37-SPG Fam. Advoc. 28

Family Advocate
Spring, 2015

Feature

AUTHENTICATING FACEBOOK POSTS, PHOTOS, AND OTHER EVIDENCE

Melanie K. Reichert[a1]

Your client's estranged spouse files for disability maintenance. She claims she can't work. Her long-term struggles with ruptured disks, sciatic nerve pain, and back spasms (all likely the results of her three grueling and difficult pregnancies, years of carrying those children everywhere, and even more years of tirelessly cooking and cleaning) require surgery and months of physical therapy. She may never return to 100 percent of her previous "normal." Discovery yielded two boxes of medical records showing steroid injections, chiropractic visits, and prescriptions galore.

You know she's embellishing. You beg your client to hire an expert to refute her claims. One look at the expert's retainer agreement, however, and your client balks. "My wife has played tennis twice a week and has maintained a gym membership throughout the marriage. Surely that's enough to refute her disability claims," your client says. Your hands are tied, and you're so frustrated with your client that you can't see straight. Trial is in two weeks.

Then, your client's third cousin calls. She's still "friends" with her soon-to-be ex-cousin-in-law on Facebook. The wife unfriended your client, his parents, his siblings and their spouses, his dear friends, and co-workers, but she completely overlooked the cousin.

The wife just updated her cover photo--a gorgeous picture of her current vacation in the Bahamas, looking fit and toned in a swimsuit, with her hair blowing in the breeze--riding bareback as her huge horse gallops in the surf.

Now what? How do you use this glorious information at trial?

During the past 20 years, social media and electronic communication have revolutionized the manner in which ***29** people form and maintain relationships--especially their intimate and familial relationships. Thus, it is no surprise that those who litigate or negotiate the transitions of family relationships must account for ever-changing technology. Despite the permeation of social media and electronic communications and numerous published cases and articles regarding admissibility, some domestic relations judges, arbitrators, mediators, and attorneys still develop a "deer in the headlights" look when presented with electronic evidence. They allow words such as "spoliation" and "hacking" to diminish the reliability and importance of electronic evidence.

Start with the law

When facing a legal dilemma, start with the rule of law. Here, we begin with Federal Rule of Evidence

authentication rules that mirror the language of the federal rule. The portions of FRE 901 relevant to electronic information state:

Rule 901. Authenticating or Identifying Evidence

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

(b) Examples. The following are examples only--not a complete list--of evidence that satisfies the requirement:

(1) *Testimony of a Witness with Knowledge*. Testimony that an item is what it is claimed to be.

(3) *Comparison by an Expert Witness or the Trier of Fact*. A comparison with an authenticated specimen by an expert witness or the trier of fact.

(4) *Distinctive Characteristics and the Like*. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

(9) *Evidence About a Process or System*. Evidence describing a process or system and showing that it produces an accurate result.

Authentication is that simple--providing evidence that supports a finding that the item is what you purport it is. Attorneys who err in admitting electronic evidence tend to overthink authentication and assume that some sort of ironclad proof is required.

A witness with knowledge

The most common evidence that supports a finding that an item is what it is purported to be is testimony of a witness with knowledge. In the example of the horseback-riding invalid, that testimony would be from your client's third cousin. As soon as you learn of the new profile picture, ask the witness to take and print several screen shots of the wife's Facebook account--especially her newsfeed, her profile page, and the album showing prior profile pictures. If the new profile picture is part of an album of other vacation photos, a screen shot of that album would be helpful as well.

At trial, ask the cousin questions to establish the Facebook relationship she has had with Wife. How long have they been Facebook friends? Is she familiar with Wife's activity on Facebook? Does the profile information from the printout match what the cousin personally knows about Wife? With the printouts, ask the cousin questions similar to those you would ask when authenticating photographs. What steps did the cousin take to produce the printouts? Do the printouts accurately reflect what the cousin viewed on Wife's Facebook page on the date in question?

In this example, the testimony cannot come from your client if he did not have the ability to view the relevant portions of Wife's Facebook page at the time she changed her profile picture. The fact that Wife "unfriended" him would not, in and of itself, necessarily preclude him from viewing her page, her profile, and her photos. However, assuming her security settings are sufficient, your client would not be a "witness with knowledge" unless he accessed the account and produced the screen shots.

party then serves as your "witness with knowledge." For example, use interrogatories to ask for all e-mail accounts opened or utilized by a party, the e-mail address to which communications are primarily sent and received, the contact information that appears on the screen of the mobile device used when calling or texting, and the user names for any and all social media accounts. A string of tweets from a Twitter handle matching that identified in responses to interrogatories should be deemed sufficiently authenticated.

