (8)); related to authorized wiretaps (18 U.S.C §§ 2702(b)(2), 2517, 2511(2)(a)(ii)); or made in compliance with certain criminal or administrative subpoenas issued in compliance with federal procedures (18 U.S.C. §§ 2702(b)(2), 2703)).

The SCA does *not* include an exception for civil subpoenas. Several courts have concluded that this means that EC holders may not produce "content" records in response to a civil subpoena and cannot be compelled by court order to do so. (see, e.g., *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423; 44 Cal. Rptr. 3d 72 (2006); *Theofel, supra*; *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp.2d 606, 609-10 (E.D. Va. 2008); *Federal Trade Commission v. Netscape Communication Corp.*, 196 F.R.D. 559, 559, 561 (N.D. Cal. 2000); *Flagg v. City of Detroit*, 252 F.R.D. 256 (E.D.Mich. 2008).)

Note that, if your subpoena does not call for production of records containing "content," the SCA does not bar enforcement. What constitutes "content" is uncertain. In response to my pending subpoena to LinkedIn, a paralegal from the legal department called to tell me that they would not produce content. When I pointed out that one category sought dates and times only, she said they had "never dealt with that issue before." After speaking with the General Counsel, however, that paralegal advised that it was their position that this *is* content. I am waiting for the formal response.

On the other hand, after sending a form letter objection, Google has stated they will produce records showing solely the dates and times of emails sent by the account holder, if the plaintiff does not object within 20 days.

So how does a defendant go about obtaining potentially significant evidence from an EC holder like Facebook or Google? Obtain "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." (18 U.S.C.A. §2703(b)(3).)

What must be included in that consent? I have been trying, so far without success, to obtain that information or a form from either Facebook or Google. From information available on the internet, I would suggest, at least when the person giving consent is the subscriber, the following:

- The full name of the account holder or user of the service from whom you want the records;
- The person's "user id" or "group id" (if available; this is probably not necessary if the user has an unusual name; it is likely essential if the user's name is at all common);
- If the user's name is not unusual (this may be unnecessary where the user's name is very uncommon so that it will be easy for the ISP to eliminate all users except the one in whom you are interested), the user's:
 - "user id" or "group id";
 - Birth date; and
 - Full address as registered with the ISP;
- For an email account, the email address;
- A precise description of the records sought (to avoid objections of vagueness and overbreadth);
- Citation to the SCA and in particular to 18 U.S.C.A. §2703(b)(3); and
- Have the signature of the person giving consent be notarized (I think belt and suspenders make sense here – I would get as many originals as there are sources of records).

I have not had occasion to seek EC records based on the consent of the "originator or an addressee or intended recipient of such communication," and have not analyzed the additional issues that may arise and the additional information the EC holder may require.

What if the plaintiff-user refuses to sign a consent? In what appears to be its form letter response to a civil subpoena, Google cited authority that a party may be compelled to sign the consent. (*O'Grady v. Superior Court; Flagg*, 252 F.R.D. at 348, 366-7.) *O'Grady* involved Apple suing an internet news site which had published articles about not-yet-released Apple products and seeking discovery of emails and other EC records concerning the sources of that information. As a result, it involves other complicated issues. *Flagg* involved a wrongful death suit against the City of Detroit and several police officers. The plaintiff sought text messages between various defendants, and others. In that case, the court concluded that a party could be

compelled, in the context of a Rule 34 request for production, to produce non-privileged and relevant text messages under its control *including* those held by the ISP.⁵

In either case, the records will be turned over to the account holder or his attorney only, who may then be compelled to produce them to the defense.

You can assume the EC holder will contend that the records sought can and should be obtained from the plaintiff directly. Both Google and Facebook have done so in response to my subpoenas (although Google later dropped that demand when it concluded I was not seeking “content”). That may be possible depending on the information sought. However, as anyone who has spent any time on Facebook soon learns, accessing all of the plaintiff-user’s posted information is virtually impossible from the user side (at least with regard to active users). I think that establishing through an initial request for production that this cannot be achieved is an essential step in setting up getting the records from the EC holder. Once the plaintiff responds he can’t make a full production (or objects based on burden), the stage is set for a motion to compel.

