Social Media – Evidentiary Issues

State Bar of Texas

Labor & Employment Law Section

Fall 2019 Seminar

San Antonio, Texas

August 23-24, 2019

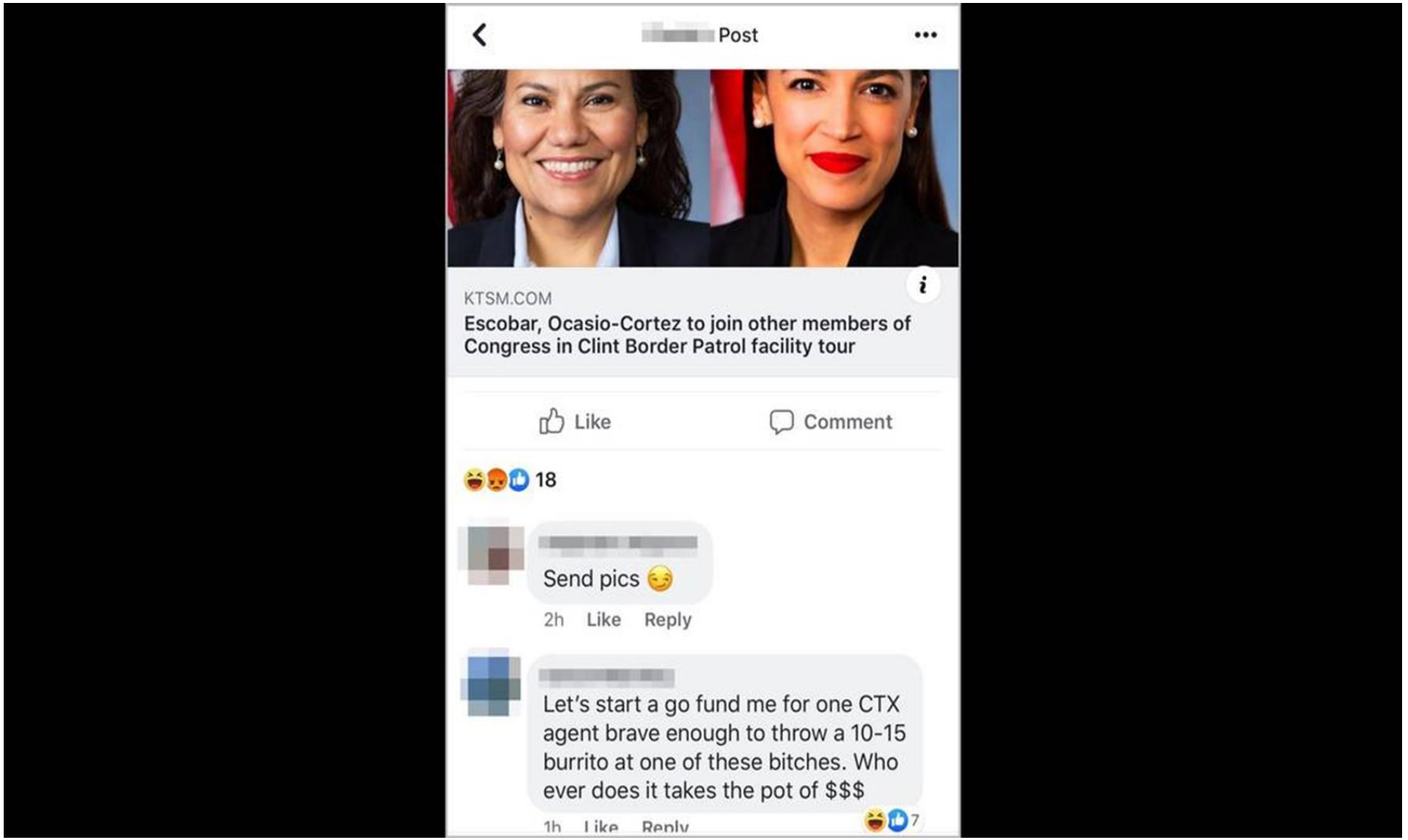
John A. Wenke
Attorney at Law
501 E. California Ave.
El Paso, Texas 79902
(915) 351-8877
johnwenke.com

Social media icons | 30 icons

FLATICON

How we connect with family . . .

