# ELECTRONIC EVIDENCE:
# CLOUDY WITH A CHANCE OF DATA

*Presented by:*
**HON. EMILY MISKEL,** *McKinney*
470th District Court

*Co-author:*
**T. HUNTER LEWIS,** *Dallas*
Orsinger, Nelson, Downing & Anderson, LLP

State Bar of Texas
**43RD ANNUAL**
**ADVANCED CRIMINAL LAW COURSE**
July 17-20, 2017
Houston

**CHAPTER 35**

# HON. EMILY A. MISKEL

Judge, 470th District Court, Collin County, Texas
emily@emilymiskel.com ▪ www.emilymiskel.com

## BIOGRAPHICAL INFORMATION

### EDUCATION

**Harvard Law School**, J.D.
**Stanford University**, B.S., Mechanical Engineering, with distinction

### PROFESSIONAL AFFILIATIONS

State Bar of Texas, Pattern Jury Charge Oversight Committee, 2017-2020
Texas Center for the Judiciary, Finance Committee
Henderson Inn of Court, Barrister
Texas Academy of Family Law Specialists (TAFLS), Member
Harvard Club of Dallas, Vice President – Law School

### PROFESSIONAL RECOGNITION

Board Certified, Family Law — Texas Board of Legal Specialization
Joseph McKnight Award for Best Article, Family Law Section of the State Bar of Texas, 2016
Exemplary Article Award, Texas Center for the Judiciary, 2016
Texas Bar Foundation Fellow
Super Lawyers Rising Star, 2012-2015
D Magazine Best Lawyers in Dallas, 2015
Best Lawyers in America, 2016

Author of the book INTERCEPTION: A PRACTICAL GUIDE TO WIRETAPPING AND INTERCEPTION LAWS FOR CIVIL AND FAMILY LAW ATTORNEYS (Amazon 2014, Barnes & Noble 2015).

## RECENT PUBLICATIONS AND PRESENTATIONS

*Wiretapping and Electronic Torts*, Frisco Bar Association Meeting (2017).
*Illegal Evidence - Wiretapping, Hacking, and Data Interception*, Sex Drugs & Surveillance Course, State Bar of Texas (2017).
*Social Media and the Law*, guest lecturer, Southern Methodist University (2017).
*Revenge Porn & Other New Causes of Action*, Dallas Minority Attorney Program, Dallas Bar Association (2017).
*My Rights and Responsibilities*, Plano Youth Leadership Program (2017).
*Revenge Porn and Other New Causes of Action for Family Law*, San Antonio Bar Association Family Law Section Meeting (2017).
*Digital Dirt—The Impact of Social Media on Your Case*, Innovations: Breaking Boundaries in Custody Litigation Course, State Bar of Texas (2017).
Presiding Judge, 2017 Trial Institute, Texas Academy of Family Law Specialists (2017).
*Advice from Judges on How to Present Your Case in Any Texas Court*, Handling Your First (or Next) Divorce Case Course, State Bar of Texas (2017).
*Online Impersonation, Revenge Porn, and Other New Causes of Action*, Family Law & Technology Course, State Bar of Texas (2016).
Planning Committee, Sex, Drugs & Surveillance Course, State Bar of Texas (2016-2017).
*Reunification Therapy and Court Orders: Best Practices to be on the Same Page*, 12th Symposium on Child Custody Evaluations, Association of Family and Conciliation Courts (2016).
*The Trial Lawyers Toolbox – Technology Tools for Litigation*, Technology for Litigators Course, State Bar of Texas (2016).
Planning Committee, Advanced Family Law Course, State Bar of Texas (2016-2017).
*Peeping Toms in the New Millennium: Digital Dos and Don'ts*, New Frontiers in Marital Property Course, State Bar of Texas (2016).
*Restraining Orders, Protective Orders, and Peace Bonds*, Collin County Council on Family Violence (2016).
Course Director, Handling Your First (or Next) Divorce Case Course, State Bar of Texas (2016-2017).
*Prepare and Present a Case for Final Trial*, Family Law 101 Course, State Bar of Texas (2016).
*Cloudy with a Chance of Data*, Advanced Criminal Law Course, State Bar of Texas (2016).
*From Private Practice to the Bench: Practice Management Tips*, Law Practice Management Section, Collin County Bar Association (2016).

