The Admissibility of Social Media/Electronic Evidence in Alabama

By:

Terry McCarthy[1]

Introduction

In 2014, Allison Nichols-Gault and I published as article in Alabama Lawyer called *A Guide to the Admissibility of Social Media/Electronic Evidence in Alabama*. See 75 Ala. Law. 42 (Jan. 2014). The intent of the article was to give Alabama attorneys a general overview of evidentiary hurdles that frequently arise with admitting social media and electronic evidence such as emails, text messages, websites, and posts from social media accounts such as Facebook and Twitter.

At the time the article was published in 2014, while this type of evidence was routinely being introduced in Alabama trial courts, the Alabama appellate courts had not yet really weighed in on admissibility requirements for such evidence. Fortunately, the Alabama appellate courts have spoken to these issues on a few occasions in the last few years, as have courts from other jurisdictions. The purpose of this article is to update the 2014 article with some of those sources.

---

[1] Terry McCarthy is a partner at the Birmingham law firm of Lightfoot, Franklin & White, and is co-author of the Third Edition of *Gamble's Alabama Rules of Evidence* and the forthcoming Seventh Edition of *McElroy's Alabama Evidence*. He is a member of the Alabama Rules of Evidence advisory committee, and has taught evidence courses at Birmingham School of Law, Cumberland School of Law, and The University of Alabama School of Law. He may be reached at tmccarthy@lightfootlaw.com.

Evidentiary Issues with Electronic Evidence

As was the case with the 2014 article, it should go without saying that, 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 many other well established rules of evidence. This article, however, will focus on the rules that typically will pose the most challenges: (1) authentication; (2) hearsay; and (3) (to a much lesser extent) the best evidence rule.

I. Authentication

A. Alabama Rules of Evidence and Civil Procedure

As with any tangible piece of evidence such as a document, recording, photograph, or object, electronic/social media evidence must be authenticated. That is, the proponent of the evidence must lay a specific foundation to show the piece of evidence is what it is purported to be. Ala. R. Evid. 901(a). Traditionally, the authenticity bar is not a high one, and the evidence does not have to be conclusive or overwhelming. Ala. R. Evid. 901(a) advisory committee's note. The proponent is required to make a threshold showing "sufficient to support a finding that the matter in question is what its proponent claims." Ala. R. Evid. 901(a).

Despite the traditionally low bar to establish a piece of evidence as authentic, some courts have subjected electronically stored information to greater scrutiny than more traditional evidence. As the Mississippi Supreme Court has observed, "anyone can create a fictitious [social media] account and masquerade under another person's name," and "anyone…can gain access to another's account by obtaining the username and password." Smith v. State, 136 So. 3d 424, 432 (Miss. 2014) (holding that trial court

abused its discretion in admitting social media posts; error, however, was harmless). In short, "[c]reating a Facebook account is easy," as is any other social media account. Id. Thus, it has been said that "[t]he authentication of social media poses unique issues regarding what is required to make a prima facie showing that the matter is what the proponent claims." Id.

The result of this is that courts will often require two steps for social media type evidence to be authenticated if the relevance of the evidence depends on whether a particular person is the author/poster. First, the proponent must lay a predicate that the piece of evidence (Facebook post, tweet, etc.) is what it is purported to be, i.e., something from the account/phone/email address of the subject person. Second, the proponent must lay a predicate to link the post/chat/email/tweet to the relevant person, i.e., a showing that a juror could reasonably believe that the subject person actually authored it.

It should be noted that this two step authentication requirement is not unique to social media, and has technically been in play long before social media and electronic evidence became prevalent. A letter purportedly handwritten by the defendant saying he committed the crime, for example, would go through a similar authentication analysis – the proponent must show what it is purported to be and link it to the defendant. Indeed, in the original edition of Gamble's Alabama Rules of Evidence, published long before social media came about, Dean Gamble stated as follows: "Any party offering writings, objects, and other real or demonstrative evidence must lay a foundation to show that it is what the offering party purports it to be. If the claim is that the evidence was sent, authorized, used or acted upon by a particular person then preliminary evidence must be

introduced warranting a finding of the truth of that claim." Charles W. Gamble, Gamble's Alabama Rules of Evidence, § 901(a) (1st ed. 1996).

