

How to Get Damaging Evidence From Litigants' Social Media Sites: PRACTICE TIPS IN DEALING WITH THE STORED COMMUNICATIONS ACT



John R. Crawford and
Benjamin A. Johnson*



"Humans like to know about the good, the bad, and the ugly side of people, places, and situations, as well as to share this information with others, often as quickly as possible."

Lon Safko and David Brake,
Authors of "The Social Media Bible"

"Social media" is a relatively new term and covers a wide range of websites that allow users to create an on-line profile to share pictures, comments, messages, news stories, and music. The best known of these is Facebook, which has approximately 845 million users, and 483 million of those users are active every day.¹ MySpace, which was in significant decline, recently experienced a period of renewed interest when new investors including Justin Timberlake purchased it.² At the time this article was written, Twitter was closing in on 600 million users, and was adding accounts at the rate of 12 per second.³ Anyone with a Facebook account can tell you that the users post witty comments about current events, trade barbs after football games, and post an unbelievable amount of personal information.

Discovery relating to social media has become an integral part of personal injury litigation. Social media provides a new way to see if a party's postings undermine his or her claim.

Many people doubt the value of discovery related to social media. How likely is it, they wonder, for a person to post pictures or statements that contradict their claims? An anecdote from a case this law firm handled shows the value of social media discovery. A woman suffered soft tissue injuries in a relatively minor motor vehicle accident. However, her medical and chiropractic records showed ongoing complaints related to neck and back pain, long after she should have recovered from the accident. Discovery provided by her attorney did not explain the ongoing complaints. However, her Facebook page included several photographs showing this plaintiff lifting weights. The photographs were at a national bench press competition, and were taken after the accident. As a result of the photographs and other information obtained regarding the plaintiff's weightlifting, the value of the case dropped dramatically.

Most forms of social media have levels of privacy protection. Users can often set their own controls, and limit how much information members of the general public can see.⁴ As people have become more concerned about online privacy, the information

available to the general public has shrunk. As a result, it is no longer possible to rely on a quick online search to determine if a person has shared any information. Attempting to gain access to a person's account by misrepresenting yourself is not ethical.⁵ This article will explain the law regarding discovery of a plaintiff's social media postings and provide several practice tips to transportation lawyers.

"Privacy is dead, and social media hold the smoking gun."
Pete Cashmore, Mashable CEO

I. The Stored Communications Act

In 1986, Congress adopted the Stored Communications Act.⁶ That Act was designed to extend privacy protection to areas which the Fourth Amendment did not cover.⁷ Under the Fourth Amendment, individuals lose any expectation of privacy in information they turn over to a third party.⁸ There are several well-known exceptions to this rule, including attorney-client privilege, or doctor-patient privilege. In addition sealed first-class mail and packages are protected by the Fourth Amendment.⁹ However, electronic communication presented a new challenge in which a person entrusts an unsealed message

*Johnson & Lindberg, P.A. (Minneapolis, Minnesota). Authors' Note: For an excellent article regarding relevancy and privilege regarding social media site information, see Eric L. Zalud, *Don't Let Your "Friends" Become Your "Frenemies": Discovery Dilemmas and Privilege Paradoxes in the Age of Social Media*, 13 *THE TRANSPORTATION LAWYER* 43 (April 2012).

to a provider (email provider, text message provider, etc.), that provider sends the message to the recipient, but the provider also typically retains a copy of the message for some amount of time. The Stored Communications Act clarified that an entity providing electronic communication services or remote storage services cannot divulge the contents of a communication.¹⁰ A government agency can obtain the information with an appropriate warrant, administrative subpoena, or court order.¹¹ Cases have been clear that an “administrative subpoena” does not include a discovery subpoena *duces tecum*.¹² Information can be released with the consent of the party who sent the message.¹³

There is much more that can be said about the Stored Communications Act. But for the purposes of this article, it is sufficient to say that an entity covered by the Act will not produce communications in response to a subpoena *duces tecum*.