****Complete list available at www.emilymiskel.com****

# TABLE OF CONTENTS

I. INTRODUCTION. ..... 1

II. ACQUIRING ELECTRONIC EVIDENCE. ..... 1
A. Acquiring Cell Phone Content ..... 1
1. Cellebrite Touch. ..... 1
2. Reasonable Expectation of Privacy in Phone Data and Law Enforcement Searches Incident to Arrest. ..... 1
3. iCloud Accidental Sharing. ..... 2
B. Recovering Deleted Data. ..... 2
1. Forensic Data Recovery ..... 2
2. Recovering Deleted Data by the Home User. ..... 2
3. iTunes Backup on Computer: ..... 3
C. Acquiring Social Media Content ..... 3
1. Expectation of Privacy in Online Communications. ..... 3
2. X-1 Social Discovery Software. ..... 3
3. Archive Social. ..... 3
4. Next Point Social Media Collection. ..... 3
5. Hanzo Social Media Collection. ..... 3
6. Downloading a User's Own Social Media Data. ..... 3
D. Discovery Tools ..... 4
1. Acquiring User Content from Service Providers ..... 4
2. Your Client's Own Social Media ..... 4
3. Spoliation Letters ..... 4
4. Discovery Requests ..... 4
E. Illegal Ways to Obtain Data ..... 5
1. Wiretapping ..... 5
2. Intercepting Communications ..... 5
3. GPS Monitoring ..... 5
4. Illegally-Obtained Data not Admissible in Criminal Trials ..... 5

III. ANALYZING DATA. ..... 5
A. Faked and Forged Evidence ..... 5
1. Fake A Baby ..... 5
2. Cell Phone/Text Spoofing ..... 5
3. Fake Document Services ..... 6
4. Disappearing Text Apps ..... 6
B. Computer Software Analysis ..... 6
C. Encryption ..... 6

IV. AUTHENTICATION & IDENTIFICATION. ..... 7
A. Admitting Electronic Evidence Under Existing Rules. ..... 7
B. Electronically Stored Information (ESI) ..... 7
C. Tienda v. State (Tex. Crim. App. 2012) ..... 7
D. Email ..... 10
E. Reply-Letter Doctrine ..... 11
F. Text Messages. ..... 11
G. Internet Website Postings. ..... 12
H. Tinder and Other Online Personals ..... 13
I. Facebook. ..... 13
J. Chat Room Content. ..... 14
K. Stored versus Processed Data ..... 15
L. Computer Stored Records and Data. ..... 15
M. Digital Photographs and Videos. ..... 16
1. Original Digital Photograph. ..... 17
2. Digitally Converted Images. ..... 18

3. Digitally Enhanced Images. ..... 18
N. Voicemail or Other Audio Recordings. ..... 19
O. Conclusion on Authenticating ESI. ..... 19

V. BEST EVIDENCE RULE. ..... 19

VI. RULE OF OPTIONAL COMPLETENESS. ..... 20

VII. HEARSAY ISSUES IN ELECTRONIC EVIDENCE. ..... 20
A. Unreflective Statements. ..... 21
1. Present Sense Impression. ..... 21
2. Excited Utterance. ..... 21
3. Then Existing Mental, Emotional, or Physical Condition. ..... 22
B. Reliable Documents. ..... 22
1. Recorded Recollection. ..... 22
2. Records of Regularly Conducted Activity. ..... 22
3. Market Reports, Commercial Publications. ..... 23
C. Statements That Are Not Hearsay. ..... 23
1. Computer Generated "Statements." ..... 23
2. Metadata ..... 24
3. Admissions by a Party-Opponent. ..... 24

VIII. WITNESSES. ..... 24
A. Writing Used to Refresh Memory. ..... 24
B. Impeachment. ..... 25
1. Prior Inconsistent Statement. ..... 25
2. Impeaching Hearsay Statements ..... 25
C. Character Evidence. ..... 25

IX. UNFAIR PREJUDICE. ..... 26

X. EXPERT TESTIMONY AND OPINIONS. ..... 26
A. Basis of Expert Testimony and Opinions. ..... 26
B. Factors Relied Upon. ..... 26
C. Jury Trials ..... 27

XI. DEMONSTRATIVE EVIDENCE. ..... 27

XII. CONCLUSION ..... 28

# ELECTRONIC EVIDENCE: CLOUDY WITH A CHANCE OF DATA

## I. INTRODUCTION.

Social media has quickly become one of the most common means by which a person expresses himself publicly. With the invention of Twitter, LinkedIn, Facebook, Instagram, and countless other applications, people are airing their thoughts, intentions, locations, and feelings to the public quite often. While social media is prevalent in many adversarial hearings, there are several forms of additional evidence that courts are beginning to see which illustrate the need for important foundational evidence and procedures in order to authenticate electronic evidence.