Requests for admissions are invaluable tools when authenticating electronic evidence. Requests can include admissions that a printout of a Facebook page accurately reflects the party's newsfeed or profile on a certain date, that a string of text messages is complete and accurate, or that the party sent a particular e-mail. With the admissions, ***30** include interrogatories and requests for production that ask the responding party to state reasons for any denials or to produce what he or she purports to be true and accurate copies of the communications.

To further authenticate Facebook information, include in your requests for production a request for a complete activity log with instructions to the answering party on how to produce the same. (*See* "How to Produce the Facebook Activity Log" on page 29.) Obtaining the activity log helps to rebut any allegations that an account has been hacked. In our case study, Wife may claim that someone else changed her profile picture using a photo of someone who looks like her from a distance. However, Wife's credibility is damaged if the log activity immediately before and after the profile picture change shows common practices for Wife or acts not likely to be those of a hacker ("liking" a picture of her sister's dog, a status update that she just scheduled parent/teacher conferences, etc.).

Of course, depositions should be dedicated to authenticating any electronic evidence you may offer at trial or to lay the foundation to later impeach the party with the electronic evidence. Ask the deponent to log into his or her social media account from a computer during deposition and review any activity with him or her.

Comparison by an expert or trier of fact

Using comparison to authenticate is most commonly associated with handwriting. Experts and lay witnesses can look at two handwriting samples and testify as to whether they believe both samples were written by the same person. The same principles apply to electronic evidence.

Comparing an e-mail, text, or post in question to those the witness admits are hers can authenticate the offered evidence. For example, if one denies sending a scathing e-mail to her spouse, yet that e-mail mirrors the same tone, grammar, or spelling errors as innocuous e-mails she admits to sending, the trier of fact should find the e-mail sufficiently authenticated. Similarly, screen shots of text messages can be compared to the actual phone while a witness testifies.

With a copy of the Facebook activity log or copies of a series of tweets, the pattern of social media behavior can be compared to the evidence to ascertain whether the witness, or someone else, likely authored the post or tweet.

If you plan to authenticate using comparison, knowing your trier of fact is essential. Not all judges are sufficiently "tech savvy" to confidently authenticate by comparison. In those jurisdictions, retaining an expert to testify regarding the comparison method and her opinions based on methodology may be prudent.

Distinctive characteristics

witness that the evidence is not authentic. The admission of electronic evidence has been affirmed in numerous states and jurisdictions when the communications, viewed in light of all the circumstances, featured characteristics that rebutted the witness's claim that information was forged. Michigan State law student, Scott Milligan, provides criminal case summaries in a 2013 blog post. (See "Case Studies" box at left.) Evaluating these cases provides a list of distinctive characteristics (such as profile pictures, unique writing patterns or spellings, or facts only known by the poster) that can be offered to courts in authenticating social media posts and other electronic evidence.

Evidence about a process or system

As a means of authenticating electronic evidence, family law attorneys likely will not turn first to replicating the process ***31*** or system. However, authenticating electronic evidence in this manner is especially powerful if the evidence remains online and readily accessible.

Blog posts tend to be especially susceptible to this form of authentication. When entering litigation, parties remember to edit their Facebook pages and to delete disparaging tweets.However, they tend to forget that late night blog post on www.MothersOfAbusedChildren.com, the antisocial rant on www.MilitiasUnite.org, or late-night musings regarding the beneficial effects of giving Vicodin to a colicky three-month-old on www.BabiesSuck.net.

Offer a printout of the blog or post. As authentication, hand the witness a laptop computer or tablet and ask him to type in the URL of the blog post lurking in cyberspace. When the blog appears with the full name or e-mail address (or photo) of the poster, the post is authenticated.

Public or business records available online also can be authenticated with evidence of process or system. For example, replicate a search of the county recorder's database to authenticate an assessment and tax information for the marital residence. Authenticate related matters pending in other states by providing the court with the URLs for chronological case summaries. If the electronic evidence has not been deleted, witnesses can be asked to log into their Facebook or e-mail accounts to confirm authenticity.

Refuting authenticity

What if you represent the horseback-riding invalid who claims her Facebook account was hijacked? Many of the discovery and authentication tips noted above also can help prove fraud or forgeries.

Make sure that the proffered evidence can actually be authenticated pursuant to FRE 901and object when it cannot. Is the sponsoring witness someone with knowledge? Based on the security settings of the Facebook user, only certain individuals may have actual knowledge of the content on a given day. If the sponsoring witness could not have accessed the electronic content, that person cannot offer testimony with knowledge.

The comparison method also helps to dis-authenticate certain electronic evidence. When seeking to prove that electronic evidence is not what it purports to be, again, think of the methods used with other more traditional forms of evidence. For example, if a client alleges that a medical record has been doctored, test the allegation by reviewing the records for inconsistencies. The same is true of electronic evidence.