“Don’t say anything online that you wouldn’t want plastered on a billboard with your face on it.”

**Erin Bury, Sprouter
community manager**

II. Relevant Case Law

The first cases addressing social media began to appear around 2007.¹⁴ Some defendants sought discovery directly from plaintiffs while others served subpoenas on the social network providers. For example, in *Mackelprang v. Fidelity Nat. Title Agency of Nevada, Inc.*, the defendant was attempting to obtain information from messages sent through MySpace.¹⁵ MySpace refused to provide the messages in response to a subpoena *duces tecum*, and the defendant sought the information directly from the plaintiff instead of seeking to enforce the subpoena. In contrast, in *Ledbetter v. Wal-Mart Stores, Inc.*, the court rejected the plaintiff’s motion to quash subpoenas served on Facebook, MySpace, and Meetup.com based on the theory that the subpoenas violated

the doctor-patient privilege and spousal privilege.¹⁶

In 2010, the Central District of California issued an opinion that has become the touchstone case on the issue of obtaining discovery from social networking sites. In *Crispin v. Christian Audigier, Inc.*, the plaintiff was an artist who agreed to license some of his images. The defendant placed the images on clothing, and sold the clothing. The plaintiff then sued, alleging that the images had been placed on products he did not approve, and that the products sold did not conform to the agreement. The defendants served subpoenas *duces tecum* on several social networking websites, including Facebook and MySpace, seeking communications between the plaintiff and other individuals that referenced the defendant in any way. The plaintiff sought to quash the subpoenas, arguing in part that the third party internet providers were prohibited from disclosing the information under the Stored Communications Act.¹⁷ In a lengthy decision that discussed the Stored Communications Act in detail, the court made several important findings:

- First, the court held that a plaintiff has standing to bring a motion to quash the subpoenas served on the third party social media providers.¹⁸
- Second, the court determined that the SCA does not specifically allow a party in a civil suit to obtain information by serving subpoenas on the providers.¹⁹
- Third, the court found that the SCA applied to messages sent through the social networking site, regardless of whether the messages had been opened by the recipient or were being held in storage.²⁰
- Fourth, the court said that wall posts on Facebook or MySpace were also covered by the SCA.²¹
- Finally, the court directed the parties to provide additional information on the plaintiff’s

privacy settings on the theory that information available to the general public would be discoverable.²²

In short, the decision said that a defendant cannot obtain any information, other than that available to the general public, by serving subpoenas on social media providers.

Serving requests on the plaintiff has become the accepted way to obtain social media information. In *Bower v. Bower*, the Court cited the applicable language of the SCA and noted that, “[f]aced with this statutory language, courts have repeatedly held that providers such as Yahoo! and Google may not produce emails in response to civil discovery subpoenas.”²³ But the court also commented that there is support for a party to make a document request and require an opposing party to obtain and produce its own emails because the SCA did not supersede the normal discovery rules.²⁴ In *Glazer v. Fireman’s Fund Ins. Co.*, the court determined that it did not need to address the SCA in its order “because it may simply direct that [the plaintiff] consent to disclosure if the chats are likely to contain information relevant to this case.”²⁵

Some courts have found that posts on social media sites are almost always relevant. In *Bass ex rel. Bass v. Miss Porter’s School*, the court commented that “Facebook usage depicts a snapshot of the user’s relationships and state of mind at the time of the content’s posting. Therefore, relevance of the content of Plaintiff’s Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff’s own determination of what may be ‘reasonably calculated to lead to the discovery of admissible evidence.’”²⁶

In contrast, other courts have determined that a plaintiff did not need to provide access to his or her account. In *McCann v. Harleystown Ins. Co. of New York*, the court

determined that the defendant had failed to establish that the information in the plaintiff's Facebook account was relevant, and therefore the court would not allow the plaintiff to conduct a "fishing expedition."²⁷ Similarly, in *Tompkins v. Detroit Metropolitan Airport*, the plaintiff claimed injuries resulting from a slip-and-fall at the Detroit Metropolitan Airport.²⁸ The court denied the defendant's motion for signed authorizations allowing access to plaintiff's Facebook account because, while the records were theoretically discoverable, the defendant had failed to make the threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence.²⁹

