
# Social Networking Sites and the Requirement of Authentication

By Kimberly K. Seibert and Robert J. Seibert

With the escalating popularity of social networking, trial lawyers face new challenges relating to the admissibility of evidence obtained from social networking sites. This article discusses authentication techniques for common types of electronic evidence available through such sites.

Facebook, MySpace, and Twitter are among the most popular social networking sites offering free accounts to users. To date, Facebook has more than 1 billion monthly active users,[1] Twitter has an estimated 500 million registered users,[2] and MySpace has exceeded 25 million users.[3] Social media usage is growing at a rate three times that of overall Internet usage.[4] Users devote 22.7 percent of their online time to social networking sites.[5] Approximately half of Facebook users visit the site daily.[6] In 2010, Facebook surpassed Google as the most visited website in the world.[7]

These sites contain several forms of electronic communication in a single interface, a feature that makes them appealing to users but presents new challenges to trial attorneys seeking to admit their content. Evidence can include information posted on profile pages, postings between users, private messages, photographs, and videos. The sites require each user to create a unique login and password; they do not, however, employ security measures for verifying the identity of the individual creating or accessing the account.

## The authentication requirement

An attorney seeking to introduce evidence from social networking sites must first overcome the evidentiary hurdle of authentication. Under Michigan Rule of Evidence 104(a), the issue of whether to admit evidence at trial is a preliminary question to be decided by the court. A bedrock condition of admissibility is that the proffered evidence is relevant to an issue in the case.[8] If the proffered evidence is not relevant, it is not admissible under any circumstances.[9]

Evidence has no relevance if it cannot be authenticated. MRE 901(a) defines authentication as a "condition precedent" to admissibility requiring the proponent to make a threshold showing that it would be "sufficient to support a finding that the matter in

question is what its proponent claims." Whether the proponent has met this threshold is one of the preliminary questions of admissibility addressed by Rule 104(a).

Determining authenticity is a two-step process. First, "[b]efore admitting evidence for consideration by the jury, the [trial] court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic."[10] Then, "because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims."[11] In making its preliminary determination as to admissibility, the court may consider inadmissible evidence except evidence with respect to privilege.[12]

To establish authenticity, the proponent need not rule out "all possibilities inconsistent with authenticity, or…prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication, and hence for admissibility, is one of reasonable likelihood."[13] Rule 901(b) provides by way of illustration examples of authentication or identification conforming with the requirements of Rule 901(a). The most likely illustrations to apply to social networking sites include:

- Rule 901(b)(1): Testimony of Witness with Knowledge
- Rule 901(b)(3): Comparison by Trier or Expert Witness
- Rule 901(b)(4): Distinctive Characteristics and the Like
- Rule 901(b)(7): Public Records or Reports
- Rule 901(b)(9): Process or System

## Application of the authentication requirement

Although numerous cases involve the discoverability of electronic records, few decisions analyze the evidentiary issues associated with electronic evidence. Once counsel has obtained the records through discovery, the next hurdle is determining whether they are admissible in evidence. As one distinguished jurist noted, "[I]t makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence…."[14]

Any lawyer wrestling with the admissibility of evidence from social networking sites is advised to read *Lorraine v Markel American Insurance Company*,[15] widely regarded as the watershed opinion concerning the admissibility of various forms of electronically stored or transmitted information. Although examined under the Federal Rules of Evidence, the analysis is identical under the Michigan Rules of Evidence.

The *Lorraine* decision identifies the following evidentiary issues that must be addressed to assess the admissibility of electronically stored evidence:

> Whether ESI [electronically stored information] is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence…the following evidence rules must be considered: (1) is the ESI relevant as determined by Rule 401…; (2) if relevant under 401, is it authentic as required by Rule 901(a)…; (3) if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801….[16]

### Review of Michigan caselaw

Despite the widespread use of social networking sites, only two cases in Michigan have addressed issues of authentication as they relate to such evidence. In 2010, the Michigan Court of Appeals decided *People v Goins*,[17] which demonstrates how evidence from social networking sites may be authenticated by distinctive content and context and used to impeach a witness. In *Goins*, the defendant argued that the trial court erred in excluding the contents of a MySpace entry purportedly written by the complainant and defendant's former girlfriend, Holly Bradley. The photographs would be used to show a contrasting account of an alleged assault. The trial court refused to allow admission of the content because no evidence was submitted to verify that the MySpace account belonged to Bradley. The trial court affirmed this ruling even after the defendant testified that he met Bradley through MySpace, he was familiar with her account, and the statement came from her account.