… and how we denigrate and belittle others



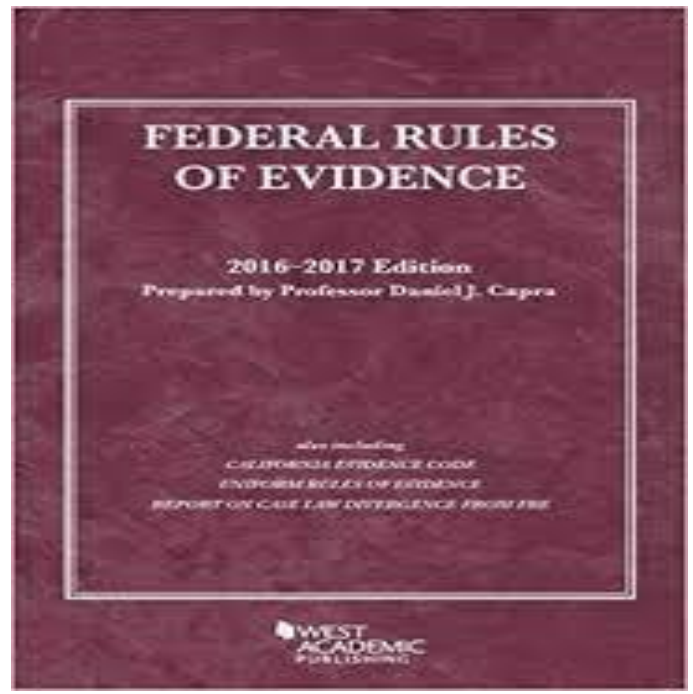
So you are getting ready for trial…

✓You have social media evidence through discovery

✓ Relevant

✓ Hearsay Exception

How do we authenticate and offer it as evidence?


FEDERAL RULES
OF EVIDENCE
2016–2017 Edition
Prepared by Professor Daniel J. Capra
also including
CALIFORNIA EVIDENCE CODE
UNIFORM RULES OF EVIDENCE
REPORT ON CASE LAW DIVERGENCE FROM FRE
WEST
ACADEMIC
PUBLISHING

FRE / TRE 104(a)
Preliminary Questions of Evidence

2 Step Process

1. The court must determine whether the proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic

    a. Proponent must make a "prima facie showing" that the exhibit is what the proponent claims the exhibit is

    b. It is "not a particularly high burden to overcome."

2. Jury ultimately decides whether evidence admitted for its consideration is what the proponent claims

FRE/TRE 901
Authenticating or Identify Evidence

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

"Judge, it is what it is."

Clearly insufficient evidence to authenticate…

Only having the person’s name or photo on a post or tweet, etc

901(b) List of Suggested Ways to Authenticate

(1) ***Testimony of a Witness with Knowledge*****.**
(2) ***Nonexpert Opinion About Handwriting*****.**
(3) ***Comparison by an Expert Witness or the Trier of Fact*****.**
(4) ***Distinctive Characteristics and the Like*****.**
(5) ***Opinion About a Voice***
(6) ***Evidence About a Telephone Conversation*****.**
(7) ***Evidence About Public Records*****.**
(8) ***Evidence About Ancient Documents or Data Compilations*****.**
(9) ***Evidence About a Process or System*****.**
(10) ***Methods Provided by a Statute or Rule*****.**

Most Common Ways to Authenticate

(1) *Testimony of a Witness with Knowledge*.

(3) *Comparison by an Expert Witness or the Trier of Fact*.

(4) *Distinctive Characteristics and the Like*.

Testimony of a Witness with Knowledge

When the Plaintiff or Defendant bad actor says: “It Wasn’t Me!!”

Orville Richard Burrell a/k/a “Shaggy”

Authentication – “Personal Knowledge”

“Knowledge” is liberally construed

(1) Someone who saw or printed out post / photo

(2) Custodian of Records for Social Media Provider

(3) IT or other Employee familiar with computer / networking systems

Comparison by an Expert or Trier of Fact

- Witness denies creating post or tweet, but . . .
- You have another post or tweet the witness has admitted creating
- Show similarities to show court that the jury could conclude it was created by the same author

Distinctive Characteristics and the Like

- Most common way of authenticating social media evidence
- Documents contain info and facts peculiar to the knowledge of that person
  - Birthday
  - Family members and names
  - Nickname
  - Screen name
  - Contact e-mail or phone number
  - Location
  - Personal photos
  - Employment
  - Vacation and Leisure

Self Authentication of Electronic Evidence FRE 902 (13) and (14)

- ***FRE 902 amended effective December 1, 2017***
- ***No Texas equivalent***

FRE 902 (13) Certified Records Generated by an Electronic Process or System.

A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

Example - data from hard drive, e-mail, etc

FRE 902 (14) Certified Data Copied from an Electronic Device, Storage Medium, or File.

Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule (902(11) or (12). The proponent also must meet the notice requirements of Rule 902 (11).

