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

Admissibility of Social Media Evidence in Illinois

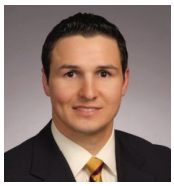
Social media evidence is generally admissible in Illinois – so long as the proper requirements are met. This article reviews the law governing the admissibility of social media evidence and how to lay proper foundation in Illinois.

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 a recent graduate of Chicago-Kent College of Law practicing in the areas of personal injury, criminal law, and family law.*

khasan@BHLattorneys.com



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

mgould@rblaw.net

IS SOCIAL MEDIA EVIDENCE ADMISSIBLE IN ILLINOIS? The short answer is yes, if the proper requirements are met. However, there's some uncertainty about what the proper requirements are in Illinois. This article looks at the law governing the admissibility of social media evidence and how to lay proper foundation in Illinois.

People v. Nunn, an unpublished opinion, addresses the admissibility of social media evidence in a criminal case.[1] In *Nunn*, the defendant was found guilty of first-degree murder. On appeal, he argued that the trial court erred in denying his request "to admit a printout of the actual Facebook message conversation into evidence at trial."[2] He argued "the messages should have been admitted because they could have been properly authenticated and were relevant and material to...defendant's claim of self-defense."[3]

The Illinois Appellate Court held that the trial court abused its discretion by failing to admit the Facebook printout. "One of the basic principles in the law of evidence is that what is relevant is generally admissible. Evidence is relevant if it has any tendency to make the existence of a material fact more or less probable than it would be without the evidence...."[4] The Facebook conversation went directly to an element of the crime – specifically, the conversation supported the defendant's self-defense claim and his theory that he did not intend to rob the victim and no robbery had occurred.

In Illinois, a number of cases have addressed the admissibility of other types of electronic evidence, such as text messaging or email. It appears that Illinois courts have analyzed the

1. *People v. Nunn*, 2016 IL App (3d) 140137-U.
2. *Id.* at ¶ 27.
3. *Id.*
4. *Id.* at ¶ 31.

admissibility of electronic evidence under the same standards used for "hard copy" documents. *People v. Chromik* illustrates what some Illinois courts have considered when evaluating the admissibility of electronic evidence, which presumably includes social media evidence.[5]

In *Chromik*, the defendant teacher was charged with aggravated criminal sexual abuse of a minor, one of his students. On appeal, he argued that the trial court committed reversible error when it allowed into evidence a document containing the transcription of text messages between the defendant and victim.

The defendant invoked several commonly used arguments against the admissibility of electronic evidence, stating, "no proper foundation for the document existed to allow the document into evidence,…it was not properly authenticated, and…its admission violated the best evidence rule."[6] On the authentication issue, he further argued "there was no way to establish who actually sent the text messages and whether the messages were accurately transcribed."[7]

Addressing the admissibility of text message evidence, the Illinois Appellate Court held that the trial court did not abuse its discretion in admitting the transcripts. The *Chromik* court analyzed the admissibility of the electronic evidence under the same standards used for "hard copy" documents, noting that the analysis applies for emails as well.[8]

Authentication: The requirements of Illinois Rule of Evidence 901(a)

The *Chromik* court addressed the admissibility question in two parts. First, the court addressed whether the foundation and authentication requirements were met.

When determining whether a document is authenticated, Illinois courts look to Illinois Rule of Evidence 901(a), which explains "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that *the matter in question is what its proponent claims*."[9] The question of authenticity is a preliminary determination by the judge pursuant to Illinois Rule of Evidence 104(b).

A document may be authenticated by direct or circumstantial evidence.[10] Illinois Rule of Evidence 901(b) provides some examples of how a party can establish that "the document is what it purports to be," such as "testimony of a witness with knowledge" and the identification of "distinctive characteristics and the like."[11]

In *Chromik*, the document introduced into evidence "purported to be a transcription created by the principal that recounted the messages as read to him by the victim."[12] Despite the fact that some words on the transcript were changed via the word processor's spell-check feature, the court held that the authentication requirement was met by virtue of the circumstantial evidence. The circumstantial evidence presented included (a) records from the phone company indicating that the state's text message transcripts contained the accurate date and time each text message was sent from the defendant to the victim, and (b) the victim's testimony as to the content of the messages, the accuracy of which was acknowledged in part by the defendant.

The relevancy requirement of Rules 401 and 402

Next, the *Chromik* court addressed whether the relevancy requirement was met. Under the Illinois and Federal Rules of Evidence, relevant evidence is generally admissible. "Relevant evidence" is that which has "*any* tendency to make the existence of *any* fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."[13]

In *Chromik*, the court quickly found that "the substance of the messages contained relevant evidence including defendant's attempts to get [the victim] to change her story."[14] As courts have repeatedly held, the relevancy threshold is generally low.[15] When electronic evidence is not admitted, it is usually for reasons other than relevance, as discussed below.

