2023 TENNESSEE JUDICIAL CONFERENCE

THE ROLE OF THE JUDGE AS EVIDENCE GATEKEEPER, PART 1

ANALYZING ELECTRONIC EVIDENCE

Presented By: Penny J. White, pwhite4@utk.edu

This course will discuss evidentiary challenges that arise out of the various types of electronic evidence and electronically stored information. Following a preliminary discussion about the foundational elements of the authentication and admissibility of electronic evidence, judges will address a case study, which will require an analysis of multiple types of electronic evidence. Judges will consider the foundational requirements, potential objections, and will articulate their rulings. Thus, after attending this session, judges will be able to:

1. Predict and analyze evidentiary challenges related to the authentication and admissibility of all types of electronic evidence and electronically stored information;
2. Rule confidently and correctly on objections to the introduction of all types of electronic evidence;
3. Differentiate between requirements for authenticating and admitting simulations and animations; and
4. Simulate evidentiary rulings on specific cases involving the introduction of webpages, social media evidence, email and text messages, call logs, real-time videos, and cell data tracking information.

I. Defining Electronic Evidence (EE) and Electronically Store Information (ESI)

EE and ESI come in a "multitude of formats, including e-mail, internet postings, digital photographs, computer-stored information; computer-generated documents; and data files. ESI may include e-mail ESI, website ESI, internet postings, digital photographs, and computer-generated documents and data files. Internet postings include: data posted by the site owner, data posted by others with the consent of the site owner, and data posted by others without consent. Computer-generated documents and files include: electronically stored records or data, computer simulation, and computer animation. These multiple types of electronic evidence raise complex issues of authentication and admissibility, which judges must address before allowing the introduction of the evidence." 2 McCormick on Evidence §227 (6th ed. 2006).

II. The Process for Authentication and Admission of ESI and EE

Just as is true of other tangible or documentary evidence, the proponent of EE and ESI must scale several hurdles in order to introduce the evidence. First and foremost, the judge must remember that it is the proponent's job to scale the hurdles of both authentication and admissibility before the EE or ESI may be introduced. Thus, reduced to its simplest formulation, EE and ESI must be both authenticated and admissible. The proponent has an obligation to authenticate the

evidence before requesting its introduction. Until the evidence is authenticated, it is irrelevant and, therefore, inadmissible.

Once the proponent authenticates the evidence and establishes its relevance, the opponent may raise admissibility objections, based on most other evidence rules. If other objections are raised, then the proponent must address and meet those admissibility objections as well. If both authentication and admissibility are established, then the proponent may publish the evidence to the jury, but it may be necessary for the trial judge to determine how the evidence will best be presented to the trier of fact, bearing in mind that the court is obligated to "exercise reasonable control" so as to make court procedures effective "for the ascertainment of the truth." S.C.R. Evid. 611(a).

III. Evidence Rules Implicated in the Authentication and Admissibility of EE and ESI

A. Evidence Rules Implicated in the Authentication of EE and ESI

Most scholars and courts agree that the issues related to the authentication of electronic evidence may be resolved by an application of the existing evidence rules. Although authentication may present unique challenges, the existing authentication rules are flexible enough in their approach to be applied to this new kind of evidence. To ease the introduction of digital evidence, the Federal Rules of Evidence have been amended to include two additional self-authenticating provisions, but those provisions do not apply in Tennessee.

The standard for authentication of tangible evidence is set out in Rule 901(a), which provides that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Tenn. R. Evid. 901(a). In addition to this overall standard, the rules include a list of illustrations, Tenn. R. Evid. 901(b), and a list of self-authenticating documents. Tenn. Evid. 902.

The most common methods for authenticating electronic evidence are set out as illustrations in Rules 901(b) (1), (4), (8), and (9).

> **(b) Illustrations.** By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
>
> (1) *Testimony of witness with knowledge.* - Testimony that a matter is what it is claimed to be.
>
> . . .
>
> (4) *Distinctive characteristics and the like.* - Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.
>
> . . .
>
> (8) *Ancient Documents or Data Compilation.* Evidence that a document or data compilation in any form, (A) is in such condition as to create no suspicion

concerning its authenticity, (B) was in a place where, if authentic, it would likely be, and (C) has been in existence thirty years or more at the time it is offered.

