

Reprinted with permission of *Trial*[®]
(December 2019). Copyright © 2019
American Association for Justice[®],
Formerly Association of Trial
Lawyers of America (ATLA[®]),
www.justice.org/publications.



KNOW THE Networks

Social media evidence can be both valuable and harmful. Learn how courts have responded to common social media discovery questions and how you can protect your client's privacy and get what you need from defendants.

By || **HEIDI L. WICKSTROM**

Litigation today requires navigating the digital histories of the people involved—which means attorneys must be up-to-date on social media discovery rules.¹ With a click of the mouse or stroke of the keys, plaintiffs can amass large numbers of social media posts, chats, tweets, and other electronic communications that are preserved for discovery seemingly forever. But understanding your client's social media presence is not the only challenge plaintiff attorneys face; we also must be ready to investigate defendants' social media use and profiles, which can offer ammunition for depositions, for settlement negotiations, or at trial.

No law prevents opposing counsel from investigating your client before litigation begins, and assuming the evidence is obtained through a legal search, people should not have any expectation of privacy on the public portions of social media sites.² Furthermore, publicly available social media information generally is not subject to claims of privilege.³ Stress this to your clients as soon as possible. Also tell them that any public posts by a spouse, child, or even a friend may be viewed by anyone, including defense counsel, especially if the client is tagged. If clients have “private” or “locked” accounts that they must give

permission for others to access, then their private information should not be fully available through simple online searches before litigation commences. But advise your clients that even “private” posts may be subject to legitimate and reasonable discovery demands if a court determines later that they are relevant to the claims made in the lawsuit.⁴

Broadly speaking, a party has a duty to preserve information relevant to litigation. But how much social media evidence needs to be preserved before litigation commences? And to what extent and in what form? Depending on your jurisdiction, the answers vary.

In all jurisdictions, increasing privacy settings on social media accounts before litigation begins is not spoliation of evidence; it’s simply good and prudent practice.⁵ However, the propriety of deleting case-related photographs and posts is a more complicated issue, and one that you should approach with extreme caution. As a general rule, litigants and attorneys should preserve



evidence they know, or reasonably should know, will be relevant to foreseeable litigation.⁶ Advising a client to delete or take down any social media posts is problematic, and many courts will treat conduct like this as spoliation of evidence.⁷ When in doubt, consult your local ethics rules.⁸

Your Client’s Social Media

Once litigation begins, you likely will receive interrogatories or discovery requests for your client’s social media information. How do you respond in a way that protects your client’s rights and privacy without violating your jurisdiction’s laws and rules governing social media discovery?

When you receive discovery requests that are overbroad, burdensome, or not specifically related to legitimate claims, remember that your client’s social media accounts are not discoverable simply because they exist.⁹ Many defendants ask for and expect unfettered access to the plaintiff’s posts and pictures after the date of the incident at issue in the case. In most circumstances, you should not honor these requests. Courts have routinely denied discovery requests for being overbroad when they request *all information* contained in plaintiffs’ social media accounts.¹⁰

Most courts have held that the information sought must be relevant and material to the issues in the case—meaning that it must be specific;

When evaluating the relevance of private portions of a party’s social media profile, courts have tended to agree that the critical factor is whether the public portion contains relevant information; a defendant “does not have a generalized right to rummage at will through information that [the] plaintiff has limited from public view.”¹³

But be aware that when claims for emotional distress and anguish are asserted, a minority of courts have broadened what defense counsel may review from a plaintiff’s social media presence.¹⁴ In one recent federal case, the court stated that “information from social media is relevant to claims of emotional distress because social media activity, to an extent, is reflective of an individual’s contemporaneous emotions and mental state”; therefore, the court ruled that the plaintiff’s social media information and communications were relevant and discoverable under Federal Rule of Civil Procedure 26(b).¹⁵

When attorneys disagree on what social media information is appropriate to provide to the other side, courts

Your client’s social media accounts are not discoverable simply because they exist.

narrowly tailored with precise dates; and relevant to the injuries, claims, and disputes at issue.¹¹ In *McCann v. Harleysville Insurance Co. of New York*, for example, an appellate court affirmed the denial of the defense’s “overly broad” request for an authorization permitting unrestricted access to the plaintiff’s Facebook account, characterizing it as “a fishing expedition” undertaken with the “mere hope of finding relevant evidence.”¹²

often order the disclosure of relevant social media evidence based on a factual predicate for the request, a sufficient showing from a public search, or a prior search that turned up deleted information.¹⁶ A printout of a plaintiff’s publicly available Facebook page depicting behavior or information that contradicts the plaintiff’s claims can be considered a sufficient basis for a court to order the production of social media records from that provider.¹⁷

Some courts also may conduct an in camera review of a party's social media information before determining what should be produced.¹⁸ Commonly, courts permit some disclosure of social media information but will impose limits based on what is appropriate in each case.¹⁹

The Defendant's Social Media

The same rules that apply to your client's social media apply to defendants too. After the case is filed, it is improper for anyone to delete already posted, potentially relevant information without saving a complete copy of what was deleted or removed from the account.