Even though Alabama appellate decisions on the admissibility of electronic evidence are still somewhat evolving, the Alabama Rules of Evidence and Alabama Rules of Civil Procedure provide ample authority for authenticating this evidence. The most prevalent sources of authority are Ala. R. Evid. 901 (done with a testifying witness); Ala. R. Evid. 902 (self-authenticating evidence); Ala. R. Evid. 201 (Judicial Notice); and Ala. R. Civ. P. 34 and 36 (Requests for Production and Requests for Admission).

Rule 901

The general rule of authentication is found in Ala. R. Evid. 901(a), which states the authentication requirement "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Ala. R. Evid. 901(b) goes on to list 10 examples of how evidence may be authenticated with a testifying witness. When authenticating electronic evidence with a live witness, the following methods are the most logical choices:

Rule 901(b)(1) – Testimony of a witness with knowledge

Rule 901(b)(1) states that a witness with knowledge may authenticate an item of evidence with "[t]estimony that a matter is what it is claimed to be." Ala. R. Evid. 901(b)(1). Traditionally, the testimony of a witness with firsthand knowledge has been "[t]he primary vehicle for establishing authentication or identification." Charles W. Gamble, Terrence W. McCarthy, & Robert J. Goodwin, Gamble's Alabama Rules of

Evidence, § 901(b)(1) (3d ed. 2014). For example, if someone personally observes another person sign a document, such testimony would be sufficient to authenticate that document. Id. Further, an individual who witnesses a murder could possibly authenticate the murder weapon.

While there appear to be no reported appellate decisions in Alabama that address a witness authenticating social media/electronic evidence under Rule 901(b)(1), "federal courts outside Alabama construing the parallel federal rule routinely find electronic evidence to be properly authenticated by a witness with knowledge." Gamble's Alabama Rules of Evidence, § 901(b)(1), Practice Pointer 6 (citing U.S. v. Bansal, 663 F.3d 634, 667-68 (3rd Cir. 2011) (website screenshots properly authenticated under Fed. R. Evid. 901(b)(1) by witness with knowledge); U.S. v. Gagliardi, 506 F.3d 140 (2d Cir. 2007) (chat room conversation properly authenticated by witness with knowledge of the chat); U.S. v. Kassimu, 188 Fed. Appx. 264 (5th Cir. 2006) (holding that computer records of post office could be authenticated by a witness with personal knowledge)).

By way of example, here is how the Rule 901(b)(1) foundation might be established with a witness who authored the item of evidence at issue:

Q. Can you please identify this document marked as Exhibit 10?

A. This is a printout of a post from my Facebook wall the night of the party.

Q. Who authored this post?

A. I did.

Q. Has it been altered or edited in any way?

A. No.

Q. So is this a true and accurate copy of the Facebook post that you posted the night of the party?

A. Yes.

The substance of Rule 901(b)(1) is the same under both the Alabama and Federal Rules, so these federal cases are persuasive authority in Alabama state courts. Ala. R. Evid. 102, advisory committee's note. Thus, authentication through a witness with knowledge should remain the predominant vehicle to authenticate evidence, electronic or otherwise.

Rule 901(b)(4) – Distinctive characteristics and the like

901(b)(4), which is patterned after the corresponding federal rule, allows a court to consider "distinctive characteristics and the like" when deciding whether a piece of evidence, electronic or otherwise, is authenticated. Ala. R. Evid. 901(b)(4). Under this method, an item of evidence "may be authenticated or identified upon the basis of its possessing distinctive characteristics which, when combined with accompanying circumstances, furnish a basis for reasonably concluding that the evidence is what the offeror purports it to be." Gamble's, at § 901(b)(4). See e.g., Royal Ins. Co. of America v. Crowne Investments, Inc., 903 So. 2d 802, 808-10 (Ala. 2004) (distinctive characteristics of letter and report, such as being written on company letterhead and referring to key dates and events, held to indicate authenticity). In other words, the court will ultimately decide, based on the totality of the circumstances, whether a reasonable juror could conclude that the evidence is what it is claimed to be. If so, the evidence is authenticated.