Attorneys may sometimes feel uncertain about using or working with social media. Rest assured that your clients, witnesses, and opposing parties do not feel the same hesitation! As social media outlets become more popular among litigants, it becomes necessary for the advanced practitioner to not only understand what electronic evidence is available, but also how to acquire it and admit for evidentiary purposes. This includes evidence that is computer generated, evidence that is electronically stored, and social media or internet evidence. In this paper, we will frequently refer to "ESI" which stands for "Electronically Stored Information."

This paper will cover electronic evidence from how to acquire it, how to analyze what you've got, and how to admit and use the evidence at trial.

## II. ACQUIRING ELECTRONIC EVIDENCE.

One of the pleasures of litigation is finding and using a party's own words to prove that the party is a liar, is violating court orders, or, in the period prior to the current court proceeding, was displaying a persona and attributes that are not consistent with what that party chooses to convey now. You just hope that the leopard trying to change his spots is not YOUR client.

Often, electronic evidence is highly public and easily obtainable. However, at times, you may want to acquire privately-held electronic evidence from computers, phones, or password-protected accounts.

Clearly the most fertile field for out-of-court statements that may have a damning influence in a criminal case is social media postings. Not surprisingly, tools have been developed to make the collection of such data easier and also address authenticity and chain-of-custody challenges. Many of these tools may prove significant weapons for the criminal law attorney who is seeking to recover or review any and all evidence that could be used against his client by the State.

### A. Acquiring Cell Phone Content

1. Cellebrite Touch.

The Cellebrite Touch device can perform logical and physical extraction capabilities for mobile phones, smartphones, portable GPS devices and handheld tablets. There are portable "field" devices that allow the technician to go to anywhere the phone or device may be and to do the extraction there—for example, a courtroom. There are also more powerful lab devices.

The device performs a forensic download complete with chain of custody authentication by a certified examiner. The capture may be followed by an in-camera review of the data to preserve attorney-client privilege or to possibly ferret out other inadmissible or irrelevant information. Sometimes courts delegate this task to a discovery master.

The data captured from the phone will include the Facebook and Twitter posts, emails, and other data either "natively" on the phone or preserved in memory caches that have not yet been overwritten. Many times data intentionally deleted from a phone can be recovered just like with a computer.

Be aware that it can be impossible to obtain data from encrypted devices unless the password is provided. For more detail about encryption, see the section below.

2. Reasonable Expectation of Privacy in Phone Data and Law Enforcement Searches Incident to Arrest.

Both the United States Supreme Court[1] and Texas Court of Criminal Appeals[2] have recognized that cell phone users can have a reasonable expectation of privacy in the content of their cell phones, noting the plethora of highly personal information that may be found there, and suggesting a certain unique relationship between owner and cell phone. The Supreme Court remarked that cell phones "place vast quantities of personal information literally in the hands of individuals" and "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[3] "Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly

[1] *See Riley v. California*, 573 U.S. ___, 134 S.Ct. 2473, 2489, 189 L.Ed.2d 430 (2014) ("The term `cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

[2] *State v. Granville*, 423 S.W.3d 399, 417 n. 66 (Tex. Crim.App.2014) (noting the different relationship people have with their phones than they did in the past).

[3] *Riley*, 134 S.Ct. at 2484-85.

three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."[4]

In *Riley v. California*,[5] the United States Supreme Court held that the warrantless search and seizure of the digital contents of a cell phone during an arrest is an unconstitutional violation of the fourth amendment. Prior law permitted law enforcement to search the body of the arrested person and the area into which he might reach, without a warrant, incident to the arrest. In the cases before the court, police had searched arrestees' cell phones to obtain pictures, contacts, texts, call logs, and video clips. The Supreme Court concluded that a warrant is required to search a cell phone.

