**The Federal Bar Association's**
**2015 Federal Litigation Conference**

**Panel 5:**

# Admitting and Authenticating Electronic Evidence in Court, Including Trial-Like Demonstrations

**Featuring:**


**Mark H. Churchill, Esq.**
Partner, McDermott Will & Emery, LLP
**Daniel D. Mauler, Esq.**
Partner, Redman, Peyton, & Braswell, LLP
**Mark J. McLaughlin**
Digital Forensic Examiner, Computer Forensics International
**Mark K. Vincent, Esq.**
U.S. Attorney's Office, District of Utah; FBA President

**Moderator:**
**Charles B. Molster, III, Esq.**
Winston & Strawn LLP


**October 27, 2015**

# Table of Contents

## 1. OBTAINING ELECTRONIC EVIDENCE

The first issue that we will briefly address is how to obtain electronic evidence. This is an important part of the process because the nature of the electronic material – and especially the ***source*** of the material – can play a very large role in determining whether the offered electronic evidence will actually be admitted. The following are some common methods for obtaining electronic evidence:

### A. Discovery Requests (Civil Litigation Only)

The Federal Rules of Civil Procedure clearly require the identification and production of Electronically Stored Information (ESI).[1]

Document requests to a party pursuant to Rule 34 are one good source of electronic evidence, and counsel should be careful to keep such requests straightforward, reasonably narrow and easy to understand – especially so that they will be easy to enforce by the Court.

Rule 34 obviously puts significant ethical obligations on your opponent to produce ESI materials – policing the responses and enforcing those obligations can be an important – and fruitful – component of you pretrial preparations.

In view of the cost of complying with requests for ESI, some Courts (including the Federal Circuit's "Model Order re ESI") have recently suggested and/or adopted limitations on such discovery rights.

While certain limitations on "fishing expeditions" certainly makes sense, counsel should be careful not to allow potential sources of probative electronic evidence to be shielded from discovery, and at a times may need to be prepared to rebut a showing that ESI materials are not "reasonably accessible because of undue burden or cost," or to show "good cause" to obtain materials that are found to not to be "reasonably accessible because of undue burden or cost."[2]

More and more often courts are considering the relative burdens regarding ESI discovery, and considering Protective Orders or other means to balance such burdens, including fee shifting.

### B. Self-production of Materials

One of the least expensive methods for obtaining electronic materials is to simply produce it from one's own lap top or other devices. This may raise questions regarding authenticity and the like, but many of those issues will likely go to the weight of the evidence, rather than its admissibility.

### C. Subpoenas in Civil Cases

---

[1] *See, e.g.* Fed. R. Civ. P. 26(a)(1)(A)(ii).
[2] Rule 26(b)(2)(B).

Rule 45 subpoenas can be a good source for obtaining electronic evidence from third parties, and again the Rule clearly requires that electronic materials be produced.[3]

Protective orders are also available to subpoenaed parties, as are issues relating to whether ESI materials are not "reasonably accessible because of undue burden or cost," or whether the party that issued the subpoena can show "good cause" to obtain materials that are found to not to be "reasonably accessible because of undue burden or cost."[4]

An important caveat: Civil subpoenas may not always be enforceable, especially when seeking the contents of e-mail messages stored by an Internet Service Provider (such as Google, Yahoo!, Hotmail, or Facebook) due to certain provisions of the Electronic Communications Privacy Act (aka The Stored Communications Act).[5] Courts generally quash civil subpoenas issued to third-party ISPs that seek e-mail contents.[6]

### D. Harvesting Off of the Internet

Similar to self-production, electronic materials can also be simply harvested off of the internet. Again, however, these types of materials may well raise issues of authenticity, manipulation and the like, thereby increasing the hurdles to admissibility. Generally speaking, it is best to have someone other than a party's counsel of record harvest the materials off of the internet. That way, the person can testify as a witness at a deposition or trial to authenticate the materials, if necessary. But the first attempts at authentication should be made via Requests for Admission and during deposition testimony.

#### a. The Wayback Machine, etc.

The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. The Internet Archive is a privately-run 501(c)(3) nonprofit organization that has partnered with various well-known institutions and libraries, including the Library of Congress.

The Internet Archive has created a service known as the Wayback Machine (http://archive.org/web/). The Wayback Machine makes it possible to surf more than 240 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a list of available dates. The visitor may select one of those dates, and then begin surfing on an archived version of the Web. The links on the archived files, when served by the Wayback Machine, point to other archived files (whether HTML pages or images). If a visitor clicks on a link on an archived page, the Wayback Machine will serve the archived file with the closest available date to the page upon which the link appeared and was clicked. The archived data made viewable and browseable by the Wayback Machine is compiled using

[3] *See* Rule 45(e)(1)(B)-(D).
[4] Rule 45(e)(1)(D).
[5] *See* 18 U.S.C. § 2701, *et seq.*
[6] *See, e.g.*, *Crispin v. Audigier*, 717 F.Supp. 2d 965 (C.D. Cal. 2010); *In re Subpoena Duces Tecum to AOL*, 550 F. Supp. 2d 606 (E.D.Va. 2008) (Lee, J.).

software programs known as crawlers that surf the Web and automatically store copies of website files, preserving these files as they exist at the point of time of capture.

Cases regarding admissibility of materials from the Wayback Machine have gone both ways.[7]

**b. Library of Congress Web Archives**

The Library of Congress has recently launched a new project to archive selected web sites. As its own site explains:

> The Library of Congress Web Archives (LCWA) is composed of collections of archived web sites selected by subject specialists to represent web-based information on a designated topic. It is part of a continuing effort by the Library to evaluate, select, collect, catalog, provide access to, and preserve digital materials for future generations of researchers. The early development project for Web archives was called MINERVA.[8]

The LCWA only includes selected web sites.

