Getting Access to Social Media Evidence

BY PROFESSOR RICHARD S. KLING, KHALID HASAN, AND MARTIN D. GOULD

Social media content is a trove of potentially powerful evidence. How do you maximize your prospects for getting access to it? The authors explain how to use discovery and other means to obtain social media evidence and identify pitfalls to avoid in the process.

RICHARD S. KLING *is a practicing criminal defense attorney and Clinical Professor of Law at Chicago–Kent College of Law in Chicago, where he has been teaching since 1981.*

rkling@kentlaw.iit.edu

KHALID HASAN *is an associate at Lucas & Cardenas, practicing in the areas of personal injury, wrongful death, and medical malpractice.*

KJH@LucasandCardenas.com

MARTIN D. GOULD *is an associate attorney at Romanucci & Blandin, LLC, concentrating his practice on wrongful death, catastrophic personal injury, and police misconduct cases.*

mgould@rblaw.net

THE NEED TO OBTAIN SOCIAL MEDIA EVIDENCE HAS BECOME BOTH COMMON and critical during the discovery process. For example, the information available on social media can be used to find other witnesses through the user's friend list, impeach a witness through prior inconsistent statements, or show bias through a witness' friends or groups they have joined. This article describes how to obtain and preserve social media evidence.

Gaining access to social media evidence

Does an account exist? The first step in gathering information from social media is to determine whether the witness has a social media account. In civil cases, this can be accomplished through formal or informal discovery.

Formal discovery can be conducted through interrogatories, depositions, or other discovery methods. Informal discovery, on the other hand, requires a search for the user's social media presence via search engines such as Google or the social network website.

Public or private? The second step is to determine whether the user has altered his profile

TAKEAWAYS >>

- Social media evidence can be invaluable to your case. It can be used to find other witnesses through the user's friend list, impeach a witness through prior inconsistent statements, or show bias through a witness' friends or groups they have joined.
- The most effective method of obtaining discovery of "private" social media content is through well-tailored discovery requests to the opposing party, or by getting consent from the opposing party to obtain the content directly from the social networking site.
- If you suspect that an opposing party's social media content will be relevant to your case and necessary for discovery, you should send out a preservation letter to opposing counsel. Your letter must be clear on what social media content you would like to have preserved for discovery purposes.

settings from "public" to "private."[1] If the account is available to the public, the attorney is free to gather any information posted there.

However, ethical issues can arise when an attorney tries to gather information from a social media profile and the settings are private. If the information contained on the page is designated "private," formal discovery might be required to gain access.

Some attorneys erroneously believe that serving a subpoena to the social media provider directly is the best way to access "private" information. Even with a valid subpoena, Federal law and Facebook policies prohibit the disclosure of users' information to a non-governmental agency.[2]

The Stored Communication Act (SCA), as interpreted in *Glazer v. Fireman's Fund Insurance Co.*, holds that entities that provide electronic communication services are prohibited from knowingly revealing "to any person or entity the contents of a communication while in electronic storage by that service."[3] The Stored Communication Act, at most, only allows social network service providers to disclose the user's basic subscriber information.[4]

Social media providers such as Facebook, however, can provide more than just the user's basic information. Notably, the provider can give additional information if the user gives the service written consent to release the information and the user is the originator or recipient of the communication.[5]

Is the content relevant? The third step in getting access to social media information is to show the content is relevant to the case. Courts have been reluctant to allow for "fishing expeditions" of social media sites during discovery.[6]

In *Richards v. Hertz Corp.*, the court allowed discovery of social media and found that "[the defendants] made a showing that at least some of the discovery sought [would] result in the disclosure of relevant evidence or is reasonably calculated to lead to the discovery of information bearing on [the plaintiff's] claim."[7]

In *Carlson v. Jerousek*, an Illinois case addressing discovery of electronically stored information ("ESI"), the court wrote that the standard established by the "supreme court rules governing civil discovery advance this principle by limiting discovery to information that is relevant to the issues in the lawsuit."[8] The rules define discoverability of relevant information "broadly to encompass not only admissible information but also information calculated to lead to the discovery of admissible information."[9]

However, the court cautioned, "this definition is not intended as an invitation to invent attenuated chains of possible relevancy."[10] The court reasoned that "compelled disclosure of highly personal information 'having no bearing on the issues in the lawsuit' is an unconstitutional invasion of privacy."[11]

Various courts have applied a standard requiring the requesting party to provide the court with a basis and rationale for the need of social media during discovery.[12] This can be achieved by showing the party's public profile contradicts what they have stated, or a position they have taken during the litigation process.

