GEORGE MASON AMERICAN INN OF COURT

ELECTRONIC EVIDENCE AND TECHNOLOGY IN THE COURTROOM

March 7, 2017

Team Members:

- **Richard D. Kelley, Esq. Moderator**
- **Jesse R. Binnall, Esq.**
- **Lousie Gitcheva, Esq.**
- **Mikhael D. Charnoff, Esq.**
- **Leslee M. Soudrette, Esq.**
- **Donald Spammer, Student Member**
- **Tim Rodriguez, Student Member**
- **Jasmine Gandhi, Student Member**
- **Meg Armstrong, Student Member**

AGENDA

- Introduction of Panel and Overview of Presentation: 7:30 – 7:40

- Presentation of Electronic Evidence Rules and Case Law: 7:50 – 8:10
  Hypotheticals of Select Electronic Evidence Rulings

    - *Wilson v. Commonwealth*, 29 Va. App. 236 (1999)
    - *U.S. v. Broomfield*, 591 Fed. Appx. 847 (11th Cir. Dec. 3, 2014)
    - *Bloom v. Commonwealth*, 38 Va. App. 364 (2001)
    - *United States v. Fluker*, 698 F.3d 988 (7th Cir. 2012)

- Technology Availability and Use in Various Local Courts: 8:10 – 8:30

    - Arlington Circuit Court
    - Fairfax Circuit Court
    - Loudoun Circuit Court
    - United States District Court for the Eastern District of Virginia (Alex. Div.)
    - Alexandria Circuit Court

    - Pros and Cons to High-Tech and Low-Tech Presentation Styles

- Adjourn—8:30

INTRODUCTION

As technology becomes more and more a part of our everyday lives, it become more and more important for attorneys to know how to recognize, capture, assess and manage the information from that technology. In addition, as attorneys recognize and capture electronic information, they must now be able to present that information to courts in not only an admissible manner, but in a medium that is both practical and effective. In short, in each case that an attorney undertakes, he or she must know what technology is involved, how it is used, how to capture and collect it, and how to present it to the court. It is the admissibility and presentation parts that we will discuss this evening, in particular the evidential rules involved and how to present a case using technology in the local courts.

Once information is detected or disclosed, how does an attorney capture that information, preserve it and then transform it into evidence that can be considered by the court? As we all know, for good reason, courts do not simply trust or admit into evidence what is out there on the Internet -- too much "fake news;" too many "alternative facts." As noted by the court in See *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999),

> Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing ..."

While courts have instituted various rules, procedures and decisions related to the Internet, the ever-changing progression of technology in different mediums and communication devices, all of which contain electronically stored information, present new challenges. Mobile phones alone now contain so many applications and programs that it is hard to tell were the device begins and the medium and reach of its information ends. With the advent of new information devices and pathways comes new evidentiary challenges.

All electronically stored information ("ESI") sought to be admitted at a hearing or trial is "electronic evidence." Electronic evidence includes any electronic communications (such as emails, text messages, chat room, and social media communications); digital photographs; website content, including social media postings; and computer-generated and computer-stored data. *See* Jonathan D. Frieden & Leigh M. Murray, The Admissibility of Electronic Evidence Under the Federal Rules of Evidence, 17 RICH. J.L. & TECH. 5 (2011). With regard to the admissibility of electronic evidence, the federal and state courts have adopted certain pathways for both consideration and admissibility of such evidence. Below we will look at some of those pathways, and then, in the attachments, is information from local courts on the technology available in the courthouses to present evidence at hearings and trial.

THE FEDERAL PATHWAY

The seminal decision regarding the admissibility of electronic evidence was issued by a court right here in our own Fourth Circuit. In Lorraine v. Markel Am. Ins. Co. 241 F.R.D. 534, 537-38 (D. Md. 2007). In that decision, Judge Grimm set forth a model for addressing the admissibility of electronic that consisted of the following five concepts: logical relevance, authentication, the Hearsay Rule, the Original Documents Rule, and pragmatic relevance.

Logical Relevance

Evidence is logically relevant when it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Federal Rule of Evidence ("FRE") 401. Relevant evidence is generally admissible; irrelevant evidence is not. FRE 402.