> The Library archives websites that are selected by recommending officers, or curators, based on the theme or event being documented. The types of sites archived include, but are not limited to: United States government (federal, state, district, local), foreign government, candidates for political office, political commentary, political parties, media, religious organizations, support groups, tributes and memorials, advocacy groups, educational and research institutions, creative expressions (cartoons, poetry, etc.), and blogs. The Library maintains a collections policy statement and other internal documents to guide the selection of electronic resources, including websites.[9]

Not only are the LCWA archives limited in scope, only a limited set of those archives are accessible online. Here is the current list of subject areas[10]:

- Brazilian Presidential Election 2010 Web Archive
- Crisis in Darfur, Sudan, Web Archive, 2006
- Indian General Elections 2009 Web Archive
- Indonesian General Elections 2009 Web Archive
- Iraq War 2003 Web Archive
- Law Library Legal Blawgs Web Archive
- Library of Congress Manuscript Division Archive of Organizational Web Sites

[7] *See Telwizja Polska USA, Inc. v. Echostar Satellite*, 2004 WL 2367740 (N.D. IL 2004) (evidence admitted); *St. Luke's Cataract & Laser Institute P.A. v. Sanderson, M.D., LLC*, 2006 WL 1320242 (M.D. Fla. May 12, 2006) (evidence not admitted, but court indicated that an affidavit from the Internet Archive would be sufficient); *Novak v. Tucows, Inc.*, 2007 U.S. Dist. LEXIS 21269 (E.D. N. Y. March 26, 2007) (evidence not admitted).
[8] *See* http://lcweb2.loc.gov/diglib/lcwa/html/lcwa-home.html
[9] *See* http://loc.gov/webarchiving/faq.html#faqs_04
[10] *See* http://lcweb2.loc.gov/diglib/lcwa/html/lcwa-home.html.

- Papal Transition 2005 Web Archive
- Philippine General Elections 2010 Web Archive
- Public Policy Topics Web Archive
- September 11, 2001 Web Archive
- Single Sites Web Archive
- Sri Lankan Presidential and General Elections 2010 Web Archive
- Timor Leste Collection Web Archive
- United States 107th Congress Web Archive
- United States 108th Congress Web Archive
- United States Election 2000 Web Archive
- United States Election 2002 Web Archive
- United States Election 2004 Web Archive
- United States Election 2006 Web Archive
- United States Election 2008 Web Archive
- United States Election 2010 Web Archive
- Visual Image Web Sites Archive

Access to other archived sites in the LCWA may be obtained onsite at the Library of Congress.

Each archive contains material from a number of sites. For example, the "Single Sites Web Archives" is a collection of archived pages from 74 sites. At a glance most of those appear to be related to historic events or people of historic significance. Similar to the Way Back Machine (the software for which is used to access the LOC archives), it only captures the pages on a few dates. *See e.g.* http://webarchive.loc.gov/lcwa0013/*/home.att.net/~rjnorton/Lincoln2.html And, as the archive titles reflect, those dates are limited to the year or years that the curators decided to document.

The LCWA has been integrated into the rest of the Library of Congress' website and the archives available online are accessible through the Library's main search function. *See* http://www.loc.gov/websites/collections/ Archived sites can also be accessed via The Library of Congress Web Archives page: http://lcweb2.loc.gov/diglib/lcwa/html/lcwa-home.html

Archived web pages accessed via the Web Archives page are marked at the top with a statement identifying it as an archived Web site from the LC collection, when it was archived (date and time down to the second), and indicating how many of the pages are contained in the archive and the date ranges:


Archived web pages accessed via the Library's main search function reflect similar authenticating information:


Unless you have a matter that relates to one of the topics that the Library of Congress has selected to document (like an election), the LCWA is unlikely to prove a better tool for gathering evidence for litigation than the Way Back Machine at the present time. But it does appear that the Library of Congress intends to expand the subject areas in which it archives in the future. And if a useful website is archived by the Library of Congress, a compelling argument can be made that a printout of the archived page is self-authenticating under FRE 902(5) as an "official publication" of the U.S. Government.[11]

### E. Issues in Criminal Cases

Electronic evidence in criminal cases usually consists of evidence obtained by law enforcement through search warrants to search a defendant's electronic media or through government-issued subpoenas to third parties pursuant to the Stored Communications Act, 18 U.S.C. § 2703. The Fourth Amendment requires the government to obtain a warrant before attaching a GPS tracking device to a defendant's vehicle[12], and that a warrant is required to search a cell phone seized at the time of arrest.[13]

Many courts have concluded that the Fourth Amendment does not apply to historical cell site location data — information that identifies where a cell phone was used based on cell tower locations — and the government needs only reasonable suspicion as required by the Stored Communications Act to obtain such data.[14] But a few courts have found that the Fourth Amendment does apply.[15]

Given the ubiquity of cell phones, the acquisition and admissibility of location data promises to be an area of substantial litigation in the future, and more and more defendants may seek to obtain cell site data from third-party providers themselves pursuant to Federal Rule of Criminal Procedure 17.

---

[11] *See Williams v. Long*, 585 F.Supp.2d 679, 688-90 (D. Md. 2008) (printouts from government websites were "self-authenticating" under FRE 902(5)).
[12] *U.S. v. Jones*, 132 S. Ct. 945 (2012).
[13] *Riley v. California*, 134 S. Ct. 2473 (2014).
[14] *See, e.g., In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *U.S. v. Graham*, 846 F.Supp.2d 384 (D. Md. 2012).
[15] *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell Site Info.*, 809 F.Supp.2d 113 (E.D.N.Y. 2011); *Commonwealth v. Augustine*, 467 Mass. 230 (Feb. 18, 2014).

## 2. THE APPLICABLE RULES OF EVIDENCE

In general, the same rules of evidence that apply to paper documents apply to electronic documents and materials.

