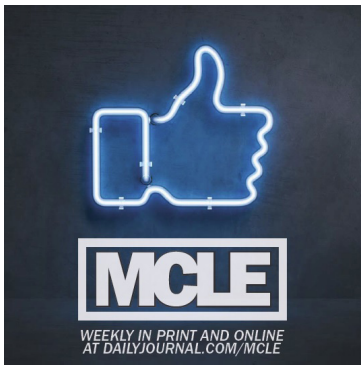
LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, APRIL 1, 2019

MCLE–PART 1

Social media discovery: 20 commonly asked questions

By Peter R. Boutin
and George A. Croton



Social media saturates nearly every aspect of our lives. As a result, social media accounts can be a goldmine of potentially discoverable information for parties in litigation. Unfortunately, courts, legislatures and practitioners have struggled in developing cohesive guidelines for keeping up with the fast-paced world of tweets and hashtags. Thus, seeking discovery of posts, comments and messages on social media platforms can be fraught with traps for the unwary. In this two-part series, we address 20 basic questions that often arise when parties seek social media records or other forms of electronically stored information, or ESI. Here are the first 10.

1. What type of information is contained in social media? A wide variety. Social media sites store vast amounts of user data, including pictures, messages, videos, emojis, public and private posts, details about the users' friends and acquaintances, and an abundance of associated metadata stating when, where and how the account holder used the platform. In litigation, this type of information often makes or breaks a case.

2. Do courts allow social media "fishing expeditions"? Generally no. Most courts refuse to allow overbroad requests for social media data where there is no showing that the information sought is likely to lead to relevant evidence, or where the requests are disproportionate to the needs of the case. *See Montgomery v. Wal-Mart Stores, Inc.*, No.: 12cv3057-JLS (DHB), 2015 U.S. Dist. LEXIS 188010, *25 (S.D. Cal. July 17, 2015) ("Plaintiff objects to producing any and all social media information as it is a dramatically overbroad and harassing fishing expedition. The Court agrees with Plaintiff.") (citations omitted); *see also Winchell v. Lopiccolo*, 38 Misc. 3d 458, 461 (N.Y. Sup. Ct. 2012) ("[D]igital 'fishing expeditions' are no less objectionable than their analog antecedents.").

Some courts, however, have been more receptive to broad requests for social media data. S*ee Nucci v. Target Corp.*, 162 So. 3d 146, 151 (Fla. 4th DCA 2015) (finding photographs on social media sites were relevant in the context of a personal injury case because there was "no better portrayal of what an individual's life was like than those photographs the individual has chosen to share through social media before the occurrence of an accident causing injury"). Whether a court deems requests for social media information overbroad likely depends on the claims in the case: Photographs posted online are more likely to be relevant in a personal injury claim than in a trade secrets dispute. Tailored, targeted requests for relevant information are more likely to be enforced than demands for the entirety of a party's online presence.

3. Will courts order a party to produce his or her login or password? Usually no. Allowing a party unrestricted access to social media content implicates significant privacy concerns, so most courts are unwilling to force a party to produce login information. *See Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 U.S. Dist. LEXIS 141368, at *3 (S.D. Ohio Oct. 1, 2012) (finding that "defendants' discovery request is overbroad" because plaintiff's "username and password would gain defendants access to all the information in the private sections of her social media accounts — relevant and irrelevant alike"); *Holter v. Wells Fargo & Co.*, 281 F.R.D. 340, 344 (D. Minn. 2011) ("Just as the Court would not give defendant the ability to come into plaintiff's home or peruse her computer to search for possible relevant information, the Court will not allow defendant to review social media content to determine what it deems is relevant.").

Although ordering the production of login information is drastic, some courts have been willing to go to that extreme under certain circumstances, such as in personal injury cases or where much of the information is already publicly available. *See Largent v. Reed*, No. 2009-1823, 2011 Pa. Dist. & Cnty. Dec. LEXIS 612, at *17 (Nov. 8, 2011) (Pa. CP Franklin Nov. 8, 2011) (compelling personal injury plaintiff to turn over her login information to defense counsel and allotting defense counsel a 21-day window in which to inspect her profile). This approach obviously glosses over the fact that turning over login information allows an adversary to discover both public information and information that the user intended to remain private.

4. What if a party obtains consent to directly access her adversary's social media account? Be careful what you ask for. A party may be willing to provide direct access to her social media accounts and may even voluntarily share her login information. While this initially might seem appealing, volunteered access presents its own challenges.

First, although voluntarily providing direct access may appear to be a good faith gesture, it also shifts the burden of hunting for relevant information to the requesting party. *See SolarCity Corp. v. Doria*, No.: 16cv-3085-JAH (RBB), 2018 U.S. Dist. LEXIS 8286, at *15-16 (S.D. Cal. Jan. 18, 2018) ("Because [Defendant] provided SolarCity with the 'username and password to all [of his] social media accounts and e-mail accounts[,]' Plaintiff may efficiently search the electronic data in those accounts," but by "casting a wide discovery net, SolarCity may not now complain about the burden of 'sifting through' the produced ESI for the documents it seeks."). Second, by accessing the account directly, the requesting party risks altering, corrupting or otherwise damaging the account's contents. *See German v. Micro Elecs., Inc.*, 2013 U.S. Dist. LEXIS 4594, *21 (S.D. Ohio Jan. 11, 2013).

It almost always will be preferable to require the responding party to produce specific responsive content while remaining ready to move to compel in the event the responding party does not comply.