The Court of Appeals noted that in "what certainly appears to be Bradley's MySpace page are descriptive details of the assault that fit within what a reasonable person would consider to be 'distinctive content' not generally known to anyone other than Bradley, defendant, or someone in whom one or the other confided."[18] Given the content of the entry, which was only slightly less inculpatory than Bradley's own testimony, and the unlikelihood she would have given her account password to a third party, the Court ruled that the jury could have reasonably found that Bradley authored the content. The Court held that these indicia were sufficient for the jury to reasonably find that Bradley was the author of the MySpace content.

In *People v Mills*,[19] a jury convicted Ellis Mills of second-degree murder. Mills admitted he shot the victim, Jordan Clark, but claimed he did so in self-defense after Clark pointed a gun at him. Mills argued that the trial court erred in excluding photographs of the victim's MySpace page depicting the victim holding

**FAST FACT**

"[C]onsidering the significant costs associated with discovery of [electronically stored information], it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence…because the proponent cannot lay a sufficient foundation to get it admitted."

a black-and-silver gun. Mills did not know who photographed the victim or posted the photographs on MySpace. The Court noted that Mills had "no way of knowing if the photos were altered in any way."[20] Further, Mills could not prove the guns in the photos were actually real. The Court affirmed the lower court's ruling in excluding the photographs.

### Review of other jurisdictions

Given that few Michigan cases have considered the admissibility of evidence from social networking sites, it is helpful to review cases from other jurisdictions that have addressed the issue. In *Tienda v Texas*,[21] the Texas Court of Criminal Appeals affirmed the defendant's murder conviction, concluding that the trial court did not abuse its discretion in admitting evidence of MySpace profile pages allegedly authored by the defendant. The profile pages were provided to the prosecution by the victim's sister, who testified that she believed the defendant registered and maintained the sites. Messages contained on the profile pages included specific references to the circumstances surrounding the crime. The defendant argued that the prosecution failed to prove he was responsible for creating and maintaining the content of the MySpace pages by merely presenting the photos and quotes from the website.

Given that few Michigan cases have considered the admissibility of evidence from social networking sites, it is helpful to review cases from other jurisdictions that have addressed the issue.

In affirming the trial court's admission of the evidence, the Court of Criminal Appeals held that the internal content of the MySpace postings—photographs, comments, and music—was sufficient circumstantial evidence to establish a prima facie case that a reasonable juror could have found that the content was created and maintained by the defendant.

The Appellate Court of Illinois in *People v Downin*[22] upheld the admissibility of e-mails purportedly sent by the defendant to his underage victim in a sexual abuse case. The Court found that the prosecution authenticated the e-mails by introducing evidence that the victim knew the defendant personally, had exchanged e-mails with him in the past at an address she knew to be his, and the e-mail contained information that would have been known exclusively by the defendant.

In *State v Eleck*,[23] the Connecticut Court of Appeals upheld the lower court's refusal to admit a printout from the defendant's Facebook page. The defendant attempted to impeach the testimony of a prosecution witness who claimed she had not communicated with him since the evening of an assault that gave rise to the criminal charges. The defendant proffered messages from his Facebook page that he claimed he received from the witness. Although the witness identified the user name as her own, she denied sending the messages, explaining that someone had hacked her Facebook account and changed her password several weeks prior.

The Court explained that "proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship."[24] In this case, the witness denied authorship of the messages and testified that her account had been hacked, and there was insufficient evidence of distinctive characteristics to authenticate the messages.

The Supreme Court of Massachusetts recently ruled that there was insufficient evidence to authenticate MySpace messages allegedly sent by the defendant's brother to a friend of the defendant. In *Commonwealth v Williams*,[25] the Court found it significant that there was no testimony regarding how secure the web page was, who could access the MySpace page, or whether codes were needed for access to the page. In short, "[t]here was no basis for the jury to conclude that the statements from the MySpace page were generated, adopted, or ratified by the defendant or, indeed, that they had any connection to him."[26]

In *People v Clevenstine*,[27] the New York Supreme Court held that the prosecution offered ample testimony to authenticate numerous instant messages from the defendant's MySpace account involving the defendant and sexual abuse victims. A legal compliance officer for MySpace testified that the messages on the defendant's computer had been exchanged by users of accounts created by the defendant and the victims, and the defendant's wife recalled that the sexually explicit conversations she viewed in her husband's MySpace account were on their computer.