However, because of their nature, the risk of manipulation, and questions of authorship, additional hurdles often arise as to the admissibility of electronic materials. Further, different issues arise depending on the various types of electronic evidence that are being sought to be admitted – or excluded.

This CLE will address two types of materials: 1) e-mails; and 2) social media postings.

Different courts have different standards of authenticating electronic evidence, and thus it is critical to know how your jurisdiction and/or Judge handles such matters.

### A. Competing Standards for Authenticating Social Media Evidence

The admissibility of electronic evidence, including from social media sites, turns on a number of evidentiary factors, including relevance, authenticity, hearsay and the probative value of the evidence in light of its potential for unfair prejudice.[16] Of all of these factors, authentication is often considered the "greatest challenge" for the admission of social media evidence.[17] To further complicate matters, federal and state courts have adopted divergent standards for authenticating this evidence.

This split in authority was recently highlighted by the Delaware Supreme Court in *Parker v. State*[18]. In *Parker*, the defendant, Tiffany Parker, was convicted of assaulting another woman in a fight that arose over a mutual love interest. At trial, the State sought to introduce subsequent Facebook posts that were allegedly authored by Parker to demonstrate her role in the fight, and to discredit her self-defense argument. The State authenticated the evidence using testimony of a third party who viewed the posts, as well as circumstantial evidence that the posts were written by Parker. On appeal, Parker claimed that the Facebook posts had been improperly authenticated and should have been excluded. In deciding the issue, the *Parker* Court reviewed two alternative standards for authenticating social media evidence, which the Court dubbed as the "Maryland Standard" and the "Texas Standard."

#### 1. The More-Restrictive "Maryland" Standard

Under the Maryland Standard, courts will not admit social media evidence unless the proponent of the evidence affirmatively establishes that it is authentic. This approach essentially requires the proponent to disprove the possibility that a social media post or message was fraudulently created by someone other than its purported creator. This burden applies even in the absence of proof that evidence has actually been faked.

---

[16] *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).
[17] Hon. Paul W. Grimm, *et al.*, *Authentication of Social Media Evidence*, 36 Am. J. Trial Advoc. 433, 439 (2013).
[18] *Parker v. State*, 85 A.2d 682 (Del. 2014).

*Griffin v. State* typifies this approach. In *Griffin*, the Maryland Court of Appeals held that printouts from a MySpace page could not be authenticated merely because the page contained a photo and the birthdate of the purported creator of the content.[19] Citing the "potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user," the *Griffin* court held that evidence from a social media site "requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site." The Court stated that social media evidence could be properly authenticated by: (i) asking the purported creator of the content if she in fact created it; (ii) searching the alleged creator's computer for evidence that she created the content; or (iii) obtaining information directly from the social media site that hosts the content in question.

Summarizing this line of cases, the Connecticut Court of Appeals explained that:

> The need for authentication arises in this context because an electronic communication, such as a Facebook message, an e-mail or a cell phone text message, could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Consequently, proving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship.[20]

Courts in at least three other states (Colorado, Connecticut, and Mississippi) have adopted the Maryland Standard:

- *State v. Eleck*, 23 A.3d 818, 824 (Conn. App. 2011)—affirmed trial court ruling excluding Facebook messages b/c there was no direct evidence of authorship and the content of this exchange (circumstantial evidence) did not provide sufficient distinctive characteristics to authenticate message.
- *Smith v. State*, 136 So.3d 424, 433 (Miss. 2014)—finding trial court abused discretion by admitting Facebook messages b/c there was insufficient evidence tying both the Facebook profile and the Facebook message to the purported author.
- *People v. Glover*, 2015 WL 795690, *4 (Colo. App. Feb 26, 2015)—holding that the trial court properly admitted Facebook messages where witness testimony and circumstantial evidence linked defendant to the account and messages and noting that no evidence suggested that anyone other than the defendant used the account.

### 2. The Less-Restrictive "Texas" Standard

Under the "Texas Standard," such evidence can be authenticated by introducing sufficient facts to persuade a reasonable juror that the evidence was created by the person who the

[19] *Griffin v. State*, 19 A.3d 415 (Md. 2011).
[20] *State v. Eleck*, 23 A.3d 818, 822 (Conn. App. Ct. 2011).

proponent alleges created it. Judge Paul W. Grimm (D. Md.), a leading authority on the admissibility of electronic evidence, summarized this alternative approach:

> When all that the objecting party offers is speculation or conjecture about who, other than the putative creator, 'could' have created the evidence, such questions are properly left to the jury in determining how much weight, if any, to give to the evidence—provided that the trial judge is convinced that the proponent has met the relatively low threshold required by Rule 901(a) of producing facts that would be sufficient for a reasonable jury to conclude that the evidence was created by the putative creator.[21]

*Tienda v. State* is representative.[22] In *Tienda*, the defendant was charged with murder in Texas state court. The State sought to introduce several printouts from MySpace pages allegedly used by the defendant. To authenticate the pages, the State cited circumstantial evidence of authenticity on the pages, including photos of the defendant, e-mail addresses using the defendant's name or nicknames, and messages referencing the acts in question. The Texas Court of Criminal Appeals affirmed the trial court's admission of the evidence. The Court acknowledged that "[i]t is, of course, within the realm of possibility that the [defendant] was the victim of some elaborate and ongoing conspiracy" to fabricate multiple MySpace pages.[23] "But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the [defendant], not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages."[24]

### 3. Trending Towards the "Texas" Standard

Across the nation, the trend amongst courts (both state and federal) appears to be towards the Texas Standard. One indication of this trend is a recent, April 2015 case from the Maryland Court of Appeals itself, which appears to adopt the "reasonable juror" test of the Texas Standard in principle.[25] In reality, however, the Maryland high court appears to continue with its heightened "Authentication-Plus" standard that requires additional evidence affirmatively showing that other third-parties did not produce the social media posts.