The types of "distinctive characteristics" offered depend on the facts and circumstances at issue. If an email is being offered against a defendant, for example, some of the "distinctive characteristics" might be testimony that the defendant frequently used the email address at issue, the defendant attended a later meeting that had been scheduled in the email, or the email included topics of discussion unique to the knowledge of the defendant. As long as the proponent can offer enough circumstantial evidence that a reasonable juror could conclude the evidence is authentic (See Ala. R. Evid. 104(b)), the authentication hurdle is cleared.

While Rule 901(b)(4) is not frequently cited in Alabama appellate decisions, it "is one of the most frequently used to authenticate email and other electronic records." Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007). It has been used, for example, to authenticate emails, text messages, chat room conversations, and other types of electronic evidence. See e.g., U.S. v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (email properly authenticated by circumstantial evidence, including the defendant's email address, content, use of defendant's nickname, and testimony of a witness who spoke to the defendant about the subject of the email); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp.2d 1146, 1153-54 (C.D. Cal. 2002) (website posts ruled authentic due to circumstances); Tienda v. State, 358 S.W. 3d 633 (Tx. Ct. Crim. App. 2012) (content of postings on defendant's social media web page was sufficient circumstantial evidence to attribute the postings to the defendant in a prosecution for murder).

Although emails have been around for many years and are routinely offered into evidence in Alabama courts, no Alabama appellate court had "directly addressed the

proper authentication of emails" until 2014 in Culp v. State, 178 So. 3d 378, 384 (Ala. Crim. App. 2014). Consistent with decisions across the country, the Alabama Court of Criminal Appeals held in Culp that the subject emails were properly authenticated based on their distinctive characteristics and the like.

In Culp, the court concluded that, in accordance with Rule 901(b)(4), that the e-mails at issue were properly authenticated under Rule 901(b)(4) as having been sent by the defendant. The defendant's girlfriend testified that the defendant sent her the e-mails, that she assisted him in setting up his e-mail account, that each e-mail contained the defendant's photograph and screen name, that many of the e-mails concluded with the defendant's initials, and that the e-mails contained code words uniquely used by the defendant and his girlfriend for referencing methamphetamine. Thus, there was enough circumstantial evidence to authenticate the emails.

Soon after Culp was decided, in Smith v. Smith, the Alabama Court of Civil Appeals quoted Culp extensively in this child custody case and found there was enough circumstantial evidence to authenticate the emails and text messages at issue under Rule 901(b)(4). See Smith v. Smith, 196 So. 3d 1191 (Ala. Civ. App. 2015). The emails and text messages at issue allegedly involved the mother asking a witness named Rettig for prescription pain medication. At trial, Rettig testified that the emails and text messages were sent between her and the mother. In addition, the court looked to the "totality of the emails and the text messages and the circumstances under which they were sent," including the tone and syntax, the fact that the mother admitted the phone number was hers, and that Rettig and the mother made plans to do things and clearly responded to

each other's messages. There was enough circumstantial evidence to support the trial court's ruling that they were admissible.

Finally, in Municipal Workers Compensation Fund, Inc. v. Morgan Keegan & Company, Inc., 190 So. 3d 895 (Ala. 2015), the Alabama Supreme Court relied upon Rule 901(b)(4) to rule that website materials were properly authenticated. See also, Knight v. State, CR-16-0182, 2018 WL 3805735, at *22 (Ala. Crim. App. Aug. 10, 2018) (Not Yet Released For Publication) (while not specifically mentioning Rule 901(b)(4), holding that copies of defendant's Facebook page with pictures of El Camino were properly authenticated; detective testified that page was under defendant's nickname, it included pictures of defendant, defendant told detective he wanted an El Camino, and detective testified that screen shots had not been altered or changed); Mun. Workers Comp. Fund, Inc. v. Morgan Keegan & Co., Inc., 190 So. 3d 895 (Ala. 2015) (holding that website printouts, which lacked Web addresses and dates, were properly admitted "[b]ecause [] the highly technical nature of the financial documents" shown in the printouts constituted strong enough "distinctive characteristics . . . in light of the circumstances" to meet ALA. R. EVID. 901(b)(4)).

Rule 902(5) -- Self authentication of Official Publications

"Some written forms of demonstrative evidence are deemed to be self-authenticating." Gamble's, at § 902. This means that the item of evidence may be authenticated without the sponsoring testimony of a witness. While most of the items discussed above (i.e., chats, text messages, and Facebook postings) will not have self-

authenticating status, some forms of internet based evidence can have self-authenticating status.