If Facebook evidence is being offered to suggest that a client "liked" pornographic material related to children, review the complete Facebook activity log and obtain a forensic examination of the client's computer hard

an argument can be made that the activity cannot be sufficiently authenticated when compared to other aspects of that client's digital footprint.

A parent in a paternity case might create a false Facebook profile for the other parent, posting inappropriate things. Again, the activity log provides insight into the legitimate nature of the page. Has there been any activity since page creation? Is there any personal information or "distinctive characteristic" on the page or in the profile? Are the language patterns consistent between the page and known writings of the parent?

When your client denies the post, e-mail, or text, ask for her computer and mobile devices. Then retain an expert to examine those devices for evidence of hacking or spyware. Proof of hacking has been sufficient grounds to exclude electronic evidence. A Google search for "social media forensic experts" yields numerous advertisements and links to professional websites. Law enforcement (both local and federal) utilize experts in criminal matters and also can be good starting points to locate qualified experts who have already testified in your jurisdiction.

As the old saying goes, however, an ounce of prevention is worth a pound of cure. Include in your engagement letter a recommendation that your client disable or deactivate (but not delete) all social media accounts while the case is pending. At the very least, security settings should be such that only "friends" or those specifically authorized, can view social media information. Request that, absent an absolute emergency, all communication with the other party be via one e-mail address. Ask that either you or a neutral (CASA, GAL, parenting coordinator) be copied on those e-mail communications. Having a second recipient virtually eliminates the likelihood that altered versions of the communications will be offered as evidence.

As with all evidence decisions, the admission or exclusion of electronic evidence is at the broad discretion of your local judges. Initiate dialogues in your legal community so that the bench and bar can share their perspectives on proper authentication of electronic evidence.

Authentication is but one of the evidentiary landmines you must navigate when offering evidence--electronic or otherwise. Be aware of hearsay and relevance objections. Lastly, please remember that being able to admit electronic evidence doesn't mean you should.No trier of fact wants to see 156 Instagram selfies in an evidence binder.

How to Produce the Facebook Activity Log

1. Access the Facebook account from a computer or Web browser (rather than a tablet or smartphone app).

2. Click on the downward-facing carrot in the upper-right corner of the user's Facebook page and scroll down to "Activity Log." The log will populate recent activity, which can be printed from the Web browser.

If a log of activity prior to the time that is automatically populated must be produced, use the timeline located on the right side of the activity log to access and print earlier activity.

--M.K.R.

Case Studies

Identifying distinctive characteristics

message, and each message contained his photo. Thus "the appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances may be sufficient to [authenticate pieces of evidence]."

Campbell v. Texas (Tex. Ct. App. 2012). Facebook messages authenticated and admitted as (1) the messages contained Defendant's unique speech patter (the defendant spoke in a Jamaica dialect); (2) the communications referenced the underlying nature of Defendant's charge known to only a few people; (3) Campbell indisputably used the Facebook account; (4) only he and one other person had access to the account; and (5) the messages at issue contained Campbell's electronic signature.

California v. Archuletta (Cal. Ct. App. Apr. 9, 2013). The court held that the fact that Facebook sites are password protected would allow a reasonable jury to conclude that the person whose page it is authored the posts.

Tienda v. Texas (Tex. Crim. App. 2012). A combination of different factors sufficiently authenticated the MySpace page. These factors included: (1) the numerous pictures of Tienda on the page that displayed his unique tattoos; (2) the reference to the victim's death and details about the victim's funeral; (3) a connection between the MySpace page and an e-mail address resembling Tienda's name; and (4) witness testimony speaking to the MySpace subscriber reports.

Illinois v. Mateo (Ill. App. Ct. 2011). The court held that the extensive corroborating circumstances surrounding the identity of the victim and Defendant as authors of messages on MySpace properly authenticated the correspondence.

Burgess v. State (Ga. Apr. 29, 2013). The court held that MySpace content was properly authenticated because the State confirmed Defendant's use of a nickname used repeatedly on the page, the defendant's sister confirmed that Defendant used the name, and an officer compared known pictures of the defendant to pictures on MySpace and determined the person to be the same.

California v. Zamora (Cal. Ct. App. Jan. 31, 2013). A defendant, confessing to his probation officer that he used and operated the MySpace page, properly authenticated the content of the page for trial purposes.

--M.K.R.

Footnotes

a1 **MELANIE K. REICHERT** has focused her practice on family law since joining the Indiana Bar in 1998. She is an experienced litigator who frequently tries complicated custody matters, jurisdictional issues, child and spousal support, allegations of child abuse or neglect, allegations of domestic violence, and property distribution cases. Melanie served as a part-time judicial officer in Marion County Circuit Court Paternity Division from 2001 to 2004.