Other states appear to adopt and apply the Texas Standard in whole. For example, after reviewing both standards, the Delaware Supreme Court adopted the Texas Standard and held that "the trial judge as the gatekeeper of evidence may admit the social media post when there is evidence 'sufficient to support a finding' by a reasonable juror that the proffered evidence is what its proponent claims it to be."[26] The *Parker* Court recognized that "the concern that social media evidence could be falsified," but it determined that the Rules of Evidence already provided for this risk insofar as a juror could give the evidence as much weight as he or she thinks it deserves.

---

[21] Grimm, *et al*. *supra* note 2, at 458.
[22] 358 S.W.3d 633 (Tex. Crim. App. 2012).
[23] *Id*. at 646.
[24] *Id*.
[25] *Sublet v. State*, 442 Md. 632, 113 A.3d 695 (2015)
[26] *Parker v. State*, 2014 WL 621289, at *5.

In addition to the Delaware state court, courts in at least six other states (Tennessee, Ohio, Georgia, Kansas, Massachusetts, and Missouri) have adopted the Texas Standard:

- *State v. Burns*, 2015 WL 2105543, *12 (Tenn. Crim. App. May 05, 2015)—expressly agreeing with Texas approach.
- *State v. Gibson*, 2015 WL 1962850, *9 (Ohio App. 6 Dist. May 01, 2015)—expressly agreeing with Texas approach.
- *Burgess v. State*, 742 S.E.2d 464, 467 (Ga. 2013)—finding trial court did not abuse discretion by admitting printout from MySpace profile b/c it was sufficiently authenticated by circumstantial evidence. It was unnecessary for State to prove who owned/created profile or to subpoena website provider.
- *State v. Jones*, 318 P.3d 1020 (Table), *6 (Kan. App. 2014)—finding proper authentication of Facebook profile where defendant admitted the page was his. His denial that he authored the posts went to the weight, not the admissibility, of the evidence, and was for the jury to decide.
- *Commw. v. Foster F.*, 20 N.E.3d 967, 971 (Mass. App. Ct. 2014)—finding that trial judge did not err by admitting Facebook communications b/c sufficient evidence was presented, including "conforming circumstances," for a reasonable jury to find by a preponderance of the evidence that the defendant authored the messages.
- *State v. Snow*, 437 S.W.3d 396, (Mo. App. S.D. (2014)—finding that trial court did not abuse discretion by admitting MySpace messages b/c by reviewing the "entirety" of the message, and "considering all circumstances," it was reasonable to conclude that the defendant authored the message. Any weaknesses in the authentication evidence (*i.e.*, testimony of defendant's girlfriend that she authored message) were for the jury to weigh.

Federal courts appear to be trending towards the Texas Standard, but the careful practitioner will attempt to build as many connections as possible between the author and the exhibit:

- *United States v. Barnes*, 2015 U.S. App. LEXIS 17222 *11 (5th Cir. Miss. Sept. 30, 2015). Facebook and text messages were authenticated by a witness testifying that she had seen the defendant use Facebook and that the messages matched the defendant's manner of communicating.
- *United States v. Brinson*, 772 F.3d 1314, 1319 (10th Cir. 2014). The government successfully authenticated an individual's Facebook account by showing by a preponderance of evidence that the defendant was the individual named on the account through (1) linking the account to an email address; (2) the defendant's self-identification in a Facebook message; (3) witness testimony; and (4) matching the phone number from the defendant's car bill to the phone number on the Facebook account.
- *United States v. Vayner*, 769 F.3d 125, 132 (2d Cir. 2014). A finding that the government failed to authenticate the Russian equivalent of a Facebook page by providing no extrinsic information showing that the defendant created the page or was responsible for the contents, despite his name, picture, and some details of the defendant's life appearing on the page.

- *United States v. Lebowitz*, 676 F.3d 1000, 1009 (11th Cir. 2012). MySpace chat printouts were admissible based on witness testimony.
- *Rea v. Wis. Coach Lines, Inc.*, 2015 U.S. Dist. LEXIS 27916, *13-14 (E.D. La. Mar. 5, 2015). In deciding a motion in limine, the court states that authenticity of Instagram photos "may be established through the cooperation of a testifying witness."
- *Mould v. NJG Food Serv.*, 37 F. Supp. 3d 762, 768-69 (D. Md. 2014). On summary judgment, the court held that Plaintiff's statement that Instagram pictures are "true and correct copies of photographs that were viewed on Facebook and Instagram" was "insufficient to authenticate the photographs as substantially correct representations of the behavior they purport to represent."

### B. The Fourth Circuit: Is E-mail Not A Business Record?

In *U.S. v. Cone*[27], the Fourth Circuit indicated that e-mails present unique problems of recent vintage in the context of the business records exception, and the court referenced a Maryland District Court decision that asserted that e-mail is typically a more casual form of communication than other records usually kept in the course of business, such that it may not be appropriate to assume the same degree of accuracy and reliability. As e-mail is more commonly used to communicate business matters both internally and externally, however, more formal paper records are becoming more unusual.[28] The district court in Maryland case excluded the e-mails on the basis that "more specificity is required regarding the party's record keeping practices to show a particular e-mail in fact constitutes a reliable business record." *Id*.

The Fourth Circuit noted that while properly authenticated e-mails may be admitted into evidence under the business records exception, it would be insufficient to survive a hearsay challenge simply to say that since a business keeps and receives e-mails, then ergo all those e-mails are business records falling within the ambit of FRE 803(6)(B). "An e-mail created within a business entity does not, for that reason alone, satisfy the business records exception of the hearsay rule."[29] The Fourth Circuit stated that the district court's observation that the e-mails were kept as a "regular operation of the business" is insufficient on that basis alone to establish a foundation for admission under Rule 803(6)(B).

