New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 248—NO. 65
TUESDAY, OCTOBER 2, 2012

FEDERAL E-DISCOVERY

Authenticating Social Media Evidence

By **H. Christopher Boehning** | And **Daniel J. Toal**

The influence of social networking sites like Facebook, Twitter, LinkedIn, and MySpace has exploded in recent years. So perhaps it should come as no surprise that social media is increasingly playing a significant role in federal and state court decisions. Such evidence has been used in cases ranging from trademark infringement[1] to sexual harassment[2] to worker's compensation,[3] often to devastating effect.

In *Romano v. Steelcase*, for example, the plaintiff claimed that she sustained permanent injuries that left her largely bedridden. In an effort to rebut these claims, the defendant sought to discover and introduce pictures from plaintiff's Facebook and MySpace accounts that post-dated the alleged debilitating injury and yet showed her "smiling happily in a photograph outside the confines of her home."[4]

Similarly, in *Targonski v. Oak Ridge*, the plaintiff in a hostile environment sexual harassment case who complained of sexual rumors circulating about her in the workplace testified: "I'm a Christian and I strive really hard to be a moral person. So for someone to start thinking of me as someone who has orgy parties at my house while my son is home, that's severely humiliating to me."[5] The defendant attempted to show that the rumors could not have been subjectively offensive to the plaintiff given posts from the plaintiff's Facebook page that discussed orgies to be filmed by her husband. And the number of court decisions relying on social media evidence is only growing.[6]

Because social media is often stored on remote servers, is accessed through unique interfaces, can be dynamic and collaborative in nature, and is uniquely susceptible to alteration and fabrication, evidentiary standards developed for other types of electronically stored information (ESI) may not be adequate. Chief Magistrate Judge Paul W. Grimm—a leading expert on electronic evidence—writes that "[a]s electronic evidence becomes more ubiquitous at trial, it is critical for courts to start demanding that counsel give more in terms of authentication, and counsel who fail to meet courts' expectations will do so at their own peril."[7] Recent court decisions also highlight the perils of presenting social media evidence without proper authentication.

In *Griffin v. Maryland*, for example, the prosecution in a murder trial had introduced printouts from a MySpace page in an effort to impeach a defense witness.[8] Although the witness—the defendant's girlfriend—testified in person, the state neglected to ask whether she wrote the thinly veiled threat against potential witnesses that appeared on her MySpace page. On appeal, the court held that the witness' picture, birthdate, and location were not sufficiently distinctive characteristics on a MySpace profile page to authenticate the printout. Because the trial court had given "short shrift" to concerns that someone other than the putative author could have accessed the account and had "failed to acknowledge the possibility or likelihood that another user could have created the profile in issue," admitting this evidence was held to be reversible error.[9]

By contrast, in *Tienda v. Texas*, the prosecution in another murder trial successfully introduced evidence from Tienda's MySpace page that tended to implicate Tienda in the shooting death of the victim.[10] There, the circumstantial evidence consisted of relevant metadata fields including Tienda's username—which was consistent with his commonly known nickname, his stated location, his user ID number, an email address registered to the account, and several photos of Tienda with date and time stamps. The court stated this was "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the Appellant and that he created and maintained them."[11]

Taken together, *Griffin* and *Tienda* demonstrate that if the characteristics of the communication proffered as evidence are genuinely distinctive, courts are likely to allow circumstantial authentication based on content and context. By contrast, if the characteristics are general, courts may require additional corroborating evidence. These cases also illustrate courts' concerns that someone other than the purported owner of the account can manipulate social media sites. Litigators can more successfully clear authentication hurdles by addressing these concerns and by carefully collecting, preserving, searching, and producing social media data in order to provide a sufficient foundation.

Authenticating Social Media

What social media may be used as evidence?

H. CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* AMY BEAUX, *an associate, assisted in the preparation of this article.*

Profile pages, public messages, digital photographs, video, chat transcripts, or private messages all potentially have critical evidentiary significance in litigation. In the relatively informal environment of social media, and often acting with the false assurance that their posts are private and ephemeral, users frequently drop their guard and act with an uncommon degree of candor. To be admitted into evidence, however, such materials still must be properly authenticated. Federal Rule of Evidence 901(a) and its state law analogs require laying a foundation of "evidence sufficient to support a finding that the matter in question is what its proponent claims." Rule 901(b) provides an illustrative list of methods by which evidence can be authenticated.