The 2014 *Granville*[6] case from the Texas Court of Criminal Appeals addressed whether a person retains a legitimate expectation of privacy in the contents of his cell phone while the phone is temporarily stored in a jail property room. A high school student was arrested for causing a disturbance on the school bus. His cell phone was taken from him during booking and placed in the jail property room. The school resource officer who was not involved in the arrest drove to the jail, retrieved the phone, and examined its contents without a warrant. The Court held that a person does not lose all privacy protection when property is in a jail property room, and that a person retains a reasonable expectation of privacy in his cell phone.

3. iCloud Accidental Sharing

iCloud can allow text messages, contacts, and more to be shared across multiple devices. If devices are set up on the same Apple ID or iCloud account, the information will automatically update and be available on all devices.

An issue that is more commonly appearing in family law cases is that a party will realize that the iPad bought for the child to use now has access to mommy or daddy's texts, photos, and more. This may let one spouse or parent spy on the other, obtaining information intended to be private but unknowingly revealed.

There is insufficient guidance from higher courts as to whether there is anything improper about using evidence obtained in this manner.

**B. Recovering Deleted Data.**

When computers or devices store data, they keep track of where files are by using "pointers." The pointer tells the computer where each file's data begins and ends on the hard drive. When a file is deleted, the computer just deletes the pointers and indicates that those portions of the drive are now available. The data will remain on the drive until it is actually overwritten. It can even be possible to recover data that has been overwritten. To ensure that a file is permanently deleted and cannot be recovered, programs like Eraser, CCleaner, and FileShredder will write new data over the old data multiple times.

1. Forensic Data Recovery

Forensic professionals can analyze devices and recover data even after it's been deleted. For example, forensic professionals can recover deleted files and data from hard drives, the cloud, servers, computers, mobile devices, and more.

2. Recovering Deleted Data by the Home User.

The benefit of using a forensic professional to recover data is that they have chain-of-custody procedures, they recover the data in a forensically-verifiable format, and there is an expert witness available to testify that the process leads to a reliable result. However, your client may not have the budget for a forensic professional. A client can recover data from a device in his or her possession using tools easily available over the internet. Be aware that these methods may give you problems with authentication at trial, but with enough knowledge about how these programs work, your clients may be able to authenticate the evidence.

**iPhone:**

The latest iPhone OS has a feature to easily recover recently-deleted photos from the last 30 days. In the Photos App, there is an album for "Recently Deleted" photos that may be recovered or permanently deleted.

**Apps:**

Apps are available that can recover deleted information directly on the phone itself, for example, the DiskDigger app for Android. The user downloads and installs the app from the Google Play store. Then the app can be used to scan the device and recover recently-deleted files.

**Desktop Programs:**

Continuing to use a device increases the risk that deleted data will be overwritten and lost. Many data recovery tools are desktop computer programs. The phone will have to be connected to the desktop, and the desktop program will use the computer to scan the phone. This helps reduce data loss. Options include programs like Dr. Fone, Kvisoft, and PhotoRec. As a personal anecdote, I accidentally wiped a phone that I realized contained baby photos. I downloaded a data

[4] *Id*. at 2490.

[5] *Riley v. California*, 573 U.S. ___, 134 S.Ct. 2473, 2489, 189 L.Ed.2d 430 (2014)

[6] *State v. Granville*, 423 S.W.3d 399 (Tex. Crim.App.2014)

recovery program for about $35, and it recovered photos that had been deleted years previously.

3. iTunes Backup on Computer:

If an Apple user has ever connected the device to a computer with iTunes, an enormous amount of data can be obtained from that computer, even without access to the device. For example, it is possible to obtain call logs, text messages, contacts, email, calendar, photos, web history, Google Maps info, GPS tracking data, passwords, and app data (Facebook, etc). A forensic professional is capable of retrieving and analyzing this data. A home user can also use software such as iPhone Spy Python, to accomplish this, with the caveat that the home user may experience authentication issues.

**C. Acquiring Social Media Content**

1. Expectation of Privacy in Online Communications.

Courts continue to grapple with the intersection of the 4th Amendment with online communications. There are no Texas cases that directly address which communications are private and which are not. A search of federal cases reveals that the degree to which a communication is public reduces a person's reasonable expectation of privacy. For example:

- Accessing a defendant's profile on Facebook through a cooperating witness is not a violation.[7]
- No reasonable expectation of privacy in an email once it has been forwarded.[8]
- No reasonable expectation of privacy in communications sent in an internet chat room.[9]
- No reasonable expectation of privacy in a publicly-posted Tweet.[10]
- Private direct messages and private chats may retain some protection.[11]

In summary, it appears that the extent to which communications are made public will determine their protection under the 4th Amendment.