The Fourth Circuit concluded that the e-mails could not be admitted under the business records exception to the hearsay rule based on the record in that case. This conclusion, however, was only *dicta*, and the Fourth Circuit held that the district court's admission of the e-mails was harmless error. Based on the harmless error, the Fourth Circuit affirmed the defendant's conviction on this count.[30]

---

[27] *U.S. v. Cone*, 714 F.3d 197 (4th Cir. 2013) (Judges Agee, Wynn, and Flyod).
[28] *Id.* at 219-20 (*quoting It's My Party, Inc. v. Live Nation, Inc.*, No. JFM–09–547, 2012 WL 3655470 at *5 (D. Md. Aug. 23, 2012) (unpublished)).
[29] *Id.* (*quoting Morisseau v. DLA Piper*, 532 F.Supp.2d 595, 621 n.163 (S.D.N.Y. 2008)). But different courts have gone different ways on this point. *See, e.g., ATS Intern. Servs., Inc. v. Kousa Intern., LLC*, No. RDB-12-2525, 2014 WL 1745004, at *5 (D. Md. May 1, 2014) (authenticating emails because "business emails containing information showing the origin of the transmission and identifying the employer-company may be sufficient to authenticate an email under Rule 902(7).")); *Lorraine*, 241 F.R.D. at 554.
[30] *Id.* at 220.

### C. The Fourth Circuit: Self-Authenticating Facebook Pages and YouTube Videos

A year after *U.S. v. Cone*, the Fourth Circuit handed down another criminal case that seems inconsistent with the *dicta* of *Cone.* In *U.S. v. Hassan*[31], the Fourth Circuit affirmed a district court's ruling that a defendant's Facebook pages and YouTube videos were self-authenticating under FRE 902(11) because the exhibits were accompanied by certificates of custodians employed by Facebook and Google (the owner of YouTube).[32]

That, however, was not the end of the matter. The Government "pursuant to Rule 901" was still required to "prove that the Facebook pages were linked" to the defendants.[33] The Fourth Circuit then noted that the Facebook pages were "captured via 'screenshots,' taken at various points in time and displaying Hassan's and Yaghi's user profiles and postings. The screenshots of the Facebook pages also included photos and links to the YouTube videos. On the Facebook pages, Hassan and Yaghi had posted their personal biographical information, as well as quotations and listings of their interests. Each Facebook page also contained a section for postings from other users, on what is called a 'wall.'"[34]

The Fourth Circuit held that the government satisfied its burden of "link[ing]" the Facebook pages to the defendants by "tracking the Facebook pages and Facebook accounts to Hassan's and Yaghi's mailing and email addresses via internet protocol addresses."[35]

Significantly, the Fourth Circuit cited FRE 901(a) and the court's previous case law for the standard applied to authentication decisions: "Turning to Rule 901, subdivision (a) thereof provides that, to 'establish that evidence is authentic, the proponent need only present evidence sufficient to support a finding that the matter in question is what the proponent claims.' Importantly, the burden to authenticate under Rule 901 is not high—only a prima facie showing is required, and a district court's role is to serve as gatekeeper in assessing whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic."[36]

This application by the Fourth Circuit seems to mirror Judge Grimm's formulation in *Lorraine* and the "Texas" standard. Perhaps this decision cuts back on the *dicta* in *Cone.*

### D. Conclusion

Both the "Maryland" and "Texas" standards appear to be alive and well in courts throughout the country, but it appears the trend is to follow the Texas standard. Judge Grimm

---

[31] *U.S. v. Hassan*, 742 F.3d 104 (2014) (Judges King, Wilkinson, and Wilson)
[32] FRE 902(11) provides that a "domestic record" (usually a business record of a private entity) that is accompanied by a certification of a custodian is self-authenticating. This relatively-new rule was added in 2000.
[33] *U.S. v. Hassan*, 742 F.3d at 132-33.
[34] *Id.* at 133.
[35] *Id.* The defendants' e-mail addresses had been established earlier in the case.
[36] *Id.* (*quoting* Fed. R. Evid. 901(a) *and U.S. v. Vidacak*, 553 F.3d 344, 349 (4th Cir. 2009)).

has strongly advocated in favor of the Texas Standard, asserting that, under Federal Rule of Evidence 104(b), a judge should withdraw the question of authenticity from the jury only when "the judge finds that the evidence is clearly authentic, or clearly inauthentic, and determines that a reasonable jury could not find to the contrary." In all other cases, the question of authenticity is for the jury to decide. On the other hand, proponents of the Maryland standard are mindful of the risks apparent in evidence gathered from the Internet and the abundant opportunities for fraud or other malfeasance. Under the more stringent approach, the proponent has the burden eliminate alternative explanations for the evidence (such as affirmatively proving that an e-mail could *only* have been written by the defendant and not by third-parties). In practice, this often amounts to proving a negative, a difficult thing to do at trial.

Therefore, trial lawyers should take great care to determine which standard will apply before seeking the introduction of electronic evidence, especially electronic evidence gathered from the Internet and/or social media sites.

Moreover, a party should not assume that just because an e-mail appears to have been generated in the ordinary course of business does not mean that it is a company record. Care should be taken by the proponent in making sure that other avenues to admit e-mail are available, which includes appropriate collection of the e-mail in the first place.