The primary example is Rule 902(b)(5), which gives self-authenticating status to "[b]ooks, pamphlets, or other publications purporting to be issued by public authority." Ala. R. Evid. 902(b)(5). While no Alabama appellate decision has addressed this issue, multiple courts construing the parallel federal rule and state rules have held that printouts from government websites can be self-authenticating. See e.g., Firehouse Restaurant Group, Inc., v. Scurmont, LLC, 2011 WL 3555704, at *4 (D.S.C. 2011) ("Records from government websites are generally considered admissible and self authenticating."); Williams v. Long, 585 F. Supp.2d 679, 689 (D.Md. 2008) ("The printed webpage from the Maryland Judiciary Case Search website is self-authenticating under Rule 902(5) . . ."); Hispanic Broad Corp. v. Educational Media Foundation, No. CV027134CAS (AJWX), 2003 WL 22867633 at *5 n.5 (C.D. Cal. 2003) ("Other exhibits which consist of records from government websites, such as the FCC website, are self-authenticating."). Presumably, unless there would be some reason to question the trustworthiness of official publications from a government website, self authenticating status should be available in Alabama courts.[2]

[2] By way of example, the parallel federal rule has been found to be satisfied where: (1) the printout of the record included the website address; (2) the printout included the date on which it was printed; (3) the court verified that website; and (4) the website was maintained by a government agency. E.I. Du Pont de Nemours & Co., 2004 WL 2347559 (E.D. La. 2004).

Rule 201 -- Judicial Notice

As some types of electronic evidence become more accepted and part of society, authentication may possibly be accomplished through judicial notice. Rule 201 allows a court to judicially notice an adjudicative fact "not subject to reasonable dispute that is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Ala. R. Evid. 201(b).

Even though some judges are still somewhat skeptical of electronic evidence, it has become common for courts in many jurisdictions to take judicial notice of information published on government websites. See e.g., Pickett v. Sheridan Health Care Center, 664 F.3d 632, 648 (7th Cir. 2011) (judicial notice taken of consumer price index on government website); Kitty Hawk Aircargo, Inc. v. Chao, 418 F.3d 453, 457 (5th Cir. 2005) (judicial notice of National Mediation Board approval published on agency's website); Reeves v. PharmJet, Inc., 846 F. Supp.2d 791, 794 n. 1 (N.D. Ohio 2012) ("The Court may also take judicial notice of matters of public record including records of the FDA available on its website.").

Although Alabama appellate decisions on this issue are scarce, there is some evidence that Alabama courts are beginning to follow this trend with regard to reliable government websites. For example, in Cooper v. MTA, Inc., 166 So. 3d 106, 108 n. 3 (Ala. 2014), the Alabama Supreme Court said in a footnote that certain information relating to "Treasury Offset Program" could be found on the United States Department of Treasury website and at least implied that the Court took judicial notice of such information pursuant to Ala. R. Evid. 201(b)(2). See also, Rimpsey Agency, Inc. v. Johnson, 218 So. 3d 1242, 1243 n. 1 (Ala. Civ. App. 2016) (stating that the court "may take judicial notice of matters of public record, including records of the Secretary of State"); Petty v. Allen, 77 So. 3d 1182, 1184 n. 3 (Ala. Civ. App. 2011) (judicial notice of regulations found on Department of Corrections website); Johnson v.

Hall, 10 So. 3d 1031 , 1035 (Ala. Civ. App. 2008) (recognizing that a Kentucky appellate court in Polley v. Allen, 132 S.W.3d 223, 226 (Ky. Ct. App. 2004) observed that a court can take judicial notice of "public records and governmental documents available from reliable sources on the internet.").

Until the Alabama case law becomes more fully developed, proponents of reliable government websites have numerous federal cases to rely upon in seeking admission of this evidence. Alabama courts appear to be following this lead.

Alabama Rules of Civil Procedure

Finally, a piece of electronic evidence may be authenticated through the Alabama Rules of Civil Procedure. It has long been the rule in Alabama, for example, that a party is relieved from having to authenticate evidence that is produced by an adverse party and the party that produced the evidence is a party to it or claims a benefit thereunder. See e.g., Jordan v. Calloway, 7 So. 3d 310, 314 (Ala. 2008); Ala. Power Co. v. Tatum, 306 So. 2d 251, 258 (Ala. 1975). Furthermore, a party may take advantage of Ala. R. Civ. P. 36 (Requests for Admission) and request the adverse party to admit that a piece of evidence is genuine.