Facebook has a “Safety For Law Enforcers” page which includes information regarding civil subpoenas.⁶ Among other statements, it says: “If a Facebook user deletes content from their account, Facebook will not be able to provide that content.” I’m not sure that is true.⁷ Apparently relying on the *Flagg* case, Facebook states: “To the extent a user claims it does not have access to content (e.g., the user terminated their account), Facebook will restore access to allow that user to collect and produce the information to the extent possible. Even with consent, Facebook will not produce content to anyone other than the Facebook user and/or the user’s attorneys.”

In response to a subpoena, Facebook will provide “basic subscriber information for a particular account.” This is not “content.” It will only respond to a California or Federal subpoena which should be served on: Custodian of Records, Facebook, Inc., c/o Corporation Services Company, 2730 Gateway Oaks Drive, Suite 100, Sacramento CA 95833. We are waiting to see whether Facebook considers “date and time” information “content.”

Google takes the astonishing (and, I believe, completely invalid) position that it will only accept subpoenas issued from Santa Clara Superior Court (home of Silicon Valley). A subpoena to Google must be served on Google Custodian of Records, 1600 Amphitheater Parkway, Mountain View, CA 94043.

Facebook (and other EC holders, I expect) also demand a fee to perform a search for a users records. I have found a number of links which suggest that Facebook’s fee varies. A July 2009 blog post quotes a letter from Facebook demanding a \$150 fee.⁸ Its “Safety For Law Enforcers” page now quotes a price of \$500 per user account, plus \$100 for a notarized declaration. However, Facebook’s objection last week to a subpoena I issued specifies \$250 “in

⁵ The *Flagg* court relied in part on *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 903-09 (9th Cir. 2008). Certiorari has been granted in this case. (130 S. Ct. 1011 (2009).)

⁶ <http://www.facebook.com/help/?safety=law>.

⁷ I understand that Facebook’s Director of Security testified this spring (in the Knoxville trial of the student who had hacked into Sarah Palin’s email and then boasted about it on Facebook) that Facebook maintains records “continuously”. I don’t know if the student tried to delete those posts.

⁸ <http://lawyerist.com/subpoena-facebook-information/>

minimum processing fees for the costs of production.” Google is not charging a fee to respond to a subpoena which asks solely for the dates and times of any activity initiated by the account holder. I haven’t been able in quick searches to find a statement of their fee and their form letter was silent on the subject.

Contact information for search warrants for many ISPs can be found at <http://www.search.org/programs/hightech/isp/default.asp#212>.

Awareness of the types of records an entity such as Facebook will have which are related to an individual user of the website is helpful in focusing a “consent” so as to avoid a claim of undue burden by the EC holder. A broad “all records” request by the user is likely to be met with either a flat refusal by the site or a demand for a substantial fee for the search and production of records. I suspect the fees Facebook quotes only get you in the door. Further, a broad request is likely to yield less information than a more specific request.

While I am not (yet) an expert on all the types of information that can be requested from these various sites (a good reason to get a IT consultant involved where the case warrants it), I have found a useful source: a Computerworld.com blog along with a detailed listing of types of information available from Facebook and Comcast.⁹ Every EC holder is likely to have, in addition to site-specific information, a form of IP Log. LinkedIn’s paralegal states it will provide the date and time of every “login” by the user. This is not deemed by LinkedIn to be “content” and they state they will be producing it. As of 2007, Facebook’s IP Log was “generally retained for 90 days from present date.” It is unknown what they do now.

For those who wish to research this area, I recommend as good starting points Kerr, Orin S., A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, *George Washington Law Review*, 2004¹⁰; Ackerman, Consent and Discovery Under The Stored Communications Act, 56 *The Federal Lawyer* p. 42, November/December 2009.¹¹; and Rolf & Salvesson, The Usefulness of Social Networking Websites to a Resourceful Defense Team, Vol. 3 No. 1 *Strictly Speaking*, Winter 2008.¹²

⁹http://blogs.computerworld.com/15667/leaked_intelligence_documents_heres_what_facebook_and_comcast_will_tell_the_police_about_you

¹⁰ Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860.

¹¹ Available at http://www.pattersonsheridan.com/images/uploads/SCA_Control_article_PUBLISHED-crop.pdf.

¹² Available through DRI at <http://www.dri.org/ContentDirectory/Public/Newsletters/0200/2008%20Product%20Liability%20Committee%20Strictly%20Speaking%20Winter.pdf>