5. May parties use a subpoena to obtain relevant social media evidence directly from the social media platform? It depends. If a party claims she is unable to produce records or postings from her social media account, a natural solution might be for the requesting party to subpoena the information directly from the social media platform. Not so fast. Social media providers almost always object to subpoenas for social media content based on the Stored Communications Act. *See* 18 U.S.C. Sections

2701 (2012), et seq. The SCA substantially limits a social media provider's ability to disclose the contents of electronic communications. *See Shenwick v. Twitter, Inc.*, U.S. Dist. LEXIS 22676, *7 (N.D. Cal. Feb 7, 2018). In most circumstances, the SCA permits disclosure of only "non-content" information about the account (such as the subscriber's name, address, records of session times and duration, etc.) in response to a subpoena. As the California Supreme Court recently explained, however, communications configured as "public" by the user and that remain "public" at the time the subpoenas were issued, fall within the SCA's "lawful consent" exception. *Facebook, Inc. v. Superior Court*, 4 Cal. 5th 1245, 1271-77 (2018).

6. What about asking the court to order a party to consent to the discovery of their social media content? You may be on to something here.Given the challenges identified above, parties seeking social media content might have better luck persuading a court to order the responding party to consent to the platform's disclosure of the sought-after social media, which triggers an exception to the SCA. 18 U.S.C. Section 2702(b)(3) (permitting disclosure of the contents of communication with the lawful consent of the originator or an addressee or intended recipient of the communication). This approach has been successful in a number of cases. *See Juror No. One v. Superior Court*, 206 Cal. App. 4th 854, 855 (2012) (discussing the trial court's decision to order a juror to execute a consent form authorizing a social media provider to release for *in camera* review all items he posted during the trial); *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 656 (2010) (ordering plaintiff to deliver to counsel for defendant a properly executed consent and authorization permitting defendant to gain access to plaintiff's social media records); *Glazer v. Fireman's Fund Ins. Co.*, No. 11 Civ. 4374 (PGG) (FM), 2012 U.S. Dist. LEXIS 51658, at *8 (S.D.N.Y. April 4, 2012) (declining to decide whether social media communications were protected by the SCA and ordering the plaintiff to consent to disclosure).

7. What if the account privacy settings restrict access? Generally this will not matter if the content is otherwise discoverable, although courts can consider privacy interests in evaluating the proportionality of discovery requests. *Henson v. Turn, Inc.*, 2018 U.S. Dist. LEXIS 181037, at *15 (N.D. Cal. Oct. 22, 2018). Otherwise, there is no general privilege or privacy right that attaches to social media information. The mere fact that users may have set their profiles to "private" will not render their information immune from discovery. *See Nucci*, 162 So. 3d at 153-54 ("We agree with those cases concluding that, generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings."); *Patterson v Turner Constr. Co.*, 88 A.D.3d 617, 618 (1st Dep't 2011) (ruling that the postings on plaintiff's social media accounts, if relevant, "are not shielded from discovery merely because plaintiff used the service's privacy settings to restrict access"). Private social media information is discoverable in the same manner as a private personal diary. *Id.*

8. Will a court agree to conduct an in camera review of a party's social media evidence? Generally no. Most courts decline to conduct an in camera review of social media evidence because it forces the court to spend precious time and resources sifting through what could be an ocean of irrelevant information. *See generally Tompkins v. Det. Metro. Airport*, 278 F.R.D. 387, 389 (E.D. Mich. 2012).

Exceptions do exist, however. *See, e.g., Juror No. One*, 206 Cal. App. 4th at 855; *Offenback v. L.M. Bowman, Inc.*, No. 1:10-CV-1789, 2011 U.S. Dist. LEXIS 66432, at *7 (M.D. Pa. June 22, 2011) (conducting a "thorough in camera review" of the personal injury plaintiff's social media account).

9. Might a court order the production of profiles for "attorney's eyes only"? Maybe. Some courts have ordered a responding party to produce social media evidence on the condition that only the requesting party's attorney may review the materials. *See Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMPVCF, 2012 U.S. Dist. LEXIS 85143, at *13-14 (D. Nev. June 20, 2012). In *Thompson*, the court ordered the plaintiff to upload all information from her social media accounts to a hard drive and to provide the hard drive to the defendant's attorney. The court instructed the defendant's attorney to provide a list of discoverable material to the plaintiff's counsel within seven days of receiving the hard drive.

The method utilized in Thompson arguably protects against overly intrusive forays into a responding party's privacy while simultaneously allowing the requesting party's attorney access to relevant, discoverable information. The drawback is that it places the burden of searching for that information on the requesting party's shoulders.

10. Will a court order the production of Fitbit or other activity tracking data? Possibly. At least one court has contemplated ordering this type of content. *See Hinostroza v. Denny's Inc.*, 2018 U.S. Dist. LEXIS 109602, at *11-12 (D. Nev. June 29, 2018). In Hinostroza, the defendant requested that the personal injury plaintiff produce data from a Fitbit or other activity tracker for a period of five years. *Id.* The defendant argued that information obtained from an activity tracker was relevant because, "if Plaintiff is walking/ running miles every day, then this would affect the validity of her claim [and allegation of future lumbar surgery]." *Id.* The court agreed and ordered the plaintiff to supplement her response to fully describe the search she conducted for Fitbit data.

Peter R. Boutin *is a partner at Keesal, Young & Logan in its San Francisco office, and* **George A. Croton** *is an associate at the firm. The opinions expressed in this article are those of the authors and do not necessarily reflect the views of the firm or its clients. The contents of this article are intended to convey general information only and not to provide legal advice or opinions. An attorney should be contacted for advice on specific legal issues.*


BOUTIN


CROTON