B. Examples of authenticating specific types of electronic evidence

We will now focus on specific types of electronic evidence common in litigation and address the means courts have used to authenticate these types of evidence.

Email

Email evidence is obviously very common, and authenticating an email is not difficult. Here are the most common ways:

- Rule 901(b)(1) – a witness included on the email chain can typically authenticate an email by testifying that he has personal knowledge of the email discussion and that the printout is a true and accurate copy of the email. See e.g., Navedo v. Nalco Chemical, Inc., 848 F.Supp.2d 171, 178-79 (D.P.R. 2012).
- Rule 901(b)(4) – an email may be authenticated purely by circumstances, including the email address, email suffix, whether it was a reply email, and by information contained in the email exchange. Smith v. Smith, 196 So. 3d 1191 (Ala. Civ. App. 2015) (citing Culp v. State, 178 So. 3d 378 (Ala. Crim. App. 2014), and ALA. R. EVID. 901(b)(4)) (holding, in child custody case where mother denied she was the person who sent e-mails and text messages to a friend requesting help in procuring prescription pain pills, that a review of text messages and e-mails between the mother and friend covering a wide range of topics over several months provided sufficient circumstantial evidence for admissibility; observing that the tone, syntax, and appearance of the e-mails and text messages remained consistent, and that the circumstances under which they were sent—casual conversation between friends—supported admissibility; rejecting mother's argument that authentication of e-mails and text messages required subpoenaing telephone records for the "sending phone" to see if the records reflect a message having been sent to the "receiving phone" at the same time); U.S. v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000); U.S. v. Safavian, 435 F. Supp.2d 36 (D.D.C. 2006).

- Rule 902(7) (trade inscriptions) – inscriptions, signs, tags, or labels purporting to have been fixed in the course of business and indicating ownership, control, or origin may be deemed self-authenticating. See ACCO Brands, Inc. v. PC Guardian Anti-Theft Products, Inc., 592 F.Supp. 2d 1208, 1219 (N.D. Ca. 2008).

Website Postings

Typically, it is not overly difficult to authenticate information posted on a website. A witness who actually viewed the website may testify that a printout of the website fairly and accurately depicts what was on the site when the witness viewed it. The information on the website is presumptively attributable to the owner of the website. Generally, there are three foundational questions that must be answered either explicitly or implicitly to authenticate a posting from a website:

1. What was on the website?
2. Does the exhibit or testimony accurately reflect what was on the website?
3. If so, is it attributable to the owner of the site?

Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007) (quoting Gregory P. Joseph, *Internet and Email Evidence*, 13 Prac. Litigator (Mar.2002), *reprinted in* Stephen A. Saltzburg, et al., Federal Rules of Evidence Manual, Part 4 at 20 (9th ed. 2006)).

In deciding whether to admit a website posting, the court may consider the following factors:

- The length of time the data was posted on the website.

- Whether others report having seen it.
- Whether it remains on the website for the court to verify.
- Whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations).
- Whether the owner of the site has elsewhere published the same data.
- Whether others have published the same data, in whole or in part.
- Whether the data has been republished by others who identify the source of the data as the website in question.

After considering those factors and possibly others, the court will decide whether a sufficient foundation has been established for a reasonable juror to conclude that the evidence is what it is purported to be. Mun. Workers Comp. Fund, Inc. v. Morgan Keegan & Co., Inc., 190 So. 3d 895 (Ala. 2015) (holding that website printouts, which lacked Web addresses and dates, were properly admitted "[b]ecause [] the highly technical nature of the financial documents" shown in the printouts constituted strong enough "distinctive characteristics . . . in light of the circumstances" to meet ALA. R. EVID. 901(b)(4)).