1. See Deborah Jones Merritt, *Social Media, the Sixth Amendment, and Restyling: Recent Developments in the Federal Law of Evidence*, 28 Touro L. Rev. 27, 48 (2012).
2. See John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites*, 14 SMU Sci. & Tech. L. Rev. 465, 473 (2011).
3. *Glazer v. Fireman's Fund Insurance Co.*, No. 11 Civ. 4374 (PGG) (FM), 2012 WL 1197167, at *2 (S.D.N.Y. Apr. 4, 2012) (citing 18 U.S.C. § 2702(a)(1)).
4. See Browning, *supra* note 2, at 473.
5. See *Glazer*, 2012 WL 1197167, at *2.
6. See, *e.g.*, *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012).
7. *Richards v. Hertz Corp.*, 953 N.Y.S.2d 654, 656 (App. Div. 2012).
8. *Carlson v. Jerousek*, 2016 IL App (2d) 151248, ¶ 37.
9. *Id.*
10. *Id.*
11. *Id.*
12. See, *e.g.*, *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 652 (Sup. Ct. 2010).

SOME ATTORNEYS ERRONEOUSLY BELIEVE THAT SERVING A SUBPOENA TO THE SOCIAL MEDIA PROVIDER DIRECTLY IS THE BEST WAY TO ACCESS "PRIVATE" INFORMATION. IT IS NOT.

Is the request too burdensome? The fourth step in getting access to social media information is to overcome the proportionality balancing test, even if the information requested is relevant.[13] The proportionality balancing test requires the court to determine both monetary and nonmonetary factors in determining whether the burden associated with producing the requested social media evidence outweighs the benefit.[14]

Illinois Supreme Court Rule 201(c)(3) provides a list of the monetary and nonmonetary factors courts should consider. The court is permitted to consider factors such as "the extent to which the discovery sought represents a substantial invasion of the privacy interests of the responding party."[15] An invasion of privacy is permitted only when the invasion of privacy is "unreasonable" is it forbidden.[16]

In addition, the Illinois rules committee has generated a list of ESI that is generally not discoverable because of the high burden involved in producing the information.[17] However, "[d]iscovery of these categories of ESI is not absolutely prohibited…the committee comments suggest that these categories of ESI are presumptively nondiscoverable, shifting the burden to the requesting party to justify the making of an exception based on the particular circumstances of the case."[18]

Assessing the relevance of private info. So how can attorneys know whether "private" information on a user's profile is relevant when ethical guidelines may prevent them from viewing the content in the first place? There is no clear answer to this question.

In civil cases, attorneys should employ more formal discovery methods, such as depositions and interrogatories, before asking the court for access to a user's "private" social media account. Based on what they learn through formal methods, attorneys should make a clear and focused case for their need to access the user's "private" information.

Courts have been more inclined to allow access to "private" information when the request is narrowly focused.[19] Requests confined to specific time periods, conditions alleged by the victim, and damages sought are generally granted.[20]

Courts have rejected discovery requests they regard as overly broad, failing to show a connection between the case and the need for social media evidence, or made before formal discovery methods have been employed.[21]

The most effective ways to get discovery of "private" social media content is through well-tailored discovery requests to the opposing party or by getting the party's consent to obtain the content directly from the site. Parties or the court may also request an in-camera inspection of the evidence to decide whether it is relevant.[22]

Other ways to get social media evidence. What if the social media company objects to the subpoena on grounds that it violates the SCA or the profile cannot be produced in its original form? Courts may order parties to a case to produce or change their social media information.[23]

Courts have used creative ways to allow access to users' profiles. For example, a court ordered a party to change a Facebook picture back to "the allegedly infringing picture for a brief time" so that the opposing party may print the relevant Facebook picture as it existed at the prior time.[24] Courts have also recommended that certain individuals "friend" the judge "on Facebook for the sole purpose of reviewing photographs and related comments *in camera*."[25]