. . .

(9) *Process or system.* - Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

(10) *Methods Provided by Statute or Rule* - Any method of authentication or identification provided by Act of Congress or the Tennessee Legislature or by other rules prescribed by the Tennessee Supreme Court.

The most frequently used self-authenticating methods apply to public records and business records. Numerous other documents and records may be self-authenticated under Rule 902(b), which provides:

Extrinsic evidence of authenticity as a condition precedent to admissibility is not required as to the following:

. . .

(4) *Certified Copies of Public Records* - A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or the Tennessee Legislature or rule prescribed by the Tennessee Supreme Court.

. . .

(5) *Official Publications* - Books, pamphlets, or other publications purporting to be issued by public authority.

. . .

(6) *Newspapers and Periodicals* - Printed material purporting to be newspapers and periodicals.

. . .

(11) *Certified Records of Regularly Conducted Activity* - The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by an affidavit of its custodian or other qualified person certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of and a business duty to record or transmit those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and

declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

B. Evidence Rules Implicated in the Admissibility of EE and ESI

As is true of all evidence, the admissibility of EE and ESI depends upon the purpose for which the evidence is offered. The purpose of the evidence will control whether it is relevant and, even if relevant, whether it should be excluded because of certain dangers inherent in the evidence. *See* Tenn. R. Evid. 403. Depending upon the purpose for which the EE or ESI is offered, the admission may also be impacted by the hearsay rules and the original writing rules, when the EE or ESI is offered to prove the content or establish the truth of the information contained within the EE or ESI. Additionally, EE and ESI also may implicate other rules such as the opinion rules and the personal knowledge rule; in unique circumstances, the admission of electronic evidence may be influenced by constitutional principles.

IV. Challenges Presented by Authentication and Admissibility of EE and ESI

A. General Challenges Presented by All EE and ESI

While many of the evidentiary challenges that apply to other documentary evidence apply as well to electronic evidence, some greater challenges exist in authenticating electronic evidence. As one judge has noted, "courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources." *Lorraine et al. v. Markel American Insurance Company*, 241 F.R.D. 534, 543 (D. Md. 2007).

As noted in Weinstein's text on evidence rules,

> In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.
>
> The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination. Factors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems. The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the

computer operation, and the ability to test and verify results of the computer processing.

Determining what degree of foundation is appropriate in any given case is in the judgment of the court. The required foundation will vary not only with the particular circumstances but also with the individual judge.

B. Particularized Challenges Presented by Specialized EE and ESI

1. Evidence from Social Media

Social media is a prominent force in the lives of millions. Subscribers to Facebook, LinkedIn, Twitter, and other social media sites communicate regularly through their social media networks. As a result, when those communications become relevant to a matter in court, evidentiary issues arise.

At least one study commenting on the importance of the use of social media evidence in litigation has concluded that "it is a matter of professional competence for attorneys to investigate relevant social networking sites." *See* Sharon Nelson et al., "The Legal Implications of Social Networking," 22 Regent U.L. Rev. 1, 1–2 (2009/2010). Practitioners and academics alike have written extensively on the use of social media evidence in litigation. *See* Edward M. Marsico Jr., "Social Networking Websites: Are MySpace and Facebook the Fingerprints of the Twenty-First Century?" 19 Widener L.J. 3, 967 (2010); Andrew C. Payne, "Twitigation: Old Rules in a New World," 49 Washburn L.J. 3, 841 (Spring 2010); Katherine Minotti, "Evidence: The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession," 60 S.C. L. Rev. 1057 (Summer 2009); Grossman, "No, Don't IM Me—Instant Message, Authentication, and the Best Evidence Rule," 13 Geo. Mason L. Rev. 1309 (2006); John S. Wilson, "MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence," 86 Or. L. Rev. 1201 (2007).

The starting point for analysis of the admission of social media website information is the traditional analysis employed for determining the foundation for any written or photographic evidence. Some factors unique to social media evidence, however, bring additional dimensions to the analysis.

One prominent issue is the reliability of information posted on social media. Because of anonymity in some forums, the matter of attribution is more complicated. As a result, commentators have encouraged judges to consider the admissibility of social media evidence with healthy skepticism. Despite this cautious approach, many courts admit social media postings and treat the issues of attribution as a matter of weight or conditional relevance.