5. *People v. Chromik*, 408 Ill. App. 3d 1028 (3d Dist. 2011).
6. *Id.* at 1046.
7. *Id.* at 1047.
8. *Id.* at 1047-48.
9. *Id.* at 1046-47 (citing Ill. R. Evid. 901(a)) (emphasis added).
10. *Id.* (citing *People v. Towns*, 157 Ill. 2d 90 (1993)).
11. Ill. R. Evid. 104(b).
12. *Chromik*, 408 Ill. App. 3d at 1047.
13. Ill. R. Evid. 401, 403 (emphasis added).
14. *Chromik*, 408 Ill. App. 3d at 1046-48.
15. See, *e.g.*, *United States v. Aranda-Diaz*, 31 F. Supp. 3d 1285, 1289 (D.N.M. 2014).

TAKEAWAYS >>

- Social media evidence is admissible in Illinois, but there is some uncertainty as to what the proper admissibility requirements are. It appears that Illinois courts have been analyzing the admissibility of electronic evidence under the same standards used for "hard copy" documents.

- There is currently no clear standard for how to authenticate electronic evidence. In light of recent decisions, lawyers presenting electronic evidence in Illinois should err on the safe side and prepare to meet strict authentication requirements.

- The easiest way to lay the proper foundation for electronic evidence is through witness testimony from the person who created the electronic document or maintains the evidence in its electronic form. If a witness is unavailable or uncooperative, circumstantial evidence can also be used.

THERE IS STILL NO CLEAR STANDARD FOR HOW TO AUTHENTICATE ELECTRONIC EVIDENCE, SO ILLINOIS LAWYERS SHOULD ERR ON THE SAFE SIDE AND PREPARE TO MEET STRICTER REQUIREMENTS.

Admissibility hurdles

While there is limited guidance from Illinois case law about the foundation requirements for admitting electronic evidence, the Illinois Rules of Evidence, Federal Rules of Evidence, and cases from other jurisdictions are instructive about how Illinois attorneys and courts should proceed. One well-known decision addressing the admissibility of electronic evidence is Maryland-based federal Magistrate Judge Paul W. Grimm's opinion in *Lorraine v. Markel American Insurance Co*.[16]

Judge Grimm stated that electronically stored information (ESI) is admissible only when all of the relevant evidentiary "hurdles" are cleared.[17] Specifically, when ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered:[18]

1. Relevance: is the ESI relevant as determined by Rule 401?

2. Authentication: if relevant under 401, is it authentic as required by Rule 901(a)?

3. Hearsay: if the ESI is offered for its substantive truth, is it hearsay as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804, and 807)?

4. Best Evidence Rule: is the form of the ESI being offered as evidence an original or duplicate under the original writing rule or, if not, is there admissible secondary evidence to prove the content of the ESI (Rule 1002)?

5. Probative Value: is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by Rule 403 such that it should be excluded despite its relevance?

As with any piece of evidence, electronic/social media evidence must satisfy the relevancy requirement of Rule 401, pass the balancing test of Rule 403, and conform to many other rules of evidence. While hearsay issues do sometimes arise, they can often be overcome by Illinois Rule of Evidence 801(d)(2), which provides exceptions for opposing party statements, present sense impressions, excited utterances, and then-existing mental, emotional, or physical conditions.[19]

The main concern: Authenticity

While there is much to be said about the admissibility of electronic evidence, the rules likely to be the source of most challenges are those on authentication, Rules 901 and 902. As discussed, authentication is critical because without a sufficient showing that the object offered into evidence is what it purports to be, the court will not get to the other evidentiary issues.

In *Lorraine*, Judge Grimm recognized that authenticating ESI presents a number of concerns because "technology changes so rapidly" and is "often new to many judges."[20] Unlike letters or hard copy documents, ESI is stored on remote servers, is accessed through unique interfaces, is often the product of collaboration, and is uniquely susceptible to alteration and fabrication.

Social media evidence has garnered the most distrust. As one court explained, "[t]he concern arises because anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password."[21] Another concern is that regardless of whether the information is genuine or fabricated, it is "available by performing a Google search... forever," giving the impression that it is accurate and true.[22]

A split among the courts: Higher v. less stringent standards

The increased potential for fabrication has struck a nerve with a number of courts, leading to higher standards of authentication in certain jurisdictions. A recent decision by the highest court in Maryland is illustrative of the point. In *Griffin v. State*, the defendant was charged with and convicted of murder arising out of a shooting.[23] At trial, the state sought to introduce the defendant's girlfriend's MySpace profile to show that prior to trial, the girlfriend had threatened one of the state's witnesses.