## Practice pointers

The potential for fabricating or tampering with electronically stored information on social networking sites poses significant challenges from the standpoint of authentication of printouts of the site. The current trend is to require more evidence than just a distinctive profile page to authenticate a specific posting or message on the social networking site. As explained by the Court in *Griffin v State*:[28]

> [W]e recognize that other courts, called upon to consider authentication of electronically stored information on social networking sites, have suggested greater scrutiny because of the heightened possibility for manipulation by other than the true user or poster.[29]

Some or all of the following forms of authentication should be used when attempting to introduce evidence from social networking sites:

- Testimony from the creator of the profile and relevant postings
- Testimony from the person who received the message
- Testimony about the distinctive aspects in the messages revealing the identity of the sender
- Testimony regarding the account holder's exclusive access to the account
- Testimony from the social networking website connecting the post to the person who created it

The rules concerning authentication are flexible and offer a variety of methods for validating evidence from social networking sites. Authenticating such evidence is in large part no different from authenticating more traditional forms of evidence. Whether seeking to admit hard copies of photos, videos, correspondence, accident reports, or information from social networking sites, the trial attorney must offer sufficiently reliable proof that the proffered evidence is what he or she claims it to be. ■

*Kimberly K. Seibert is a member of Plunkett Cooney's Insurance and Professional Liability Department who focuses her practice in the areas of motor vehicle negligence and no-fault law. She is a graduate of the University of Michigan and Wayne State University Law School.*

*Robert J. Seibert is a principal in Seibert and Dloski, PLLC. He is a graduate of Western Michigan University (cum laude) and Wayne State University Law School (cum laude).*

## ENDNOTES

1. Smith, Segall & Cowley, *Facebook reaches one billion users* <http://money.cnn.com/2012/10/04/technology/facebook-billion-users/index.html>. All websites cited in this article were accessed June 24, 2014.
2. Halliday, *MySpace adds 1m new users in 30 days* <http://www.guardian.co.uk/technology/2012/feb/14/myspace-one-million-users>.
3. Bennett, *Twitter on Track for 500 Million Total Users by March, 250 Million Active Users by End of 2012* <http://www.mediabistro.com/alltwitter/twitter-active-total-users_b17655>.
4. The Nielsen Company, *State of the Media: The Social Media Report Q3 2011*, available at <http://blog.nielsen.com/nielsenwire/social/>.
5. *Id.*
6. *Id.*
7. MediaLiteracyClearinghouse <http://www.frankwbaker.com/mediause.htm>.
8. MRE 401.
9. MRE 402.
10. *United States v Branch*, 970 F2d 1368, 1370 (CA 4, 1992).
11. *Id.* at 1370–1371.
12. MRE 104(a).
13. *United States v Holmquist*, 36 F3d 154; 168 (CA 1, 1994).
14. *Lorraine v Markel Am Ins Co*, 241 FRD 534, 538 (D Md, 2007).
15. *Id.*
16. *Id.* at 538.
17. *People v Goins*, unpublished opinion per curiam of the Court of Appeals issued January 21, 2010 (Docket No. 289039).
18. *Id.* at *2.
19. *People v Mills*, unpublished opinion per curiam of the Court of Appeals issued March 24, 2011 (Docket No. 293378).
20. *Id.* at *13.
21. *Tienda v Texas*, 358 SW3d 633 (Tex Crim App, 2012).
22. *People v Downin*, 828 NE2d 341 (Ill App Ct, 2005).
23. *State v Eleck*, 23 A3d 818 (Conn App Ct, 2011).
24. *Id.* at 822.
25. *Commonwealth v Williams*, 926 NE2d 1162 (Mass, 2010).
26. *Id.* at 1173.
27. *People v Clevenstine*, 891 NYS2d 511 (NY App Div, 2009).
28. *Griffin v State*, 19 A3d 415 (Md, 2011).
29. *Id.* at 424.