In summary, case law has established that a defendant cannot go directly to a social media provider to obtain the private messages or postings of a plaintiff. Instead, the defendant must make discovery requests to the plaintiff, and be prepared to bring a motion to compel a response to that request. In the motion, the defendant must be able to show that the information sought is relevant to the claims or the defense.

"Twitter is a great place to tell the world what you're thinking before you've had a chance to think about it."

Chris Pirillo, blogger

III. Practice Tips

When seeking a plaintiff's social media information, expect a battle from the plaintiff's attorney. It is important to lay the groundwork for a motion to compel as early as possible. Remember that case law disapproves of broad fishing expeditions. Therefore, any information related to the plaintiff's use of social media can help show the court that you have investigated as much as possible before bringing a motion.

There is usually no reason to send a subpoena directly to Facebook or another social media provider. As

discussed above, the SCA prevents the company from turning over more than basic information in response to a subpoena. Such a subpoena may be appropriate if a plaintiff denies having a social media presence, and you need to confirm or dispute that fact. However, the subpoena will usually be an exercise in futility.

Instead, the first step should be an internet search to determine whether the plaintiff has a profile that is open to the public. If so, it is important to print or save any relevant information since users generally have the ability to delete posts.

A defense firm should next send out standard Interrogatories with requests designed to uncover the existence of a social media presence. Interrogatories should ask for specific information at this stage. Many people use part of their email address as a "user name," and therefore a plaintiff's email address can reveal additional information. Interrogatories should request all email addresses in order to avoid receiving a work email address that does not relate in any way to a plaintiff's social media accounts. In both state and federal cases, one interrogatory should be used to ask the plaintiff to identify all social media sites on which he or she has a profile or account.

With the Interrogatories, a defense firm should serve a Request for Production of Documents. The initial request should include a request that the plaintiff sign an authorization to allow collection of his or her social media accounts. However, it is likely that such a request will be denied as overly broad. In that event, the appropriate response is to send targeted requests for specific information from the plaintiff's social media postings. Remembering that case law has shown skepticism of requests that appear to be a pure fishing expedition, the requests should focus on items that can be directly connected to the lawsuit: photographs of a plaintiff after an accident, postings about activities,

and postings that reference the accident. Facebook users can download an entire copy of their user data through the menu in their accounts list, so a plaintiff should not be able to argue that it is unduly burdensome to acquire that information. In addition, that request may give a court some middle ground between ordering the plaintiff to produce signed authorizations that provide full access to an account, and prohibiting any discovery on the issue at all.

If a plaintiff refuses to provide information related to social media after receiving targeted requests for documents, it is time to decide whether to proceed with a motion to compel that information. The key to a motion to compel will be convincing the court that there is, in fact, relevant information that the plaintiff is refusing to disclose. Therefore, any information that shows a plaintiff's activities and social media usage after an accident will be helpful. If you have nothing more than the fact that a plaintiff has a Facebook profile, the court is much less likely to force the plaintiff to provide any information. Therefore, it may prove to be appropriate to take the plaintiff's deposition first. Questions in the deposition should establish the plaintiff's use of social media, use since the accident, and postings including photographs that show or reference activities by the plaintiff. Alternatively, some narrow surveillance might also bolster a motion by showing that the plaintiff is engaged in certain activities.

Any motion to the court should include alternatives. As all practitioners know, most judges are hesitant to shut the door on an avenue of discovery completely. However, the likelihood that a judge will refuse to allow discovery increases when the defense cannot show that the discovery is relevant, or when the judge feels that the discovery is burdensome and invasive. References to a plaintiff's ability to download a copy of his or her entire user data simply shows

that the information is easy to access and requests for specific categories of postings limits the release of personal information. In addition, the motion to compel should include the option of an in camera review of the information by the court to determine what, if anything, is relevant.