At trial, the investigator testified that he printed the profile page, he could match up the birthdate on the posting with the girlfriend's date of birth, and he could identify the girlfriend in the picture. Maryland's high court held that because the trial court had given "short shrift" to the concerns that someone else could have accessed the MySpace account, it was reversible error to admit the social media evidence.[24]

The court further explained that social media evidence "requires a greater degree of authentication" given the potential for abuse and manipulation.[25] In that regard, one court explained that to rule on authentication it needed to first hear testimony about how secure the social media website was, who could access it, and whether codes were needed to get access.[26]

By way of contrast, numerous other state and federal courts have held that social media printouts and messages can be authenticated simply with the testimony of a person who has knowledge of the creator of the social media profile.[27] And to complicate matters further, some

16. *Lorraine v. Markel American Insurance Co*., 241 F.R.D. 534 (D. Md. 2007).
17. *Id.* at 538.
18. *Id.*
19. Ill. R. Evid. 801(d)(2), 803.
20. *Lorraine*, 241 F.R.D. at 541.
21. *Griffin v. State*, 19 A.3d 415, 421-22 (Md. 2011).
22. *Id.*
23. *Id.*
24. *Id.* at 423.
25. *Id.*
26. *Commonwealth v. Williams*, 926 N.E.2d 1162, 1172 (Mass. 2010).
27. See, *e.g.*, *Lorraine v. Markel American Insurance Co*., 241 F.R.D. 555 (D. Md. 2007).

courts have suggested that the possibility of fabrication should be "a mere factual question to be considered by the trier of fact rather than a bar to authentication."[28]

In sum, the cases demonstrate that there is no clear standard for how to authenticate electronic evidence. In light of recent decisions, lawyers presenting electronic evidence in Illinois should still err on the safe side and prepare to meet stricter requirements.

How to lay proper foundation

As discussed above, Federal Rule of Evidence 901(a) and its state analogs require laying a foundation "sufficient to support a finding that the matter in question is what its proponent claims."[29] Rule 901(b) sets forth a non-exclusive list of 10 methods by which evidence can be authenticated.

While the list was prepared with more traditional forms of evidence in mind, most of the listed methods of authentication are easily applied to electronic evidence. The two most applicable methods are illustrated in Rules 901(b)(1) and 901(b)(4).

Witness testimony. Rule 901(b)(1) allows for authentication through the testimony of a witness with knowledge that a matter is what it is claimed to be. For non-electronic documents, the witness providing such testimony may be the person who drafted the document or who is responsible for maintaining the record. For electronic evidence, the witness providing such testimony may be the person who created the electronic document or maintains the evidence in its electronic form.

Generally, a witness authenticating electronic evidence 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."[30] As pointed out by *Griffin*, the "most obvious method [of authentication] would be to ask the purported creator if she indeed created the profile and also if she added the posting in question."[31]

Testimony of that kind by the creator would probably be sufficient in Illinois. In *Complete Conference Coordinators, Inc. v. Kumon North America, Inc.*, the court held that testimony under oath by the purported author of an email was sufficient to meet the authentication requirement.[32]

Circumstantial authentication. When a witness is unavailable or uncooperative, proponents of electronic evidence can attempt to authenticate a document through circumstantial evidence. Rule 901(b)(4) permits exhibits to be authenticated or identified by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." The commentary to Rule 901(b)(4) states "[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety."

For example, if the creator of a profile or message does not testify, an expert or a site representative can be called to show that the social media or other electronic evidence originated from a particular computer or person. The authentication requirement could be established if a computer forensic firm (or some other expert) searched the computer of the person who allegedly created the profile and posting and examined the computer's internet history and hard drive "to determine whether that computer was used to originate the social networking profile and posting in question."[33]

Tienda v. Texas provides another illustrative example of how metadata, such as location, user ID numbers, IP addresses, and so forth can also be used to link people to a computer at a specific time and place.[34]

AUTHENTICATION IS CRITICAL BECAUSE WITHOUT A SUFFICIENT SHOWING THAT THE OBJECT OFFERED INTO EVIDENCE IS WHAT IT PURPORTS TO BE, THE COURT WILL NOT GET TO THE OTHER EVIDENTIARY ISSUES.

Conclusion

Social media evidence is hardly the novelty it was only a few years ago. Many cases now hinge on the admissibility of Facebook and other social media posts.

Clearly, authentication is the central concern for those seeking to admit or challenge social media evidence. While Illinois case law is sparse, this article suggests some strategies lawyers can use in approaching the evidentiary issues that arise in this evolving area of law. IBJ

28. *Id.*
29. Fed. R. Evid. 901(a).
30. *Lorraine*, 241 F.R.D. at 545.
31. *Griffin v. State*, 19 A.3d 415, 427 (Md. 2011).
32. See *Complete Conference Coordinators, Inc. v. Kumon North America, Inc.*, 394 Ill. App. 3d 105 (2d Dist. 2009).
33. *Griffin*, 19 A.3d at 423.
34. *Tienda v. Texas*, 358 S.W.3d 633, 635 (Tex. Crim. App. 2012).

ISBA RESOURCES >>

- Gabriel Reilly-Bates, Richard Y. Hu, and Claire E. Brennan, *New Rules for Discovery of Electronically Stored Information*, 102 Ill. B.J. 480 (Oct. 2014), https://www.isba.org/ibj/2014/10/newrulesdiscoveryelectronicallystor.
- 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.