## 3. PLAN FOR USING EVIDENCE AT TRIAL

### A. Use of Properly Preserved Metadata to Bolster Authenticity

Many times, the foundation for authenticating electronic records is laid by a witness with personal knowledge about a document. The use of properly preserved and collected metadata of Tweets and Social Media postings (or any other electronic documents) can be used to bolster a proponent's likelihood of having such evidence properly authenticated, especially since potential alteration of electronic records is such a significant concern. Metadata, frequently referred to as "data about data," is electronically-stored evidence that describes the history, tracking, or management of an electronic document. Metadata includes the hidden text, formatting codes, formulae, and other information associated with an electronic document.[37] Metadata for e-mail will include the e-mail address and/or names of the senders and recipients, the subject line, the date and time, and information regarding the e-mail's Internet journey if it originated outside of a particular organization.[38] One type of metadata - system metadata - reflects information created by the user, or by the organization's information management system. Such information may track the title of the document, the identification of the computer that created it, the assigned data owner, and other document 'profile' information.[39] Properly preserved metadata can be used to strengthen the position that a document is what the proponent purports it to be, and that certain individuals had access to, created, or received the document.

---

[37] *Aguilar v. Immigration and Customs Enforcement Div. of U.S. Dept. of Homeland Sec.*, 255 F.R.D. 350, 354 (S.D.N.Y. 2008).

[38] Anne Kershaw & Joe Howie, *Judges' Guide to Cost-Effective E-Discovery* at 2 (eDiscovery Institute 2010).

[39] The Sedona Conference Working Group on Electronic Document Production, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document production, p. 60 (Sedona Conference Working Group Series 2007).

With respect to Twitter, tweets have over 150 metadata fields.[40] Some key Twitter metadata fields capture the following information: timestamp for the creation date for individual tweets, the geo-location coordinates from where the tweet was sent, and the user's name.[41] For Facebook metadata, authenticating fields of information may include similar data: user ID, account ID, the date a post was created, name of a user a wall post is directed to, and a unique identifier of a message thread.[42] Tools that properly collect metadata associated with certain Twitter and Facebook content are evolving, such that raw print-outs or screen shots of this type of evidence may be less-and-less necessary. Proponents of Twitter and Facebook evidence should consider metadata as a source of information to assist in authenticating such evidence.

### B. Chain of Custody

Care must also be taken to create a defensible chain of custody record, which establishes the handling and movement of evidence during and after collection. Any mishandlings of the collection and transfer of electronic data can adversely impact the jury's weight given to the evidence.[43] Clearly establishing that data moved from point A to point B, and only from point A to point B, is important to show that data was not at risk for being tampered or altered.

### C. Use of Internal Circumstances to Authenticate Electronic Evidence

A traditional method of authenticating evidence is through testimony of a witness with personal knowledge under FRE 901(b)(1). But counsel should be aware that this is not the only method for authenticating electronic evidence. Judge Grimm lays out a number of other, effective methods for authenticating in *Lorraine*[44], and one often over-looked method is through the "Internal Characteristics" provision of FRE 901(b)(4). According to Judge Grimm, this "rule is one of the most frequently used to authenticate e-mail and other electronic records."[45]

Under FRE 901(b)(4), testimony of a witness is not necessary. Instead, the evidence is authenticated based upon the "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances."[46] Witness

---

[40] Elizabeth Dwoskin, *In a Single Tweet, as Many Pieces of Metadata as There Are Characters*, Wall St. J., June 6, 2014, http://blogs.wsj.com/digits/2014/06/06/in-a-single-tweet-as-many-pieces-of-metadata-as-there-are-characters/.
[41] *See* Paul Ford, *The Hidden Technology That Makes Twitter Huge*, Bloomberg Business Technology, Nov. 7, 2013; http://www.businessweek.com/articles/2013-11-07/the-hidden-technology-that-makes-twitter-huge.
[42] *See* John Patzakis and Barry Murphy, *Key Facebook Metadata Fields Lawyers and eDiscovery Professionals Need To Be Aware Of*, Next Gen Law and Tech Blog, (Oct. 11, 2011, 10:06 AM), http://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of/.
[43] *See Jones v. Union Pacific R.R.*, No. 1:12-cv-00771, 2014 WL 37843(N.D. Ill. Jan. 6, 2014), where reasonable chain of custody provided and video evidence was properly authenticated. The opinion quotes precedent stating chain of custody need not be prefect (*United States v. Prieto*, 549 F.3d 513, 524-25 (7th Cir. 2008)), and the possibility of a break in the chain of custody of evidence goes to the weight of the evidence, not its admissibility (*United States v. Kelly*, 14 F.3d 1169, 1175 (7th Cir. 1994)).
[44] *See Lorraine*, 241 F.R.D. at 541-62.
[45] *Id.* at 546.
[46] Fed. R. Evid. 901(b)(4).

testimony can serve as the additional "circumstances" to corroborate the authenticity, but is not strictly necessary.

Many courts have recognized the impracticality of requiring a live witness to testify that he watched the alleged author of an e-mail push the "send" button. The Seventh Circuit noted this in *U.S. v. Fluker*, a case where the authorship of an e-mail was critical.[47] The government turned to FRE 901(b)(4) to authenticate the e-mail. The Seventh Circuit affirmed the admission of the email based upon the internal characteristics of the e-mail and the surrounding circumstances:

> Our conclusion is supported by a number of factors present in the record. The emails sent to the Norwoods had the email address "mte_123@hotmail.com," with the author identified as "Hayward Borders." Even though Melvin Norwood testified that he had never met Borders before receiving the emails, the uncontroverted testimony established that Borders was an MTE Board Member. It would be reasonable for one to assume that an MTE Board Member would possess an email address bearing the MTE acronym and have the capacity to send correspondence from such an address. Moreover, the Norwoods' email address, the address Borders' emails were sent to, was the same address to which Roy III had previously sent his email correspondence regarding the Housing Program. It would also be reasonable to assume that another MTE Board Member, in this case Borders, would have the ability to discover and send emails to the email addresses of Housing Program participants.
>
> The context of the emails further demonstrates the emails' author had significant knowledge of the Norwoods' involvement with the Housing Program and MTE. The emails discuss MTE's frozen bank accounts, the purchased property being part of the A–Buyer program, and the $108,900 of equity from the Norwoods' home that MTE received from the transaction. This is all information Borders would be in a position to know and discuss with the Norwoods.