Another issue unique to social media evidence is the privacy issue. Social network websites contain privacy statements that are endorsed by subscribers in order to secure a page. As a general rule, the policy statements advise that pages which have a privacy setting of "everyone" are publicly accessible to all and may be redistributed across the internet. Facebook in particular states that it "may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required

by law." As a result, most courts extend the principle that subscribers have no reasonable expectation of privacy in the information that is posted on a social network site with a privacy filter set to allow access to "everyone." *See Independent Newspapers, Inc. v. Brodie*, 996 A.2d 432 n.3 (Md. 2009)(noting that "[t]he act of posting information on a social networking site, without the poster limiting access to that information, makes whatever is posted available to the world at large."). Non-evidentiary privacy issues are also being litigated frequently in the courts.

Courts must also be aware of the impact of federal law on electronically stored information. The Stored Communications Act, 18 U.S.C. §§ 2701-2712, regulates the dissemination of electronically stored information in civil matters. The Act provides a cause of action for damages when electronic evidence is disclosed without authorization. Many courts have interpreted the Act to allow social networking to decline to provide stored information without consent. Many social networking sites will provide only general information when faced with a civil subpoena, but will not provide posts and communications. *See generally Ehling v. Monmoth-Ocean Hosp. Service Corp*., 2013 WL 4436539 (D.N.J. Aug. 20, 2013).

2. Format for Social Media Evidence

Information from social media pages may be offered in a number of different formats including printouts, screen captures, and as stored on a digital storage device. Courts differ on the foundation necessary and the acceptance of these different formats for the introduction of social media evidence.

Some courts allow the introduction of printouts from social media pages when offered by the parties, without foundation. Other courts require the testimony of the individual who printed the information or one who confirms that it existed on a certain page at a certain time. Some courts disallow the introduction unless the printout contains the URL address and date.

Because screen captures, taking a photo of the entire computer screen, contain the URL address and other identifying information, there may be a preference of this format for social media evidence, but few courts have discussed this issue. Like screen captures, information save to a digital storage device will include more identifying information and will also save metadata, which is information concerning the creation and modification of the data.

3. Computer-Generated Evidence

Most scholars differentiate between exhibits containing computer-stored declarations (evidence that "reiterates human declarations") and exhibits containing computer-generated output (evidence produced when computer performs programmed tasks, but not including assertions or declarations). Computer-stored declarations include accounting records, invoices, charts, graphs, summaries – basically the host of documents consisting of printouts reiterating date that was entered into the computer. Computer-generated output include automated records, such as call records, test scoring, and enhanced photographic images.

The differentiation is important because while evidence containing declarations is hearsay, most courts treat evidence containing automated output as non-assertions and thus, not impacted

by the hearsay rule. For evidence containing computer-stored declarations, both the entry of the data into the computer and the underlying assertions are out of court assertions subject to the hearsay rule.

The act of data entry is an extrajudicial statement - i.e., assertive nonverbal conduct within Rule 801(a) - as is any underlying declaration, under Rule 801(c). Data entry is usually a regularly-conducted activity within Rule 803(6) (or, in appropriate circumstances, falls within Rule 803(8) (public records exception)). It also often falls within Rule 803(1) (present sense impression exception). The real question about the data entry function is its accuracy. This is, in substance, an issue of authenticity and should be addressed as part of the requisite authentication foundation whenever a genuine doubt as to trustworthiness has been raised.

If the underlying data that are entered into the computer are themselves hearsay declarations, they in turn must satisfy a hearsay exception or exemption under Rule 805.

The paper or other hard-copy output of a computer may constitute a business or public record within Rules 803(6) and (8). At the same time, each electronic data entry contained in the computer is itself a Rule 803(6) or (8) record. In the terminology of these Rules, each electronic entry is a "data compilation, in any form."

Consequently, if each entry has been made in conformance with Rule 803(6), the computer-generated output satisfies the hearsay exception even if it: (a) was not printed out at or near the time of the events recorded (as long as the entries were timely made), (b) was not prepared in ordinary course (but, e.g., for trial), and (c) is not in the usual form (but, e.g., is in graphic form). If the data are simply downloaded into a printout, they do not lose their business-record character. To the extent that significant selection, correction and interpretation are involved, their reliability and authenticity may be questioned. Gregory Joseph, "A Simplified Approach to Computer-Generated Evidence and Admissions," (available at http://www.jha.com/us/articles/viewarticle.php?8).