After obtaining some limited information, it may be appropriate to return to the court for additional requests. Look closely at a person's pattern of use. Did the person post something every day, but then fail to post for several days after the accident? If so, it is possible that the information was deleted. Deleted information can usually be accessed by the host

website, and that may be grounds for a new motion for a signed authorization.

Finally, remember that discovery works both ways. A successful argument that the plaintiff's information is relevant may result in an argument that the truck driver's social media information is also relevant. It is a good idea to counsel drivers against posting anything related to an accident.

"What happens in Vegas stays in Vegas; what happens on Twitter stays on Google forever."
Jure Klepic, jureklepic.com

IV. Conclusion

The courts have struggled to find a way to deal with social media. They have extended the protection of federal statutes, making it almost impossible to obtain any significant information by sending subpoenas directly to the social media providers like Facebook, Twitter, MySpace, etc. However, that has not completely closed the door to that discovery. Instead, courts have acknowledged that the information can be relevant to claims. As such, after a showing by a defendant that the information is relevant, courts have required plaintiffs to sign authorizations. That is the only real method to obtain the information. 

Endnotes

1. <http://www.dailyfinance.com/2012/02/02/7-startling-numbers-we-now-know-about-facebook/>.
2. <http://www.guardian.co.uk/technology/2012/feb/14/myspace-one-million-users>.
3. <http://twopcharts.com/twitter500million.php>.
4. http://www.facebook.com/full_data_use_policy.
5. Sending such a request would likely violate various provisions of every state's Rules of Professional Conduct. Under the ABA's Model Rules, the request would violate Rule 4.1 (Truthfulness in Statements to Others), 4.2 (Communication with Person Represented by Counsel), Rule 4.3 (Dealing with Unrepresented Person), Rule 5.1 (Responsibilities of Partner or Supervisory Lawyer), Rule 5.2 (Responsibilities of Subordinate Lawyer), Rule 5.3 (Responsibilities Regarding Nonlawyer Assistant), and Rule 8.4 (Misconduct).
6. 18 U.S.C. § 2701-2712.
7. *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008).
8. *U.S. v. Miller*, 425 U.S. 435, 443 (1976).
9. *U.S. v. Van Leeuwen*, 397 U.S. 249, 251 (1970).
10. 18 U.S.C. § 2702(a)(1)-(2).
11. 18 U.S.C. § 2703.
12. *F.T.C. v. Netscape Communications Corp.*, 196 F.R.D. 559, 560 (N.D.Cal. 2000).
13. 18 U.S.C. § 2702(b)(3).
14. *See, i.e. Mackelprang v. Fidelity Nat. Title Agency of Nevada, Inc.*, 2007 WL 119149 (D.Nev.).
15. *Id.*
16. *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018 (D.Colo. 2009).
17. *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 968-69 (C.D.Cal. 2010).
18. *Id.*, at 974.
19. *Id.*, at 975-76.
20. *Id.*, at 987.
21. *Id.*, at 989-90.
22. *Id.*, at 991.
23. *Bower v. Bower*, 808 F.Supp.2d 348, 350 (D.Mass. 2011).
24. *Id.*
25. *Glazer v. Fireman's Fund Ins. Co.*, 2012 WL 1197167 (S.D.N.Y.).
26. *Bass ex rel. Bass v. Miss Porter's School*, 2009 WL 3724968 (D.Conn. 2009).
27. *McCann v. Harleysville Ins. Co. of New York*, 78 A.D.3d 1524, 1525 (S.C. A.D. Fourth Dept. N.Y. 2010).
28. *Tompkins v. Detroit Metropolitan Airport*, 287 F.R.D. 387 (E.D. Mich. 2012).
29. *Id.*, at 388-89.