Preserving social media evidence

Courts have not clearly specified what steps need to be taken to preserve social media evidence during discovery, but

13. *Carlson*, 2016 IL App (2d) 151248, at ¶ 37.
14. *Id*.
15. *Id*. at ¶ 41.
16. *Id*. at ¶ 35.
17. *Id*. at ¶ 48.
18. *Id*. at ¶ 49.
19. See, *e.g.*, *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566, 569, 571-73 (C.D. Cal. 2012).
20. See, *e.g.*, *Levine v. Culligan of Florida, Inc.*, No. 50-2011-CA-010339-XXXXMB, 2013 WL 1100404, at *5 (Trial Order) (Fla. Cir. Ct. Jan. 29, 2013).
21. See, *e.g.*, *Mailhoit*, 285 F.R.D. at 569, 571-573.
22. See *Richards v. Hertz Corp.*, 953 N.Y.S.2d 654, 656-57 (App. Div. 2012).
23. Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH 11 (2013), *available at* http://jolt.richmond.edu/v19i3/article11.pdf.
24. *Katiroll Co., Inc. v. Kati Roll & Platters, Inc.*, CIV.A. 10-3620 GEB, 2011 WL 3583408, at *4 (D.N.J. Aug. 3, 2011).
25. *Barnes v. CUS Nashville, LLC*, 3:09-CV-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).

ISBA RESOURCES >>

- Richard S. Kling et al., *Admissibility of Social Media Evidence in Illinois*, 105 Ill. B.J. 38 (Jan. 2017), https://www.isba.org/ibj/2017/01/admissibilityofsocialmediaevidencei.
- Ed Finkel, *Building Your Case with Social Media Evidence*, 102 Ill. B.J. 276 (June 2014), https://www.isba.org/ibj/2014/06/buildingyourcasewithsocialmediaevid.
- Nicholas O. McCann, *Tips for Authenticating Social Media Evidence*, 100 Ill. B.J. 482 (Sept. 2012), https://www.isba.org/ibj/2012/09/tipsforauthenticatingsocialmediaevi.

some best practices are emerging.

Notify your opponent to preserve evidence. Attorneys who suspect that an opposing party's social media content will be relevant to the case and necessary for discovery should send out a preservation letter to opposing counsel.[26]

Spoliation of evidence is defined as "destruction, mutilation, alteration, or concealment of evidence."[27] Parties engage in spoliation "if a reasonable person in the [party]'s position should have foreseen that the evidence was material to a potential civil action."[28] Therefore, the duty to preserve attaches "when a party should have known that the evidence may be relevant to future litigation."[29]

Attorneys should clearly describe in a letter to opposing counsel or an unrepresented party what social media content they want to have preserved for discovery purposes. The preservation letter serves as "the linchpin of a subsequent claim for spoliation, helping to establish bad faith and conscious disregard of the duty to preserve relevant evidence."[30]

Warn your client to preserve evidence. Attorneys should take great care to counsel clients to preserve social media and other electronic evidence that might be discoverable and relevant to your litigation. Because social media can be easily altered or deleted, "[l]itigants have a duty to preserve relevant evidence that they know, or reasonably should know, will likely be requested in reasonably foreseeable litigation, and the court may impose sanction on an offering party that has breached this duty."[31]

Attorneys should also advise their own clients in writing about the importance of preserving electronic or social media evidence. Judges are less tolerant of attorneys claiming they lost social media evidence as it has grown more important in litigation. Electronic evidence should not be treated differently from any other evidence.

Confronting the false sense of privacy

The core purpose of social media is to connect with others and share information. A fundamental reality about social media is the false sense of privacy many users have. Many believe that changing their settings to "private" or restricting content will make it anonymous and keep it from being used as trial evidence. This assumption has proved false. The trend is to treat more and more social media information as the user's public appearance.