Chat Room Discussions

Chat room discussions can pose additional authentication problems that are not present with a traditional website. Chat room participants often use pseudonyms and screen names, and unlike website postings already discussed, chat room postings are made by third parties – not the owner of the website. Thus, in addition to authenticating the chat itself, the proponent of chat room evidence will often be required to link the chat

to the individual the proponent claims was a party to the chat. The first step, authenticating the chat itself, is typically done as follows:

- Rule 901(b)(1) -- a witness with personal knowledge of a chat room conversation may testify that a printout fairly and accurately depicts the chat. Adams v. Wyoming, 117 P.3d 1210 (Wy. 2005).

The second step, linking the chat to an individual who denies having participated, courts will often look to the following factors:

- Evidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question).
- Evidence that, when a meeting with the person using the screen name was arranged, the individual in question appeared.
- Evidence that the person using the screen name identified him or herself as the individual (in chat room conversations or otherwise), especially if that identification is coupled with particularized information unique to the individual, such as a street address or email address.
- Evidence that the individual had in his or her possession information given to the person using the screen name (such as contact information provided by the police in a sting operation).
- Evidence from the hard drive of the individual's computer reflecting that a user of the computer used the screen name in question.

Gregory P. Joseph, *Internet and Email Evidence,* 13 Prac. Litigator (Mar.2002), *reprinted in* Stephen A. Saltzburg, et al., Federal Rules of Evidence Manual, Part 4 at 20 (9th ed. 2006)). See also U.S. v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000) (authenticating chat

room conversation based on the following: (1) a co-conspirator testified the printout accurately depicted the chat; (2) the defendant admitted he used a screen name used in the chat; (3) co-conspirators testified the defendant used the screen name used in the chat; and (4) co-conspirators testified that they arranged for a meeting with a person who used the screen name and that the defendant appeared for the meeting).

Text messages

Text messaging is an increasingly common form of communication. Typically, a text message can be authenticated by a witness with knowledge or distinctive characteristics and the like. State v. Jaros, 2011 WL 4529312 (Ohio. App. 2011) (text messages properly authenticated by witness who identified messages sent to her cell phone from defendant's email address, as she was familiar with the email account from having received messages from him in the past). See also Gulley v. State, 2012 Ark. 368, 11-15, where text messages were authenticated based on the content of the messages, the fact that the messages were sent from a telephone number assigned to the defendant, and witness testimony that confirmed defendant's involvement in the activities described in the messages; Smith v. Smith, 196 So. 3d 1191 (Ala. Civ. App. 2015) (citing Culp v. State, 178 So. 3d 378 (Ala. Crim. App. 2014), and ALA. R. EVID. 901(b)(4)) (holding, in child custody case where mother denied she was the person who sent e-mails and text messages to a friend requesting help in procuring prescription pain pills, that a review of text messages and e-mails between the mother and friend covering a wide range of topics over several months provided sufficient circumstantial evidence for admissibility; observing that the tone, syntax, and appearance of the e-mails and text messages remained consistent, and that the circumstances under which they were sent—casual

conversation between friends—supported admissibility; rejecting mother's argument that authentication of e-mails and text messages required subpoenaing telephone records for the "sending phone" to see if the records reflect a message having been sent to the "receiving phone" at the same time).

II. Hearsay

Authentication is just one step in the analysis. Out of court statements, written and oral, must go through the hearsay analysis. Thus, before any information from cyberspace may be admitted, it must satisfy the hearsay rules. Hearsay is defined as a statement made outside the trial offered to prove the truth of the matter asserted. Ala. R. Evid. 801. To fully perform the hearsay analysis, it is necessary to know the purpose for which the evidence is offered. While hearsay is evaluated on a case by case basis, some hearsay exemptions and exceptions are more prevalent than others in the electronic evidence context.[3] Satisfying hearsay, of course, is just one evidentiary hurdle and does not guarantee admissibility.