But it is important to note that Rule 803(6) contains a unique trustworthiness requirement. Records of regularly conducted activity are admissible "unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness." Tenn. R. Evid. 803(6). Because of the potential inaccuracies of EE and ESI created by human assertions, judges should anticipate that counsel will rely more frequently on these unique trustworthiness requirements to challenge the introduction of public and business records in cases involving EE and ESI.

4. Computer Animations and Simulations

Two kinds of computer generated evidence (CGE) are animations and simulations. If the CGE is used to illustrate and explain a witness' testimony, it is generally referred to as an animation. Its purpose is purely demonstrative. But if the CGE is based on scientific or physical principles and based upon data entered into and then processed by a computer programmed to analyze the data and draw conclusions from the data, the CGE is referred to as a computer simulation and is offered to establish the veracity of its content.

a. Authentication and Admissibility

i. Computer Animation

Computer animation is no more than a series of still images, which are shown in rapid succession so that the viewer perceives a single moving image. The animator produces this by creating key frames, which show the position of people and objects. Most commonly used in a legal context to represent incident scenes, computer animations are usually created from eyewitness accounts as well as from actual data from the scene (the position of roads and buildings, for example). Having created such key individual frames, the animator is then able to create the full set of frames that show how people and objects move between different positions with reference to eyewitness accounts and other available data from the scenes in question. The animation can be made more realistic by the inclusion of lighting and weather conditions to reflect the season and weather at the time of the incident in question. Finally, having created the animation, the software may be able to change the viewing angle. This would not be possible in real life, and accordingly observers in court may be shown scenes from angles from which no witness could actually have seen the events.

Computer animation has the potential to be a near-accurate version of a particular event. However, its accuracy is entirely dependent on the measurements taken at the scene, the memory of eyewitnesses, and the accuracy of the eyewitnesses. Computer animations may help a judge or jury to quickly form an understanding of a particular event, more vividly than if they were merely shown a series of photographs or had the event described to them. But an animation cannot be viewed as representing an exact replica of the event and as such is most useful in showing, not what did happen but what could not possibly have happened. As a result, animations are most often used by witnesses to explain or illustrate their testimony and are therefore treated as demonstrative evidence.

To authenticate an animation, the proponent must establish that it is fair and accurate representation of the evidence to which it relates. Because the purpose of animations is demonstrative, the only admissibility hurdle is Rule 403. The issue of whether the probative value of the animation is substantially outweighed by the danger of unfair prejudice, confusion of the issues, waste of time, or misleading the jury is committed to the sound discretion of the judge.

Because animations are potentially misleading, and should only be viewed as a party's recreation of his or her version of the events, courts generally give cautionary instructions when admitting animations. Some courts offer explicit instructions, for example, warning the jury that the animation is not a "re-creation of reality" and should not be used as such. *See* *State v. Farner*, 66 S.W.3d 188 (Tenn. 2001).

Judges should exercise strict discretion with regard to the use of animations or simulations during closing argument, when the evidence has not been introduced. Because of their powerful and potentially misleading nature, animations and simulations should not be treated as casually as slide presentations, charts, or diagrams, which are generously allowed during closing argument.

ii. Computer Simulation

A computer simulation is based in science and technology. Computer simulations are created by a computer program or by a network of computers attempting to simulate an actual event. Some scholars refer to computer simulations as "computer opinions." The simulation is produced by software, which, in effect becomes an expert witness. When a simulation is created, the resulting sequence is not merely an eyewitness account brought to life but a computerized demonstration of what actually happened based upon the application of mathematical and physical principles. When a computer simulation is offered in evidence, it is offered as substantive evidence or as a basis for an expert's opinion. An example would be a computer simulation which reconstructs an accident based upon scientific and other factual data entered into and then processed by a computer software program that then generates a visual image of how the accident occurred. The results of a simulation depend upon the application of scientific principles. Thus, courts treat simulations as other types of expert testimony that require proof of the scientific principles and data before admission. Thus, most courts do not allow simulations to be authenticated or admitted without expert testimony establishing the reliability and validity of the scientific principles underlying the process.