Example - copies of data from a webpage, posting, tweet, etc

Self Authentication Certifications

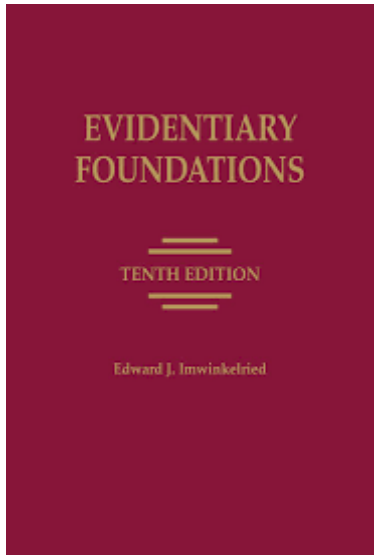
- ***Certified by "Qualified" Person, but no clear definition of qualifications;***
- ***Certification must meet other requirements set forth in 902(11) and (12) (business records requirements);***
- ***Notice Requirement -*** reasonable notice must be given to the adverse party of intent to offer the record. Written notice must allow the record and certification to be available for inspection, so that the party has a fair opportunity to challenge them.

Caveat of 902 (13) and (14)

Committee Notes

"A certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation. For example, assume that a plaintiff in a defamation case offers what purports to be a printout of a webpage on which a defamatory statement was made. Plaintiff offers a certification under this Rule in which a qualified person describes the process by which the web page was retrieved. Even if that certification sufficiently establishes that the webpage is authentic, defendant remains free to object that the statement on the webpage was not placed there by defendant. Similarly, a certification authenticating a computer output, such as a spreadsheet, does not preclude an objection that the information produced is unreliable—the authentication establishes only that the output came from the computer."

So How Do You Authenticate Evidence?



Sample predicate for witness who has knowledge about a social media page/post

- How do you know the plaintiff / supervisor (P/S)?
- Are you aware of the P/S maintaining any social media accounts?
- How do you know the P/S maintains this account?
- Are you “friends” with this person on any social media accounts?
- Have you visited his/her page on this account?
- How many times?
- Talked to the P/S about his/her social media page? Explain
- Have you communicated or messaged with the P/S through his/her social media account? Explain. How many times?
- Are you aware of anyone having access to the P/S’s account password?

Show the witness the exhibits marked for identification purposes

- Have you seen what is marked as P/D’s Exh ___ for identification purposes before?
- Where have you seen them?
- When did you see them?
- What are they?

- What types of information is on this pages? (Go over info peculiar to the knowledge of the P/S)
  - Birthday
  - Family members and names
  - Nickname
  - Screen name
  - Contact e-mail or phone number
  - Location
  - Personal photos
  - Employment
  - Vacation and Leisure
- Is the information contained on these pages accurate as it relates to the P/S?
- How do you know?
- Are P/D Exh ___ for ID purposes true and correct copies of what you saw / printed out on this account?

  Move to offer

  Anticipated Objection – counsel failed to prove that plaintiff/defendant actually posted this, or that no one else had access to his/her device or password

  Response – Your Honor, we have laid out a “prima facie showing” of authenticity under 901(b) by showing that plaintiff/supervisor maintained this account; this witness was familiar with the account and had interacted with P/S’s account in the past; that the pages from this account contained information peculiar to the knowledge of the P/S. Opposing counsel’s arguments go to the weight of the evidence for the jury to determine, and not to its admissibility.

Lorriane v. Markel American Insurance Co.
241 F.R.D. 534 (D. Md. 2007)

Authenticating Websites

Lorraine at 555-56

There are three questions that must be answered

(1) What was actually on the website? (explicitly or implicitly)

(2) Does the exhibit or testimony accurately reflect it?

(3) If so, is it attributable to the owner of the site?

Other factors that may influence the court

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

Computer Stored Records and Data

Can be authenticated by (1) Custodian of Records; or (2) Witness familiar with the record keeping system of the organization to confirm requirements of 803(6) (hearsay exception for records kept in the ordinary course of business)

Lorriane cites Prof Imwinkeried 11 elements for laying the foundation:

1. The business uses a computer (or computer / networking system);
2. The computer (or computer / networking system) is reliable;
3. The business has developed a procedure for inserting data into the computer (or computer / networking system);
4. The procedure has built-in safeguards to ensure accuracy and identify errors;
5. The business maintains the computer (or computer / networking system);
6. The witness had the computer (or computer / networking system) provide certain data;
7. The witness used the proper procedures in obtain this data;
8. The computer (or computer / networking system) was in working order at the time the data was obtained;
9. The witness recognizes the exhibit as the data;
10. The witness explains how he/she recognizes the data;
11. If the data contains foreign symbols or terms, the witness explains these to the trier of fact.