This test is applied to electronic evidence in the same way that it is applied to more traditional forms of evidence. In federal court, the logical relevance standard presents a relatively low bar for admissibility, especially in light of the fact that a trial court's determination of logical relevance is reviewed under an abuse of discretion standard. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 587, 113 S. Ct. 2786, 2793, 125 L Ed. 2d 469 (1993).

Authentication

To be admissible, electronic evidence must be authenticated; that is, it must be accompanied by other "evidence sufficient to support a finding that the matter in question is what its proponent claims." FRE 901(a). This too is fairly low bar to meet.

In federal court, electronic evidence is most often authenticated under the following rules of evidence:

- FRE 901(b)(1) - Testimony that an item is what it is claimed to be;
- FRE 901(b)(4) - The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.
- FRE 901(b)(7) - Evidence that: (A) a document was recorded or filed in a public office as authorized bylaw; or (B) a purported public record or statement is from the office where items of this kind are kept; and
- FRE 901(b)(9) - Evidence describing a process or system and showing that it produces an accurate result.

Among these, FRE 901(b)(4) is particularly helpful for electronic evidence because the metadata contained therein provides specific and distinctive information. For example, a document created on Microsoft Word will have attendant metadata that includes the documents creator, history, file name, location, format, type, size, and dates of its creation, modification, and access. "Because metadata shows the date, time and identity of the creator of an electronic record, as well as the changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4)." See Lorraine, 241 F.R.D. at 547-48.

For other kinds of electronic evidence, however, authentication can be more straightforward and in keeping with traditional legal principles. Some of those categories include the following:

- Content on Active Commercial Websites - To authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date, (2) the website where the posting appears is owned or controlled by a particular person or entity, and (3) the authorship of the web posting is reasonably attributable to that person or entity. *See, e.g.,* O'Connor V. Newport Hosp.,111 A.3d 317 (R.I. Sup. Ct. 2015).
    - Note, however, that testimony of a mere visitor to a website may not be sufficient to authenticate printouts of website content. *Internet Specialties West, Inc v. ISPWest*, No. CV 05-3296 FMC AJWX 2006 WL 4568796, at *1-2 (CD. Cal. Sept. 19, 2006) (holding that printouts of third-party websites were not properly authenticated by the testimony of a person who visited the websites but had no knowledge of the accuracy of the printouts); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (holding that evidence taken from the Internet lacked authentication where the proponent was unable to show that the information had been posted by the organizations to which she attributed it).
    - But, the testimony of the author of the content, the person who placed the content on the Internet, or a viewer or user of the content with sufficient foundational knowledge would be sufficient. *See, e.g., Perfect 10, Inc v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1154 (CD. Cal. 2002) (holding that website printouts were sufficiently authenticated where the proponent declared that they were true and correct copies of pages found on the Internet and the printouts included the appropriate web addresses and the dates printed).

- Public Records Made Available Through Government Websites - Internet content that originates from a public authority is deemed to be self-authenticating under FRE 902(5) and documents that are taken from government websites are found to be authentic under FRE 901(b)(7). *E.I. DuPont de Nemours*, 2004 WL 2347559, at *1 (E.D. La. 2004); *U.S. ex rel. Trice v. Westinghouse Elec. Corp.*, No. 96-CS-171-WFN, 2000 WL 34024248, at *18 (E.D. Wash. Mar. 1, 2000). If the evidence in question does not originate from a public entity, then a party must present a showing sufficient to satisfy the requirements of FRE 901(a).

- Emails - Emails are most often authenticated as originating from a particular person by demonstrating that: (1) the purported author's name, known email address, or electronic signature appears on the email; (2) the content of the email, such as writing style or reference to facts only known by or uniquely tied to the author, suggest that the purported author sent the email; (3) oral statements by the author, either before or after the email was sent, ties the author to the email; (4) the email originated from the author's computer or mobile device; or (5) the author produced the email in discovery.
    - Note that demonstrating that an email was actually received by a particular person almost always requires some subsequent action by the recipient, such as a reply to the email or communication or conduct by the recipient reflecting his or her knowledge of the contents of the email. In addition, an email may be demonstrated to have been received by a particular person by proof that the email was received and accessed on a computer or mobile device in the control of the alleged recipient.