Witness Testimony. Social media sites are dynamic, complex, and may be unfamiliar to many judges. Testimony about how user profiles are created, security procedures, privacy settings, metadata, and general operation may help courts to determine whether a satisfactory foundation for authenticity has been laid. Furthermore, courts have raised legitimate concerns that social networking accounts may be hacked, fictitious accounts created, and accounts left open and unattended.[12] Testimony thus should address those concerns and also explain the degree to which the social media in question may have been vulnerable to manipulation. These considerations are important both for proffering evidence and for challenging its admissibility.

Rule 901(b) (1) allows for authentication through testimony from a witness with knowledge that a matter is what it is claimed to be. Most straightforwardly, the person who created the evidence can testify to authenticate it. Testimony also may be provided by a witness who has personal knowledge of how the social media information is typically generated. In such a case, the authenticating witness must provide "factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so[.]"[13] The social media websites themselves, law review articles, and experts can all provide this type of information.[14]

Circumstantial Authentication. When a witness is unavailable or uncooperative, proving that social media content was indeed authored by the user can be a difficult task. Rule 901(b) (4) provides that circumstantial evidence, including "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," can help to authenticate evidence. Notably, the "characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety."[15]

iSTOCK

Social networking sites can include a wealth of information, such as profile pages, posts, photographs, and video, as well as several types of metadata, some of which are not publicly visible. Different types of social media evidence will require different indicia of reliability. For example, profile pages and posts may require sufficiently distinctive data, such as references about which only the author would have known.

> Evidentiary standards developed for other types of electronically stored information (ESI) may not be adequate for social media.

For example, in *Campbell v. Texas*, the judge in a domestic violence case allowed three Facebook messages from the defendant's account that contained "unique speech patterns" and demonstrated direct knowledge of the incident at issue in the case.[16] Photographs and video from social media sites can be authenticated the usual way—by the testimony of a witness familiar with the scene depicted. But such materials generally are not self-authenticating. In a recent employment discrimination case, for example, the court excluded photographs "found and downloaded from Facebook" without more to authenticate them.[17] Attorneys can avoid such a result by providing testimony about how the photographs were collected and highlighting the distinctive characteristics of the social media pages to provide context.

Circumstantial evidence visible on the social media site, if it provides enough content and context, also may be sufficient for authentication. This could include, for example, a combination of photographs, video, comments, email addresses, and posting dates.[18] Related data from other sources also may provide context to aid authentication, including email notifications of posting activity, and computer and account usage logs. Metadata, such as location, user ID numbers, IP addresses, and when messages were created or revised can provide context as well. Moreover, presenting this authenticating evidence through video or interactive demonstration software can help accurately represent dynamic information and provide a solid foundation for authentication.

Collection and Preservation. Social media evidence is most likely to be admitted at trial when it is obtained properly in the first place. As a result, thoroughly documenting and verifying the process and results of social media data collection can help the evidence withstand authentication challenges. The simplest method is to capture and preserve static images taken from social media sites. These images may be difficult to authenticate without testimony based on personal knowledge, however.

Collecting metadata for use at trial may require specialized software. Printouts, screen captures, and most archive tools will not provide all of the

available metadata.[19] For collection of this data, e-discovery software vendors are developing tools to download and collect content to better capture and preserve the unique metadata fields associated with social media.[20] This technology can help establish authenticity by, for example, generating hash values (unique document identifiers) for collected social media items and automatically creating collection logs.

More Admissibility Issues

Ethical Considerations. Collecting data from social networking sites can also raise ethical concerns. The public or semi-public nature of social networking sites allows litigators to collect information without formal discovery. In fact, in the course of informal discovery, lawyers may even send "friend requests" to Facebook users *if* they use their real names and profiles. The New York City Bar states that "ethical boundaries to such 'friending'… are not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements."[21] A conservative Philadelphia Bar Association advisory opinion, however, requires that an attorney or agent also disclose the reason for making the friend request.[22]

Essentially, attorneys must take care to avoid conduct that could be considered "pretexting" or deceptive as proscribed by state rules of professional conduct. This guidance provided by state bar associations is not binding, but does suggest best practices that will help attorneys avoid ethical pitfalls that may taint evidence and destroy admissibility.

Hearsay. Beyond the unique issues of authentication and ethics, social media evidence also must clear evidentiary hurdles such as relevance and hearsay. Such issues, however, are generally more susceptible to traditional reasoning and evidentiary standards. In a previous column we noted that electronic communications, such as emails, lend themselves to novel uses of hearsay exceptions.[23] Hearsay is an out-of-court statement offered to prove the truth of the matter asserted. Exceptions include present sense impressions, excited utterances, and then-existing mental, emotional, or physical conditions.[24] Facebook status updates, public posts, chat transcripts, Tweets, and more lend themselves well to such exceptions. Litigators who keep these exceptions in mind may be able to find creative ways to overcome the hearsay hurdle to admissibility.