*Id.* at 999-1000.

The leading case on this point from the District of Columbia appears to be *U.S. v. Safavian*[48], a case extending out of the Jack Abramoff scandal. In that case, Judge Friedman essentially followed the "Texas" standard regarding authentication, noting that the "question for the Court under Rule 901 is whether the proponent of the evidence has offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is. The Court need not find that the evidence is necessarily what the proponent claims, but that only that there is sufficient evidence that the *jury* ultimately might do so."[49] Judge Friedman then went on to authenticate 260 e-mails offered by the government that were purportedly between Abramoff and other co-conspirators. Significantly, Judge Friedman did not rely upon a proffered affidavit from an IT custodian for technical reasons, but instead relied upon FRE 901(b)(4) and the

[47] *U.S. v. Fluker*, 698 F.3d 988, 999 (7th Cir. 2012).
[48] *U.S. v. Safavian*, 435 F.Supp.2d 36, 40 (D.D.C. 2006).
[49] *Id.* at 38 (emphasis in original) (internal citations and quotation marks omitted).

inherent characteristics of the e-mails, such as the e-mail addresses, the names used in the bodies, the signature blocks, and the discussions of identifiable matters.[50] No witness was necessary to authenticate these e-mails.

Other federal courts have relied upon the "internal characteristics" of electronic evidence plus surrounding circumstances to admit the evidence.[51] These courts then conclude that any remaining argument over the true authenticity of the evidence is reserved for the jury/fact-finder. Situations involving FRE 901(b)(4) will be fact-intensive and vary from case-to-case.

### D. Alternative Authentication Methods

Remember that FRE 901(b) is a non-exclusive list of methods to authenticate evidence. In recent cases, courts have been willing to authenticate evidence using alternative methods that are not specifically set out in the rule but that would allow a reasonable jury to conclude the evidence is authentic.[52] If the enumerated avenues for authentication under FRE 901(b) are not available to you, creativity might solve the problem (but this is best tested in a motion in *limine* well ahead of trial).

## 4. POTENTIAL OBJECTIONS:

The following are some of the objections that will likely arise during the demonstrations:

### A. Authenticity

---

[50] *Id.* at 40.

[51] *See, e.g., U.S. v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (affirming authentication of an e-mail under Fed. R. Evid. 901(b)(4) because it contained the defendant's e-mail address (which was included on another e-mail introduced by defense counsel earlier in the case), in addition to the knowledge and slang displayed in the e-mail itself). *See also Camowraps, LLC v. Quantum Digital Ventures LLC*, No. 13-6808, 2015 WL 546791, at *3 (E.D. La. Feb. 10, 2015) ("With respect to authentication, defendants have submitted affidavits of the individuals who accessed the web pages which, in combination with information available on the face of the printouts themselves, suffice to establish that the printouts are what defendants claims them to be as required by Rule 901(a) of the Federal Rules of Evidence."); *Foreword Magazine, Inc. v. OverDrive, Inc.*, No. 1:10-cv-1144, 2011 WL 5169384, at * 3 (W.D. Mich. Oct. 31, 2011) (authenticating screenshots of commercial websites based upon a combination affidavits of witnesses with personal knowledge along with "other indicia of reliability (such as the Internet domain address and the date of printout) are sufficient to authenticate these exhibits" under the Texas standard); *U.S. v. Grant*, ACM S31768, 2011 WL 6015856 at *1-2 (A.F. Ct. Crim. App. Oct. 17, 2011) ("The appearance, contents, substance, internal patterns, or other distinctive characteristics [of defendant's Facebook messages], taken in conjunction with the circumstances may be sufficient to conform with the requirements of Mil. R. Evid. 901."); *Donati v. State*, 84 A.3d 156, 173 (Md. Ct. Spec. App. 2014) (affirming authentication of e-mails under state version of Fed. R. Evid. 901(b)(4) that matched evidence (a name and e-mail address fragment) found on paper in defendant's basement). *But see U.S. v. Vayner*, 769 F.3d 125, 129-33 (2d Cir. 2014) (reversing a district court's admission of screenshots of a Russian social media website purportedly related to the defendant because there was a lack of corroborating evidence to show the defendant authored the website).

[52] *See, e.g., Nola Fine Art, Inc. v. Ducks Unlimited, Inc.*, No. 13-4904, 2015 WL 631244, at *3 (E.D. La. Feb. 12, 2015) (authenticating e-mail (introduced by plaintiff) based upon a recipient's affidavit testimony and the defendant's act of producing the e-mail in discovery); *AT Engine Controls Ltd. v. Goodrich Pump & Engine Control Systems, Inc.*, No. 3:10-cv-01539, 2014 WL 7270160, at *8 n. 12 (D. Conn. Dec. 18, 2014) (noting that a party's mere act of production in discovery implicitly authenticates a document).

Authenticity is largely governed by FRE 901(a), which basically requires that the party offering the electronic evidence to present sufficient evidence to support a finding that the proposed exhibit is what the proponent claims it to be.

Authentication is usually satisfied by the testimony of a witness with personal knowledge that the exhibit is what it claims to be (FRE 901(b)(1)), though there are other – more complicated – ways to meet the authenticity requirement.

Moreover, because electronic evidence is subject to manipulation and/or questions of authorship, authentication can become a significant issue in attempting to admit such materials into evidence.

In addition to direct evidence to establish authentication, circumstantial evidence may be used, including distinctive circumstances or characteristics under FRE 901(b)(4), such as the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all of the circumstances.