- Social Networking Content - To authenticate electronic records from a social networking website, the proponent must show that: (1) the records are those of the social networking website and (2) the communications recorded therein were made by the purported author. The first element can be proven by testimony regarding how the records were obtained, the substance of the records themselves, or testimony from the social networking platform. The content can be tied to the purported author by the author's admission, direct testimony by a witness with knowledge of the purported author posting the content, or circumstantial evidence linking the purported author to the content.

- YouTube Videos - A YouTube video may be rendered self-authenticating by obtaining and proffering a Rule 902(11) or (12) certification from a Google custodian of records that the video was captured and maintained on the company's servers in the ordinary course of business at or near the time that a user posted it. *United States v. Hassan*, 742 F.3d 104, 132-33 (4th Cir. 2014) ("In establishing the admissibility of those exhibits [Facebook records and YouTube videos], the government presented the certifications of

records custodians of Facebook and Google, verifying that the Facebook pages and YouTube videos had been maintained as business records in the course of regularly conducted business activities. According to those certifications, Facebook and Google create and retain such pages and videos when (or soon after) their users post them through use of the Facebook or Google servers.")

- Note that even without testimony from a Google employee, such a video may be authenticated by the presentation of evidence identifying the individual and items depicted and establishing where and roughly when the video was recorded. *See, e.g., United States v. Broomfield*, 591 Fed. Appx. 847, 851-52 (11th Cir. Dec. 3, 2014) ("The government's evidence identified the individual in the video as Broomfield, established where and approximately when the video was recorded, and then identified the specific rifle and ammunition depicted in the video. Because authentication may occur solely through the use of circumstantial evidence, the government met its burden of presenting a prima facie case that the video depicted Broomfield in possession of a firearm.")

The Hearsay Rule

Hearsay is any "statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FRE 801. Hearsay is generally inadmissible. FRE 802.

The Hearsay Rule, however, does not apply to three types of statements expressly defined by FRE 801(d) as "non-hearsay":

(1) prior inconsistent statements—sworn statements which are inconsistent with the declarant's trial or hearing testimony,

(2) prior consistent statements offered to rebut a charge "against the declaration of recent fabrication or improper influence or motive," and

(3) admissions of a party opponent.

In addition to these hearsay exclusions, all of the hearsay exceptions applicable to traditional forms of evidence are applicable to electronic evidence. There are three hearsay exclusions or exceptions that are frequently applied to electronic evidence:

- Statements Made by an Opposing Party on its Website - Generally, statements made by an opposing party on its website are admissible as admissions of a party-opponent under FRE 801(d)(2). However, substantive information placed by a third party on an opposing party's website will not be admissible if it is not adopted by the opposing party." *United States v. Jackson*, 208 F.3d 633,637-38 (7th Cir. 2000).

- Public Records and Reports - Certain "[r]ecords, reports, statements, or data compilations, in any form, of public offices or agencies" are not made by the Hearsay Rule, even though the declarant is available as a witness. FRE 803(8). As the Rule states, the "public records exception" is not limited to traditional print documents, but includes electronic evidence.

- Market and Commercial Reports - Another exception to the Hearsay Rule exists for "market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations." FRE 803(17). When such information appears on a website, it is admissible in the same manner as similar material published in books or periodicals. *Elliott Assoc., L.P. v. Banco de la Nacion*, 194 F.R.D. 116, 121 (S.D.N.Y. 2000) (holding that rates acquired from the Federal Reserve Board website or from Bloomberg are admissible under Fed. R. Evid. 803(17).

The Original Documents Rule

An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise." FRE 1002. "For electronically stored information, 'original' means any printout -- or other output readable by sight -- if it accurately

reflects the information." FRE 1001(d). As such, the Original Documents Rule rarely presents a significant obstacle to the admissibility of electronic evidence.

Pragmatic Relevance

Under FRE 403, evidence will be held inadmissible "if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence." The test for pragmatic relevance is applied to electronic evidence in the same fashion that it is applied to more traditional forms of evidence.

THE VIRGINIA PATHWAY

Taking the same progression as the federal court(s) above, the admissibility of electronic evidence under Virginia law can be compared as follows.

Logical Relevance

Evidence is logically relevant when it has "any tendency to make the existence of any fact in issue more probable or less probable than it would be without the evidence." Virginia Rule of Evidence ("VRE") 2:401. Relevant evidence is generally admissible; irrelevant evidence is not. VRE 2:402.