Conclusion

The ubiquity of social networking sites and the amount of personal information they contain make them a fertile source of potential evidence. However, the cloud-based, transient, and collaborative nature of these sites poses challenges unique to these media. At the start of a case, litigators should consider methods of data collection that will help to ensure authentication. Carefully documenting the process of data gathering, and using sophisticated software where necessary, will help to ensure that the fruits of discovery are not excluded from evidence due to a failure of authentication.

Social networking sites can include a wealth of information, such as profile pages, posts, photographs, and video, as well as several types of metadata, some of which are not publicly visible.

1. See, e.g., *Amerigas Propane v. Opinion d/b/a PissedConsumer.com*, No. 12-713, 2012 WL 2327788 (E.D. Penn. June 19, 2012) (using evidence from Twitter account).

2. See, e.g., *Tafuto v. N.J. Institute of Technology*, No. 10-cv-4521 (PGS), 2012 WL 1247145 (D.N.J. April 13, 2012) (using Facebook posts to substantiate sexual harassment claim).

3. See, e.g., *Clement v. Johnson's Warehouse Showroom*, 2012 Ark. App. 17 (Ark. Ct. App. Jan. 4, 2012) (holding that pictures of plaintiff "drinking and partying" on Facebook and MySpace were admissible to support termination of worker's compensation benefits).

4. *Romano v. Steelcase*, 907 N.Y.S.2d 650, 654 (N.Y. App. Div. 2010).

5. *Targonski v. Oak Ridge*, No. 3:11-CV-269, 2012 WL 2930813, at *1 (E.D. Tenn. July 18, 2012).

6. See "Published Cases Involving Social Media Evidence (First Half of 2012)," http://www.x1discovery.com/social_media_cases.html (last visited Sept. 17, 2012).

7. Paul W. Grimm, et al., "Back to the Future: *Lorraine v. Markel American Insurance Co.* and New Findings on the Admissibility of Electronically Stored Information," 42 Akron L. Rev. 357, 366 (2009).

8. 19 A.3d 415 (Md. 2011).

9. Id. at 423. See also *Connecticut v. Eleck*, 23 A.3d 818 (Conn. App. Ct. 2011) (affirming trial court's exclusion from evidence of a printout of defendant's Facebook account due to inadequate authentication).

10. 358 S.W.3d 633 (Tex. Crim. App. 2012).

11. Id. at 645.

12. See, e.g., *Tienda v. Texas*, 358 S.W.3d 633 (Tex. Crim. App. 2012).

13. *Lorraine v. Markel Am. Ins.*, 241 F.R.D. 534, 555-56 (D. Md. 2007).

14. See, for example, Data Use Policy, http://www.facebook.com/about/privacy/ (last visited Sept. 20, 2012); Heather Griffith, Understanding and Authenticating Evidence from Social Networking Sites, Wash. J. L. Tech. & Arts 209 (Winter 2012).

15. Fed. R. Evid. 901, Advisory Comm. note, Ex. 4.

16. *Campbell v. Texas*, No. 01-11-00834-CR, 2012 WL 3793431 (Tex. App. Aug. 31, 2012).

17. See *Burchette v. Abercrombie & Fitch Stores*, 08 CIV. 8786 RMBTHK, 2010 WL 1948322 (S.D.N.Y. May 10, 2010).

18. See, e.g., *Tienda*, 358 S.W.3d 633 (holding that a combination of numerous photographs of the appellant with his unique tattoos, references to specific events, the user having been electronically monitored for a year—coupled with photographs of the appellant "lounging in a chair displaying the ankle monitor"—and messages from the account sent by a user going by the nickname of the appellant was sufficient internal evidence for authentication.) See also *Griffin v. Maryland*, 19 A.3d 415 (Md. 2011) (holding that admitting printouts from MySpace into evidence was reversible error due to failure to authenticate).

19. See, John Patzakis, Key Facebook Metadata Fields Lawyers and eDiscovery Professionals Need to be Aware of (Oct. 11, 2011), http://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of/ (last visited Sept. 17, 2012).

20. Id.

21. Obtaining Evidence From Social Networking Websites, Formal Opinion 2010-2, (New York City Bar Ass'n 2010).

22. Professional Guidance Committee, Opinion 2009-02, (Philadelphia Bar Ass'n, March 2009).

23. H. Christopher Boehning & Daniel J. Toal, Overcoming Evidentiary Hurdles, NYLJ, Technology Today (Oct. 23, 2007).

24. Fed. R. Evid. 803.