Send a narrowly tailored discovery request that explicitly states what you believe, based on prior investigation, are relevant social media posts, photos, or other online communications. Limit it to relevant dates and times; if possible, list the post or photo you are searching for.²⁰ For example, perhaps you took a screenshot of the defendant's tweet shortly after a motor vehicle collision with your client in which the defendant shared pictures of her car and information about the incident. Indicating the exact date, time, and substance of what you're looking for is crucial and should facilitate the efficient exchange of materials without court involvement.

Although defendants likely will request your client's social media information regardless, be ready for any of your requests to be reciprocated. Ask for email addresses; a list of social media networks and sharing sites, along with usernames; relevant videos uploaded online; copies of the posts, statuses, tweets, comments, or replies that are relevant to the action; and relevant podcasts or video posts. This list is not exhaustive—based on what you have uncovered in your preliminary investigation of the defendant's online presence, be as specific as possible.²¹

If you believe a defendant has taken down websites or webpages; erased

posts or videos; disabled webcam feeds; or directed online contacts to remove posts, videos, or comments, you need evidence to substantiate this claim. A screenshot of incriminating information revealed on a public profile or copies of previously posted photos will be valuable if the defendant has "cleaned" its online presence.

If you have proof that a defendant has destroyed or altered social media evidence, most courts treat this behavior as spoliation of evidence. In some instances, both the client and counsel can be subject to sanctions for failing to preserve evidence.²² Some courts use a less severe remedy—they order the offending party to attempt to recover what has been removed from a social media page so that the opposing party can view it.²³

You can hire internet security and social media experts to perform a more exhaustive and technical search of a defendant's web presence, especially if you believe online evidence has been altered. These experts, who are trained in social media discovery, may be able to track and uncover deleted information or photos, as well as sift through information that you might not have found yourself. If the case merits these experts, do not hesitate to retain them early.

Requesting Provider Records

Getting records from social media service providers can be very difficult. You may attempt to obtain these records via subpoena, similar to what you would send to a physician's office; however, these requests almost always go unanswered. The Stored Communications Act of 1986 (since amended to reflect technological advances) prevents social media sites from disclosing nonpublic content without a user's consent.²⁴ Many social media providers constantly change their technology, which can lead to data becoming inaccessible down the road.

DON'T FORGET

- Research your client's social media presence as soon as you sign the case.
- Instruct your client to use the highest privacy settings available on social media.
- Preserve online evidence with screenshots that are time stamped.
- Be suspicious of overly broad requests for your client's social media accounts.
- Be ready to petition the court if you feel online evidence has been destroyed.

Therefore, without the user's consent, almost all providers require a court order explicitly mandating disclosure before revealing user information in a civil case.

To subpoena information directly from a social media provider, you must show the court that an order mandating disclosure by the provider is necessary. Arm yourself with screenshots of what you believe is present on a litigant's social media page, as well as a tailored request for information that is very likely to lead to relevant evidence.


Nonparty and Expert Social Media

Social media can also be valuable when researching lay witnesses or experts. Similar to looking for the defendant's online public profiles, search for any lay witnesses who may testify at trial, such as people who may have witnessed the incident, as well as any experts hired by you or the defendant. Be mindful, however, that courts often are more protective of a nonparty's private

social media information than that of a litigant.²⁵

“Friending” or attempting to communicate through social media with the defendant—or any party in the case represented by counsel—is uniformly improper and unethical. Online communication with an unrepresented party or an expert is treated differently, depending on the venue.

In some jurisdictions, for example, lawyers “friending” a nonparty online do not need to disclose their law firm or their involvement in litigation but cannot make “deceptive” representations.²⁶ Courts in other states, however, mandate that these requests must inform the person of the lawyer’s complete identity, which includes name and firm, the name of the client, and the lawyer’s involvement in the matter being litigated.²⁷ Bottom line: Research your jurisdiction’s rules when considering connecting with a nonparty online, and when in doubt, be as forthcoming as possible.

Familiarizing yourself with social media discovery rules is more important than ever—not only to protect clients but also to uncover what could be game-changing information about the defendants and their experts and lay witnesses. 



Heidi L. Wickstrom is an attorney with *Salvi, Schostok & Pritchard* in Chicago and can be reached at hwickstrom@salvilaw.com.