Authentication

I. Fed. R. Evid. 901(b)(1) ***Testimony of a Witness with Knowledge.*** "Testimony that an item is what it is claimed to be."

   a. Sup. Ct. Rules, Rule 2:901 ***Requirement of Authentication or Identification.*** "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the thing in question is what its proponent claims."

II. Fed. R. Evid. 901(b)(4) ***Distinctive Characteristics and the Like.*** "The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item taken, together with all the circumstances."

a. Va. Notes: "Of course, appearance, contents, substance, internal patterns, other distinctive characteristics, taken in conjunction with circumstances, can be sufficient to authenticate." *See Bloom v. Commonwealth*, 34 Va. App. 364 (2001) (contents of e-mail communications establish identity).

III. Fed. R. Evid. 901(b)(7) ***Evidence About Public Records.*** "Evidence that (A) a document was recorded or filed in a public office as authorized by law or (B) a purported public record or statement is from the office where items of this kind are kept."

a. Sup. Ct. Rules, Rule 2:902(1) ***Domestic public records offered in compliance with statute.*** "Public records authenticated or certified as provided under a statute of the Commonwealth."

IV. Fed. R. Evid. 901(b)(9) ***Evidence About a Process or System.*** "Evidence describing a process or system and showing that it produces an accurate result."

a. Va. Notes: "Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result is sufficient to satisfy this requirement." *See Sabo v. Commonwealth*, 38 Va. App. 63 (2002) (audio recordings); *Wilson v. Commonwealth*, 29 Va. App. 236 (1999) (videotapes); *Midkiff v. Commonwealth*, 54 Va. App. 323 (2009) (process of producing images from computer files).

Hearsay Rule

I. Fed. R. Evid. 801(d)(2) (***An Opposing Party's Statement***) and Sup. Ct. Rules, Rule 2:803(0) (***Admission by a Party Opponent***) are substantially the same, and are used as an exception to the hearsay rule to get statements made by a party off of a website that it maintains.

II. Fed. R. Evid. 803(8) ***Public Records.*** A record or statement of a public office if:

i. It sets out

1. The office's activities;

2. A matter observed while under a legal duty to report, but not including, in a criminal case, a matter observed by law enforcement personnel; or

3. In a civil case or against the government in a criminal case, factual findings from a legally authorized investigation; and

ii. The opponent does not show that the source of information or other circumstances indicate a lack of trustworthiness.

Sup. Ct. Rules, Rule 2:803(8) ***Public records and reports.*** "In addition to categories of government records made admissible by statute, records, reports, statements, or data compilations, in any form, prepared by public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed within the scope of the office or agency's duties, as to which the source of the recorded information could testify if called as a witness; generally excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel when offered against a criminal defendant."

III. Fed. R. Evid. 803(17) ***Market Reports and Similar Commercial Publications.*** "Market quotations, lists, directories, or other compilations that are generally relied on by the public or by persons in particular occupations."

a. Sup. Ct. Rules, Rule 2:803(17) ***Market quotations.*** **"**Whenever the prevailing price or value of any goods regularly brought and sold in any established commodity market is in issue, reports in official publications or trade journals or in newspapers or periodicals of general circulation published as the reports of such market shall be admissible in evidence. The circumstances of the preparation of such a report may be shown."

The Original Document Rule

I. Fed. R. Evid. 1001(d) "An 'original' of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, 'original' means any printout — or other output readable by sight — if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it."

a. Sup. Ct. Rules, rule 2:1001(2) ***Original.*** "An 'original' of a writing is the writing itself or any other writing intended to have the same effect by a person executing or issuing it."

Pragmatic Relevance

Under VRE 403, evidence will be excluded if (a) the probative value of the evidence is substantially outweighed by (i) the danger of unfair prejudice, or (ii) its likelihood of confusing or misleading the trier of fact; or (b) the evidence is needlessly cumulative.

COURTHOUSE TECHNOLOGY

Attachment A – materials from the **Circuit Court of Arlington County**

Attachment B – materials from the **Circuit Court of Fairfax County**

Attachment C – materials from the **Loudoun County Circuit Court**

Attachment D – materials from the **United States District Court for the Eastern District of Virginia** (Alex. Div.)

Attachment E – information for the **Circuit Court for the City of Alexandria**