The privacy argument is the most common objection made when social media is requested during discovery or introduced at trial. Courts have not been receptive to privacy objections.[32]

In *Guest v. Leis*, the court held that users of social media "logically lack a legitimate expectation of privacy in materials intended for publication or public posting."[33] Similarly, in *Yath v. Fairview Clinics*, the court held that users' information posted on social media is public information.[34]

In *Roman v. Steelcase, Inc*., the plaintiff allegedly fell off a defective desk and suffered various injuries while working.[35] During her deposition, the plaintiff stated she suffered permanent injuries causing her to be bedridden and to undergo multiple surgeries.

The defendant's discovery requests asked for access to "private" portions of the plaintiff's Facebook and MySpace sites. But in fact, the defendant found that the plaintiff's "public" information conflicted with her statements of being bedridden and unable to enjoy life. It showed that she was living an active life and included pictures of her traveling to Florida and Pennsylvania during a time when she claimed her injuries prevented her from doing so. The plaintiff objected to the discovery request on privacy grounds and argued that the release of the information would violate her Fourth Amendment rights.

The court allowed the defense to access the plaintiff's "private" social media content, stating "[p]laintiffs who place their physical condition in controversy, may not shield from disclosure material which is necessary to the defense of the action."[36] The plaintiff voluntarily posted the information on her social media profile and was now trying to deny access by claiming the material was privileged. Because the plaintiff "knew that her information may become publicly available, she [could not] now claim that she had a reasonable expectation of privacy."[37]

MANY BELIEVE THAT CHANGING THEIR SETTINGS TO "PRIVATE" OR RESTRICTING CONTENT WILL KEEP IT FROM BEING USED AS TRIAL EVIDENCE. THIS ASSUMPTION HAS PROVED FALSE.

The court reasoned that, "when [p]laintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites or they cease to exist."[38]

When subpoenas are served directly to the social media website, users have been successful at asserting their right to privacy under the Stored Communications Act. *Crispin v. Christian*

26. Ed Finkel, *Building Your Case with Social Media Evidence*, 102 Ill. B.J. 276, 277 (June 2014).
27. *Midwest Trust Services, Inc. v. Catholic Health Partners Services*, 910 N.E.2d 638, 643 (2009).
28. *Boyd v. Travelers Insurance Co.*, 166 Ill. 2d 188, 195 (1995), *as modified on denial of reh'g* (June 22, 1995).
29. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).
30. Finkel, *supra* note 26, at 277.
31. *Id*.
32. See, *e.g*., *E.E.O.C. v. Simply Storage Mgt., LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).
33. *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001).
34. *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 43-44 (Minn. Ct. App. 2009).
35. *Romano v. Steelcase Inc*., 907 N.Y.S.2d 650, 650 (Sup. Ct. 2010).
36. *Id*. at 652, 657.
37. *Id*. at 657.
38. *Id*.

Audigier, Inc. is the seminal case dealing with "private" social media being exempt from discovery requests sent directly to social media service provides.[39]

In *Crispin*, the defendant served subpoenas on Facebook and MySpace seeking plaintiff's "private" communications. The plaintiff moved to quash the subpoenas by arguing the Stored Communications Act protects users' "private" communications.

The court considered the differences between "private" communications and wall postings used on social media websites and held that "private" communications were protected under the Stored Communications Act because only the sender and chosen recipient could view the messages. The court prohibited direct subpoenas to social media website requesting users' "private" communications.

The court, however, was unable to decide whether wall posts were "private" communications, because users are able to restrict access through their privacy settings. The court stated wall posts are not entirely "private" and remanded this portion of the subpoena to "develop a fuller evidentiary record regarding plaintiff's privacy settings."[40]

Note that the right to privacy under the Stored Communications Act is applicable in a very limited context. It attaches only when a subpoena is sent directly to social media websites providers, such as Facebook, for "private" information.

Generally, the right to privacy is a weak argument against a discovery request for a user's "private" social media. Courts have held there is no inherent right to privacy for "private" information on social media websites.[41] Objecting to social media discovery requests on relevancy grounds is a much stronger argument. IBJ

---

39. *Crispin v. Christian Audigier, Inc*., 717 F. Supp. 2d 965, 981-82 (C.D. Cal. 2010).
40. *Id*. at 981-82.
41. See, *e.g*., *E.E.O.C. v. Simply Storage Mgt., LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).