NOTES

1. “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education, and comply with all continuing legal education requirements to which the lawyer is subject.” Model Rules of Prof’l Conduct, R. 1.1, cmt. 8 (2015) (emphasis added).
2. *Winchell v. Lopiccio*, 954 N.Y.S.2d 421 (N.Y. Sup. Ct. 2012).
3. *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566, 570 (C.D. Cal. 2012).
4. *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387 (E.D. Mich. 2012).
5. Fla. R. Prof’l Conduct 4-3.4(a) (2019); Pa. Bar Ass’n, Formal Op. 2014-300 (2014), www.pabar.org/members/catalogs/ethics%20opinions/formal/f2014-300.pdf; N.Y. Cnty. Lawyer’s Ass’n, Ethics Op. 745 (2013), www.nycla.org/site/Files/Publications/Publications1630_0.pdf.
6. *Wm. T. Thompson Co. v. Gen. Nutrition Corp., Inc.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984) (“While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.”).
7. *Gatto v. United Air Lines, Inc.*, 2013 WL 1285285, at *3-4 (D.N.J. Mar. 25, 2013) (sanctioning plaintiff for deleting his Facebook account after the defendants requested access and he agreed to provide them the password).
8. N.C. State Bar Ethics Comm., Formal Op. 2014-5 (2015), www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2014-formal-ethics-opinion-5/; see also Va. State Bar Disciplinary Bd., *In the Matter of Matthew B. Murray*, Docket Nos. 11-070-088405 and 11-070-088422 (2013).
9. *Tapp v. N.Y. St. Urban Dev. Corp.*, 102 A.D.3d 620 (N.Y. App. Div. 2013) (“[M]ere possession and utilization of a Facebook account is an insufficient basis to compel [that party] to provide access to the account or to have the court conduct an in camera inspection of the account’s usage.”).
10. *Forman v. Henkin*, 93 N.E.3d 882 (N.Y. 2018); *Vasquez-Santon v. Mathew*, 168 A.D.3d 587 (N.Y. App. Div. 2019).
11. *McCann v. Harleysville Ins. Co. of N.Y.*, 78 A.D.3d 1524, 1525 (N.Y. App. Div. 2011) (The defendant must have a “factual predicate” based on public portions of Facebook account to seek private portions of the account.); *Potts v. Dollar Tree Stores*, 2013 WL 1176504, at *3 (M.D. Tenn. March 20, 2013) (The defendant “lack[ed] any evidentiary showing that [p]laintiff’s public Facebook profile contains information that will lead to the discovery of admissible evidence.”); *Carlson v. Jerousek*, 68 N.E.3d 520 (Ill. App. Ct. 2016).
12. *McCann*, 78 A.D.3d at 1525.
13. *Palma v. Metro PCS Wireless, Inc.*, 18 F. Supp. 3d 1346, 1347 (M.D. Fla. 2014); see also *Caputi v. Topper Realty Corp.*, 2015 WL 893663, at *2 (E.D.N.Y. Feb. 25, 2015).
14. *Hinostroza v. Denny’s Inc.*, 2018 WL 3212014 (D. Nev. June 29, 2018).
15. *Id.* at *6.
16. *Medina v. City of N.Y.*, 2015 WL 9316065 (N.Y. Sup. Ct. Dec. 22, 2015).
17. *Id.* at *2.
18. Order After In Camera Inspection at 2, *Douglas v. Riverwalk Grill, LLC* (E.D. Mich. Aug. 24, 2012) (No. 11-15230) (After reviewing “literally thousands of entries,” the court found that the majority of the issues had no relevance to the case and designated the specific entries that it determined were discoverable.); *Richards v. Hertz Corp.*, 100 A.D.3d 728, 730 (N.Y. App. Div. 2012) (When searching public portions of the plaintiff’s Facebook account, the defendants found a photo of her skiing, despite the plaintiff claiming her injuries prevented her from playing sports and pain exacerbated by cold weather. The court granted a motion for in camera review of the plaintiff’s Facebook posts and photos since the incident.).
19. *Scott v. United States Postal Serv.*, 2016 WL 7440468, at *5 (M.D. La. Dec. 27, 2016) (The court found the defendant’s discovery requests overly broad and modified them to require the plaintiff to provide the sites and her usernames but only the last time she had been on each site, not the total time she spent on each site.).
20. *Dewidar v. Nat’l R.R. Passenger Corp.*, 2018 WL 280023, at *5 (S.D. Cal. Jan. 1, 2018).
21. *Brogan v. Rosenn, Jenkins & Greenwald LLP*, 2013 WL 1742689, at *7 (Pa. Ct. Com. Pl. Lackawanna Cnty. April 22, 2013).
22. *Lester v. Allied Concrete Co.*, 83 Va. Cir. 308 (Va. Cir. Ct. 2011), *aff’d in part, rev’d in part* 285 Va. 295 (Va. 2013).
23. *KatiRoll Co., Inc. v. Kati Roll and Platters, Inc.*, 2011 WL 3583408, at *7 (D.N.J. Aug. 3, 2011).
24. Stored Communications Act of 1986, 18 U.S.C. §§2701-2712 (2018).
25. *Katz v. Batavia Marine & Sporting Supplies, Inc.*, 984 F.2d 422 (Fed. Cir. 1993).
26. Ass’n of the Bar of the City of N.Y. Comm. on Prof’l Ethics, Formal Op. 2010-2 (2010), www.nycbar.org/pdf/report/uploads/20071997-Formal_Opinion_2010-2.pdf.
27. N.H. Bar Ass’n Ethics Comm., Advisory Op. #2012-13/05 (2013), www.nhbar.org/ethics/opinion-2012-13-05.