A. Admissions

An admission of a party opponent is considered non-hearsay, and is a common way to satisfy a hearsay objection in an electronic evidence context. Ala. R. Evid. 801(d)(2). A chat room posting, Twitter, Facebook or MySpace posting, email, text

[3] Social media and other websites typically contain a significant number of photographs that could potentially be offered at trial. Because photographs are rarely considered "assertions," they are usually not excluded via a hearsay objection. U.S. v. May, 622 F.2d 1000, 1007 (9th Cir. 1980) ("a photograph is not an assertion, oral, written, or nonverbal, as required by 801(a).").

message, or website information posted by the owner of the site or account can all constitute admissions provided these items are used against the party who made the posting. See e.g., U.S. v. Burt, 495 F.3d 733, 738-39 (7th Cir. 2007) (holding that portions of chat from the defendant were party admissions and portions from the other participant were not offered for the truth of the matter asserted.); U.S. v. Hart, 2009 WL 2552347, at *4 (W.D. Ky. 2009) ("the suspect's portion of the chats contained in the chat logs are admissible as non-hearsay admissions of a party opponent under Rule 801(d)(2)."); U.S. v. Levy, 594 F. Supp.2d 427, 439 (S.D.N.Y. 2009) ("Levy's hearsay objection was not well-founded, for his statements in the transcript were not hearsay, but were statements offered by the Government against Levy as admissions of a party opponent."); Doctors Med. Ctr. Of Modesto v. Global Excel Mgmt., Inc., 2009 WL 2500546, at *9 (E.D. Cal. 2009) ("the statements from the website are party admissions, which are not hearsay and are admissible under Fed. R. Evid. 801(d)(2).").

If the person denies having made the post, that is typically more of an authentication issue than a hearsay issue. In that scenario, as discussed above, the proponent of the evidence will typically be required to make some minimal threshold showing to link the post to the individual.

B. Business Records

Ala. R. Evid. 803(6) provides a hearsay exception for records of regularly conducted activity, i.e., the business records exception. Relevant, properly authenticated website information may qualify under the business records exception, but only if the traditional business records elements are established. The website evidence offered must

be: (1) a memorandum, report, record, or compilation of data; (2) of acts, events, conditions, opinions, or diagnoses; (3) made at or near the time [of the event, condition, opinion, or diagnosis]; (4) by, or from information transmitted by, a person with knowledge; (5) kept in the regular course of business; (6) all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

The rationale underlying the business records exception is that business records have the "earmark of reliability" or the "probability of trustworthiness" because they reflect the day-to-day operations of the enterprise and are relied upon in the conduct of business. Palmer v. Hoffman, 63 S. Ct. 477 (1943). As long as the reliability threshold is met and the foundation addressed in the above paragraph is established, properly authenticated, relevant website information created and kept in the ordinary course of business can satisfy the business records hearsay exception. See e.g., U.S. v. Cameron, 762 F.Supp 2d 152, 187-89 (D. Maine 2011) (reports generated by the National Center for Missing and Exploited Children were admissible as business records, including attached contraband images); Lorraine, 241 F.R.D. at 552.[4]

C. Public Records

Many government records are considered public records and fall under the public records exception to the hearsay rule. Federal courts have frequently given the same self-

[4] Counsel should also be aware that there are several new amendments to the Alabama Rules of Evidence that are effective in proceedings that begin on or after October 1, 2013. Rules 902(11) and 902(12), which are newly added and virtually identical to their federal counterparts, provide for the self-authentication of business records. Again, this is only for those proceedings that begin on or after October 1, 2013.

authenticating status to certain government websites. Kew v. Bank of America, N.A., 2012 WL 1414978, at *3 n. 4 (S.D. Tex. 2012) ("The printout from the Harris County Appraisal District's website is a public record under 803(8)."); Bartlett v. Mutual Pharm. Co., Inc., 760 F. Supp.2d 220, 235 n. 10 (D.N.H. 2011) ("This court admitted the [Food and Drug Administration] analysis into evidence as a full exhibit, since it was a self-authenticated public record available on the FDA's website."). There is no reason to think Alabama courts should not follow suit in the proper circumstances. See Ala. R. Evid. 803(8).

D. Then Existing State of Mind or Condition

Rule 803(3) provides an exception to the hearsay rule for "[t]hen existing mental, emotional or physical condition." If a condition provided under this rule is material as to a particular witness or party, certain social media posts, chat room messages and emails can fall under this exception to the hearsay rule. For example, if a Facebook post says, "my leg hurts," or "I feel sad today," such postings could overcome a hearsay objection via Rule 803(3).