To determine the reliability of the simulation, the court must consider (1) whether the computer was properly functioning; (2) whether the software program used produces a reliable result; and (3) whether the data inputted to produce the simulation was reliable, complete, and an appropriate "fit" with the facts and issues in the case. Thus, to authenticate a simulation, the proponent should be prepared to offer evidence describing the process or system used to produce the simulation as well as evidence establishing that the process or system produces an accurate result. The underlying software must meet expert opinion standards, as must the testifying expert. If the software has historically produced reliable results, it is more appropriate to accept the simulation, than if the software is customized, particularly when to determine its reliability would require a court to scrutinize the underlying software codes. Additional issues arise when the software is proprietary, utilizing codes that are confidential, the trade secrets of a non-party, or otherwise inaccessible.

iii. The Next Evidentiary Challenge – Use of Virtual Reality Evidence

Virtual reality evidence is the next advance from computer simulations. Here, the technology allows the creation of a *three dimensional* sequence in which the viewer can participate, move around the area, look at the incidents from different viewpoints. The judge or jury could be given the impression of actually participating in the recreation of the events in question.[1]

5. Real-time Videos and the Silent Witness Theory

Videos are usually introduced based upon a foundation similar to that required for photographs. If a witness testifies that the video is a fair and accurate depiction of the event it

[1] A California court allowed the admission of virtual reality evidence to help the jury understand the treacherous terrain over which an accident victim drove a motorcycle. *Stephenson v. Honda Motors Ltd. Of America*, Cal. Super. Case No. 81067, June 25, 1992).

captures, the video is ordinarily admitted. Additionally, videos are generally admitted when used to illustrate a witness' testimony as for example, when the video captured an event that the witness was watching in real time. But a different issue is presented when a video captured an event that no one witnessed.

Real-time videos often capture important information about incidents to which there is no first-hand witness who can testify that the "matter in question is what its proponent claims." SCRE 901(a). Many courts have adopted a "silent witness" theory to allow for the introduction of the recording as substantive evidence of the events. Some jurisdictions treat the video as a "silent witness," holding that the silent witness video speaks for itself. *See* 2 McCormick on Evidence, § 215, at 23-24, § 216, at 28-29 (Kenneth S. Broun ed., 6th ed. 2006). "Under this theory, a witness need not testify as to the accuracy of the image depicted in the photographic or videotape evidence if the accuracy of the process that produced the evidence is established with an adequate foundation." *See* *State v. Stangle*, 97 A.3d 634 (N.H. 2014).

Judicial approaches to the introduction of real-time videos under the silent witness theory are both flexible and rigid. Courts utilizing the flexible approach determine the authenticity of the real-time video on a case-by-case basis, allowing the introduction of the video after its proponent establishes that the video accurately depicts the events. Other courts require a more rigid foundation, including multiple factors, including (1) how the recording system operates; (2) whether it has been established that the system was operating as intended at the time in question; (3) who has access to the system; (4) how the system is maintained; (5) the quality of the recording; and (6) the mechanism by which the recording was produced from its original format to that introduced at trial. *See generally* "Construction and Application of Silent Witness Theory," 116 A.L.R. 5th 373 (2004); *State v. Stangle*, 97 A.3d at 634 (citing numerous cases using both approaches).

6. Cell Data Tracking Information

Cellular data analysis involves collecting, analyzing, and presenting information about a cell phone's approximate location at a given time based upon data received from the wireless phone company or the cell phone itself.

Cell phone tracking involves looking at cell phone call records, cell phone tower information, and sometimes real-time information provided either by the Emergency 911 (E911) system or by Global Positioning Systems (GPS). Global Positioning Systems (GPS) are a "satellite-based navigation system . . . by which a receiver on the satellite picks up a signal delivered from a GPS chip in the cellular phone. The delivery speed is then converted into distance giving a very accurate reading of the cell phone location." Only about six percent of the cell phones in the United States have GPS capacity. Additionally, GPS only tracks the phone's location "when the cell user is explicitly using a location-based application on the phone." "Ping! The Admissibility of Cellular Records to Track Criminal Defendants," 33 Saint Louis Univ. Public L. Rev. 487, 490 (2014).