Edward J. Imwinkelried, *Evidentiary Foundations*, §4.03(2) (Mathew Bender 10th ed. 2018).

Sample Predicate Questions for Employee Familiar with Computer/Networking System

- Background (name; education; employer; date of hire; job duties)
- How are records (or specific data) maintained at company xyz?
- Explain the computer / networking systems used by company?
- What hardware does the company use?
- For how long has this been used?
- Do you find it to be dependable? Explain
- What kind of software does the company use?
- For how long has this been used?
- Do you find it to be dependable? Explain
- What personnel has access to this system? Explain
- How are personnel trained to use / input in this system?
- Who conducts training?
- How much training is personnel given?
- What procedures does the company have for using its computer / networking system to create and maintain these records / data?
- Who is involved in maintaining these records / data?
- How are these records / data maintained and preserved?
- Have they been altered or changed since they were originally created?
- How can you verify that?

- Have I asked you to retrieve and bring (describe records/data) with you for this case?
- What did you bring?
- How was it obtained? By whom? When?
- How did you verify the records / data are accurate?
- Your Honor, I would like to show the witness what has been marked for identification purposes as Plaintiff's/Defendant's Exh __.
- Do you recognize Exh___ for identification purposes?
- How?
- (If foreign symbols or terms) Can you explain to the court what these symbols or terms mean?
- Is Exh___ for identification purposes a true and correct copy of the records / data maintained by company xyz?
- Was these records kept in the course of regularly conducted activity of business? (and other predicated under FRE 803(6)
- Your Honor, we offer Exh ____ into evidence.

Digital Photos

Sample predicate areas for an expert on digital enhancement

(1) The witness is an expert in digital photography;

(2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the process by which the computer manipulates them;

(3) the witness testifies that the processes used are valid;

(4) the witness testifies that there has been “adequate research into the specific application of image enhancement technology involved in the case”;

(5) the witness testifies that the software used was developed from the research;

(6) the witness received a film photograph;

(7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer;

(8) the witness can identify the trial exhibit as the product of the enhancement process he or she performed.

Tienda v. State

358 S.W.3d 633 (Tex. Crim. App. 2012)

Ronnie Tienda

Evidence Presented by the State

State subpoenaed myspace.com for general subscriber report

- According to the subscriber reports, two of the MySpace accounts were created by a “Ron Mr. T,” and the third by “Smiley Face,” which is the appellant's widely-known nickname.
- The account holder purported to live in “D TOWN,” or “dallas,”
- and registered the accounts with a “ronnietiendajr@” or “smileys_ shit @” email address.

Testimony of Victim's sister

- how she was aware of the Defendant's accounts
- how she knew the Defendant maintained the account
- Testified about the contents of the account
- She identified each print out and explain what they were (namely declarations from the defendant)
- She identified each photos associated with the page and identified the defendant (also showed gang related tattoos and hand gestures)

State showed that the e main profile pages of the MySpace accounts contained quotes boasting about activities that could be determined by a jury as being related to the murder in question

- “You aint BLASTIN You aint Lastin”
- “I live to stay fresh!! I kill to stay rich!!”
- Under the heading “RIP David Valadez” was a link to a song that was played by Valadez's cousin at Valadez's funeral.
- Another music link posted to one of the profiles was a song titled “I Still Kill.”
- The instant messages exchanged between the defendant and other unidentified MySpace users included specific references to other passengers present during the shooting, circumstances surrounding the shooting, and details about the State's investigation following the shooting.
- messages that made specific threats to those who had been “snitchin” and “dont run shit but they mouth,”
- assigning blame to others for being the “only reason im on lock down and have this shit on my back.”
- The author also generally boasted to another user that “WUT GOES AROUND COMES AROUND” and “U KNO HOW WE DO, WE DON'T CHASE EM WE REPALCE EM.” The author accused: “EVERYONE WUZ BUSTIN AND THEY ONLY TOLD ON ME.”
- Several of the instant messages also complained about the author's electronic monitor, which was a condition of the appellant's house arrest while awaiting trial.

But what about the possibility the account was hacked?

Texas Court of Criminal Appeals response:

“It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted boastful messages about David Valadez's murder and the circumstances of that shooting, was aware of the music played at Valadez's funeral, knew when the appellant was released on pretrial bond with electronic monitoring and referred to that year-long event along with stealing the photograph of the grinning appellant lounging in his chair while wearing his ankle monitor. 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 appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages.”

One more thing . . .