In the case of an e-mail, this might include the e-mail's context, e-mail address, domain name, personal references within the e-mail, metadata (if properly harvested and produced in electronic form), and/or previous correspondence between the parties.

In the case of a Facebook posting, this may include the content, metadata, whether the posting responded to a prior posting, any distinctive nicknames, slang, abbreviations, etc., internet address, date, and any factors that may be unique to the person claimed to have authored the posting.

It is interesting to note that The Sedona Conference's Commentary of Admissibility of Electronically Stored Information (ESI) states that "[s]ystem metadata does not constitute 'hearsay,' at least not under the Federal Rules of Evidence, because system metadata is generated by a computer without human assistance. The reason is that under the Federal Rules of Evidence 'hearsay', by definition, requires human input." The Commentary continues by stating "[a]t least one federal appeals court has determined that system metadata is not hearsay for this reason. In *U.S. v. Hamilton*[53], a criminal case involving Internet pornography, the district court admitted computer generated 'header' information (screen name, subject matter of posting, date images when posting, and IP address) over defendant's hearsay objection. The Tenth Circuit Court of Appeals upheld the trial court's determination that metadata was not hearsay and noted: [T]he header information that accompanied each pornographic image is not hearsay. Of primary importance to this rule is the uncontroverted fact that the header information was automatically generated by the computer hosting the newsgroup each time Hamilton uploaded a pornographic image to the newsgroup. In other words, the header information was generated instantaneously by the computer without the assistance or input of a person. As concluded by the district court, this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition

[53] *U.S. v. Hamilton*, 413 F. 3d 1138 (10th Cir. 2005).

of 'hearsay.' In particular, there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801."[54]

Some materials are deemed to be "self-authenticating," such as information from government websites (FRE 902(5)[55]) and "printed material purporting to be a newspaper or periodical," which should include electronic newspapers and periodicals. (FRE 902(6)).

### B. Hearsay

The basic definition of "hearsay" is an out of court statement offered for the truth of the matter asserted.

However, there is often the threshold question as to whether the statement is really being offered for the truth of the matter asserted, or for some other purpose, such as knowledge, notice, or the declarant's "state of mind." A recent Fourth Circuit opinion sheds light on this issue. In *U.S. v. Edelen*[56], the court determined that a text message sent to the defendant was not hearsay, and thus was properly admitted into evidence, because the text message to the defendant was not being used for the truth of matter asserted, but merely to identify that the defendant spoke to the sender of the text, and that the defendant had access to, and likely received, information about the victim prior to the commission of the offense. The text message was introduced through testimony of the case detective.

Another threshold question is whether the statement is an admission of a party opponent, and thus not hearsay. (FRE 801(d)(2)).

Moreover, there are numerous exceptions to the hearsay rule, including the Business records exception (FRE 803(6)) and the Public records exception (FRE 803(8)-(10)).[57]

### C. The Best Evidence Rule

The Best Evidence Rule is embodied in FRE 1002. It is often misunderstood, and its application to electronic materials is in a state of flux.

The Rule requires "the original writing, recording, or photograph" to be introduced when offered to "prove the content of a writing, recording, or photograph," unless some other exception applies. The Rule emerged at a time when documents were copied by hand and when photographs could only be reprinted by hand methods.

---

[54] The Sedona Conference Commentary on ESI Evidence & Admissibility, p. 10 (Sedona Conference Working Group Series 2008).

[55] *See Lorraine*, 241 F.R.D. at 549-51.

[56] *U.S. v. Edelen*, 561 Fed. Appx. 226 (4th Cir. 2014).

[57] The "Public Records Exception" can be particularly useful to authenticate and admit printouts or screen-shots from government websites (federal, state, or local). To do this, FRE 902(5) (stating that "[a] book, pamphlet, or other publication purporting to be issued by a public authority" is "self-authenticating") is used hand-in-hand with the similar hearsay exception of FRE 803(8). *See Lorraine*, 241 F.R.D. at 549-51.

Since electronic materials start off existing in an electronic medium, who is to say which print out is the "original" and which is not. It appears that the trend of court decisions is to consider identical copies of electronic evidence as "duplicate originals" which generally satisfied the Best Evidence Rule.[58] Given that the real concerns for the admissibility of evidence go to notions of trustworthiness and reliability, perhaps courts should focus more on authenticity than the Best Evidence Rule to perform their gatekeeping function as to electronic evidence.

### D. FRE 403

FRE 403 provides that evidence should only be excluded "if its probative value is substantially outweighed by a danger of … unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time or needlessly presenting cumulative evidence." These are very fact specific inquiries – with no hard and fast rules -- and some trial lawyers believe that trail judges tend to treat Rule 403 like obscenity – i.e., "I know it when I see it."

## 5. ADDITIONAL DISCUSSION RE: ELECTRONIC EVIDENCE:

a. Use of Requests for Admissions for Authenticity/Admissibility
   - Beware of agreeing to arbitrary limits on RFAs (there are no limits under the current Rules, though this will change in the next round of amendments).

b. Preparation of witnesses for deposition or trial re: potential social media evidence.

c. Use of electronic information for jury selection (Facebook pages, Tweets, etc.).

d. Should power point slides or other demonstratives go back to the jury and be a part of the record on appeal – why or why not? *See Verizon Directories Corp. Services v. Yellow Book USA, Inc.*, 331 F. Supp. 2d 136 (E.D.N.Y. 2004) (Weinstein, J.)

[58] *See, e.g., Cobb v. Commonwealth*, No. 1526-12-1, 2013 WL 5744363, at *4-5 (Va. Ct. App. Oct. 22, 2013) ("We conclude that . . . the Verizon Wireless records of the text messages were originals or duplicate originals for purposes of the best evidence rule . . . [T]he printout of the company's records of the text messages was an original writing, just as mechanically reproduced or photocopied documents are considered originals.").