As a result of these current limitations, most cell tracking is done based upon cell site data, which includes both real-time and historical data. This method uses cellular technology to locate

the cell user. "Real-time cell site data is obtained through viewing the cell phone's activity and signals in real time . . . ." [H]istorical cell site data . . . is information obtained after the cell phone's activity is recorded using the cell companies' records of that activity." *Id.* An excellent description of how cell data is tracked can be found in Larry E. Daniel, "Cell Phone Tracking Evidence," in Cellular Location Evidence for Legal Professionals (available at http://www.ncids.org/Defender%20Training/2014SpringConf/CellPhoneTracking.pdf).

Most cell phones emit signals every second seconds and scan the area constantly to locate a surrounding tower with a strong signal. Based on a number of different methods, the most popular of which is known as triangulation, cell phones are tracked to provide an approximate location. The triangulation method is described as "fairly precise," but it may only be used when a cellular phone "pings" off two or more towers simultaneously. When that happens, mathematical equations can be used to determine the cell phone's proximity to the two towers.

A more suspect mapping system, known as simple mapping, involves taking historical cell tower data and cell phone records to "map" the location of the cell user at a given time. Simple mapping is based on a false assumption that a cell phone will always "ping" on the tower to which it is the closest. Because cell phones use the strongest, not the closest signal, the assumption underlying simple mapping is flawed.

The strength of a cell tower signal depends on a host of factors including: technical characteristics of the cell site; number of sites available; maintenance of sites; repair of sites; height of the tower; distance above sea level; wattage output; and range of coverage. Additionally, the characteristics of the cell tower antenna can impact signal strength. These factors include the number of antennas; the angle and direction of the antenna(s); the height of the antenna; and the traffic processed by each antenna. Additionally, technical characteristics of the cell phone can also impact signal strength. These factors include: wattage output, the generation of broadband capability, which is determined generally by the age of the phone. As a final consideration, the location (inside or outside) and the time of day can also affect signal strength.

Because of these reliability concerns, lawyers raise a range of evidentiary challenges to the admission of cell data tracking evidence. First, the court must determine the use of the evidence. While the proponent of cell tower data evidence may argue that the evidence map, chart, or diagram (hereafter exhibit) that is being offered is similar to an animation and purely demonstrative, this argument is implausible if the proponent wants to use the evidence substantively, i.e., to establish facts from which the cell phone location can be inferred. When the testimony or exhibits is being used substantively, authentication requires a consideration of the system used to produce the data.

If the court accepts the argument that the evidence is being demonstratively, rather than substantively, authority related to animations might be applied. When evidence is used to illustrate, it is particularly problematic, because the jury may tend to be over-persuaded by the evidence. As a result, the foundational requirement that the evidence be fair and accurate is heightened. In addition, when the court balances the probative value of the testimony and exhibit against the danger that the evidence is unfairly prejudicial, any inaccuracy or uncertainty about the underlying data that forms the basis for the exhibit will reduce the probative value of the evidence.

When the probative value is decreased, the degree of potential prejudicial necessary for exclusion is similarly decreased.

In addition to authentication concerns, cell data tracking evidence also raises numerous admissibility issues. Although relevant to establish the location of the cell phone, the evidence may not meet the Rule 401 relevance standard on the issue of the location of a particular person. This is particularly true of pre-paid, non-subscription phones.

Other admissibility issues include content-based issues arising under the hearsay, original writing, completeness, and summary rules. *See* Tenn..R. Evid. 801, 1001, 106, 1005. But by far, the most significant admissibility issue concerns the nature of the testimony. If the testimony is considered lay, it must be the result of reasoning familiar in everyday life and must be based on the rational perceptions of an individual. If, instead, the testimony results from a process of reasoning that is based on technology, science, or other specialized knowledge, the testimony can only be given by a witness qualified by skill, experience, education, and training, and must arise from a sufficiently reliable area of scientific, technical, or other specialized knowledge.