E. Present Sense Impression and Excited Utterance

Rule 803(1), the presence sense impression exception to the hearsay rule, makes it a hearsay exception for statements that describe an event while perceiving it or immediately thereafter. Ala. R. Evid. 803(1). One commentator has observed that Twitter (like Facebook) "is, in essence, a vast electronic present sense impression (e-PSI) generator, constantly churning out admissible out of court statements." Jeffrey Bellin,

Facebook, Twitter, and the Uncertain Future of Present Sense Impression, 160 U. Pa. L. Rev. 331, 335 (2012). Indeed, through the use of smart phones, Twitter, Facebook, and text messaging, users are constantly telling the world about events as they unfold (i.e., "at LSU-Bama game, and just saw the Honeybadger cheap shot Dre Kirkpatrick;" "I'm watching a great fight at the bar"). Those posts, tweets, or texts that describe an event while perceiving it or immediately thereafter, can qualify as hearsay exceptions under Rule 803(1). See e.g., State v. Damper, 225 P.3d 1148, 1152 (Ariz. App. 2010) ("On this record, we cannot conclude the superior court abused its discretion in ruling the text message constituted a present sense impression.").

Similarly, posts, tweets, or texts made under the stress and excitement of a startling event that relate to that startling event can qualify as excited utterances under Rule 803(2). Funches v. State, 2012 WL 436635, at *1 (Nev. 2012) (observing that the state argued "persuasively" that text messages were admissible under the excited utterance exception).

III. Best Evidence Rule

The best evidence rule ("BER") states that "[w]hen a party is attempting to prove the terms of a writing, the law generally requires such proof to be in the form of the original." Gamble's, at § 1002(a). There are, however, many avenues to admit secondary evidence. The BER should rarely be a problem when trying to admit electronic/social media evidence.

In Alabama, the BER applies to writings only, in contrast to the Federal Rules of Evidence where it applies to writings, recordings and photographs. Ala. R. Evid.

1001(1), which defines "writings," includes within that definition "other form of data compilation." Ala. R. Evid. 1001(1). "Use of the words 'data compilation' makes it clear that the best evidence rule is expanded by Rule 1001 to include computerized records." Ala. R. Evid. 1001(1) advisory committee's note. Under Rule 1001(2), "[t]he status of original is likewise conferred upon any computer printout." Ala. R. Evid. 1001(2) advisory committee's note. Further, Ala. R. Evid. 1004 allows secondary evidence to be used when the original is lost or destroyed (unless it was lost or destroyed in bad faith), it is not obtainable, it is in possession of the opponent, or if it involves a collateral matter.

Given the above rules, a best evidence rule objection with electronic evidence is often not very difficult to overcome. See e.g., U.S. v. Lebowitz, 676 F.3d 1000, 1009 (11th Cir. 2012) (holding that trial court did not abuse its discretion in allowing, over a best evidence rule objection, printouts of a chat conversation; recognizing that Fed. R. Evid. 1001(3) defines "original" "to include a printout of computer data shown to accurately reflect that data."); U.S. v. Lanzon, 639 F.3d 1293, 1301-02 (11th Cir. 2011) (holding that trial court did not abuse its discretion in allowing, over a best evidence rule objection, instant message transcripts, absent a showing that the originals were destroyed in bad faith); Norton v. State, 502 So. 2d 393, 394 (Ala. Crim. App. 1987) (computer printouts of electronically stored public information deemed admissible over best evidence rule objection).[5]

[5] It should be noted that in Alabama state courts the best evidence rule does not apply to photographs obtained from websites or social networking sites. Gamble's, at § 1001 (stating that the best evidence rule "has no application to nonwritten evidence such as tape recordings, photographs, and chattels.").

Conclusion

While this article has focused on authentication, hearsay, and the best evidence rule, counsel should be aware that those are not the only rules that apply to electronic/social media evidence. Obviously, any evidence offered must be relevant (Rule 401), the probative value must not be substantially outweighed by the danger of unfair prejudice (Rule 403), it must not violate the general exclusionary rule of character (Rule 404), and it must satisfy all other evidentiary hurdles.

Notwithstanding all the changes in the world of technology, those basic requirements of the evidentiary rules remain the same. And, while some courts have been skeptical of certain types of electronic evidence, such evidence may still be offered, authenticated, and analyzed under the existing Alabama and Federal Rules of Evidence. While this article is not intended to exhaust every issue that could possibly be raised, hopefully it will give the practitioner some useful tips when electronic evidence is an issue at summary judgment and trial.