V. Some Recent Tennessee Electronic Evidence Cases

State v. Murray, No. M2021-00688-CCA-R3-CD, 2022 WL 17336522 (Tenn. Crim. App. Nov. 30, 2022) (no perm. app. filed). Defendant raised issues regarding authenticity of Facebook messages, claiming that the State could not establish that he sent them. At trial, the State said that it had received a custodial affidavit from Facebook regarding records verifying that the records were true and accurate copies of the messages. The witness to whom the messages were sent identified the messages as those he exchanged with the defendant via a Facebook profile he knew belonged to the defendant. The Tennessee Court of Criminal Appeals found that this evidence was sufficient to support a finding that the messages were "what [they were] claimed to be."

State v. Ison, No. E2018-02122-CCA-R3-CD, 2020 WL 3263384 (Tenn. Crim. App. June 17, 2020). At trial, officer testified about the content of several posts on the defendant's Facebook account, which was publicly viewable and the officer had accessed on his own computer. The officer testified that the profile name and birthdate matched the defendant, and that the profile picture was of the defendant's son. The defense challenged the authenticity and admissibility of the Facebook records, arguing that the posts had to be authenticated by someone from Facebook. The Court of Criminal Appeals, however, was satisfied that the State put forth sufficient evidence connecting the Facebook profile and posts to the defendant.

State v. Spivey, No. M2018-00263-CCA-R3-CD, 2020 WL 598347 (Tenn. Crim. App. Feb. 7, 2020). At the defendant's murder trial, the State sought to introduce a still image taken from a YouTube video taken by a detective who located the video. The State called the detective to authenticate the video because the detective knew what the defendant looked like and then used the video to allow the victim to identify the defendant as the person who robbed him. The defendant had on a distinctive watch when he robbed the victim and was wearing the same watch in the video from which the image came. The trial court was satisfied that sufficient foundation had been laid to admit the video, and the appellate agreed. The opinion includes a discussion of other jurisdiction's approach to analyzing authentication issues with social media.

State v. Linzy, No. E2016-01052-CCA-R3-CD, 2017 WL 3575871 (Tenn. Crim. App. Aug. 18, 2017). Defense moved pretrial to exclude evidence of argumentative posts on Twitter and FaceBook in which the defendant and victim were involved. The defendant argued that social media posts and comments were impossible to authenticate in that a phone that was logged in could be used by anyone to tweet or post. Witness at trial testified that he could identify the victim's and the defendant's social media accounts by their profile picture and handle Over the defendant's repeated objection, the trial court found the screenshots of the arguments properly authenticated and admissible (based on its relevance to the case). On appeal, the appellate court thoroughly examined authentication for social media posts. One way in which the State can properly authenticate social media evidence is through "corroborating circumstantial evidence," but determining whether any given social media posts have been authenticated is a fact-specific inquiry The Court, respectfully, muddled the concepts of authenticity and admissibility, noting that admissibility was "easier" and involved only a relevancy determination. Unfortunately, the court also noted: "To the extent that [a] [d]efendant argued that the State was required to affirmatively prove that the [d]efendant was the author of the message, . . . such challenge goes to the weight of the evidence, not its admissibility."

VI. Recent Illustrations of the Importance of Electronic Evidence

From a non-lawyer:

> Second, prosecutors reconstructed a tight timeline of the crime using lots and lots of data. Among other sources, they extracted information from Alex, Maggie and Paul Murdaugh's iPhones, call records of family and friends, location and speed data from Murdaugh's S.U.V., entry logs from his office security system, images from automatic license plate readers mounted on public roads, communications on social networks and messaging apps, reams of financial data and video and audio recorded on Murdaugh's 911 call and by police officers at the scene.
>
> It isn't surprising that authorities would mine such data to determine basic facts like who was where and when, but prosecutors in the Murdaugh case claimed to find many deeper truths in the digital record. And it's in their interpretations of the data that they sometimes lost me. Often, they seemed to be finding patterns in the data that didn't necessarily hold true, and this made me wary that the authorities can build outlandish stories from our data.
>
> Come on — really? I can see how some of these details can paint a pretty damning picture when put together on a neat timeline. But I expected the jury to spend some time pondering the perfectly innocuous explanations for many of them.
>
> . . .

Yes, our devices now capture everything about what everyone is doing, but making sense of that data isn't trivial. In the Murdaugh case, both sides pointed to the digital record — but by the end of the trial, I felt like I had no real idea what actually happened. The jury was hardly so cautious.