2. X-1 Social Discovery Software.

X-1 is a software product which aggregates social media data in real time. This product differs from other methods of capture that typically only archive or image a specific social media account at a particular time. Therefore, because X-1 can crawl, it can capture and instantly search contents from websites, web mail, You Tube, Facebook, Twitter, and other web posts. It may capture even the Facebook "one time only viewing" that "disappears" after one use.

X-1 is expensive; a single license costs over $1,000 per year. The software can be set up to track many "persons of interest." The software is designed to accommodate legal uses and attorneys' needs. It archives and preserves the data in a forensically accurate and verified way that enhances authenticity and admissibility. The archived data is also optimized for keyword searching and producing in response to discovery requests.

3. Archive Social.

Archive Social is a social media archiving solution for recordkeeping and compliance for companies. It provides for 100% capture of social media in pure native format that satisfies legal requirements and insures compliance with industry standards. It is used by banks and the like, and is intended for banks and other large institutions to be able more easily to produce their social media generated from their businesses such as Facebook, Twitter, You Tube and LinkedIn in a manner that complies with subpoenaed requests for information.

4. Next Point Social Media Collection.

This tool gives lawyers the ability to collect websites, social media, blog content and immediately begin reviewing it for purposes of litigation. The software automatically collects, preserves, archives and indexes online content including social media and provides a comprehensive fully searchable archive of online data.

5. Hanzo Social Media Collection.

Hanzo's social media collection and preservation for e-discovery software is designed to do the same collection and preservation of web content. It has a subspecies Hanzo-On-Demand for single instance collection, preservation, and production of websites, web pages, Facebook, Twitter, Linked In, You Tube and other social media sites when required as evidence in litigation. It allows for the immediate capture of requested web content and can export to high end litigation support systems.

Internet Evidence Finder is another tool that does similar mining in or on websites or social media accounts.

6. Downloading a User's Own Social Media Data.

Services like Facebook and Twitter provide a way for the user to download their own social media data. This information can be requested in discovery from opposing parties or even third parties and witnesses.

---

[7] *U.S. v. Meregildo*, 883 F.Supp.2d 523, 525 (S.D.N.Y. 2012).

[8] *U.S. v. Charbonneau*, 979 F.Supp. 1177, 1184 (S.D. Ohio 1997).

[9] *Id.* at 1185.

[10] *People v. Harris*, No. 2011NY080152, 2012 WL 2533640, *4 (N.Y. City Crim. Ct. June 30, 2012).

[11] *Id.*

Facebook's website indicates the following instructions for downloading a user's own data:

1. Click at the top right of any Facebook page and select Settings
2. Click Download a copy of your Facebook data below your General Account Settings
3. Click Start My Archive

In practice, the process requires multiple logins to both the Facebook account and the associated email account. It can take an hour or longer to complete the process. Although information from the download includes photos, friends, posts, messages, etc., it may not include 100% of a person's Facebook account. If a person has used a third-party app to access their Facebook page, some of the information may not show up in the archive, depending on the application used. Additionally, the archive may not contain deleted messages.

Twitter's website gives the following instructions for downloading an archive of a user's own data:

1. Go to your account settings by clicking on the profile icon at the top right of the page and selecting Settings from the drop-down menu.
2. Click Request your archive.
3. When your download is ready, we'll send an email with a download link to the confirmed email address associated with your Twitter account.
4. Once you receive the email, click the Go now button to log in to your Twitter account and download a .zip file of your Twitter archive.
5. Unzip the file and click index.html to view your archive in the browser of your choice.

Please note: It may take a few days for us to prepare the download of your Twitter archive.

If you are going to ask your client to do this process or if you are going to request in discovery that a witness or opposing party do this, you are advised to test out the process yourself first. That way you can craft better discovery requests and clearly explain to a court what you've asked the person to do.

**D. Discovery Tools**

1. Acquiring User Content from Service Providers

The Stored Communications Act, a federal law, prohibits companies from disclosing customers' electronic communications or records in response to a civil subpoena. This means, for example, that you cannot send a civil subpoena to a phone company to obtain text messages. A private party cannot subpoena Facebook to obtain user posts. This is often a real bar to obtaining this information in civil cases. However, there are several exception contained in the law that allow online providers to produce user content in response to a criminal investigation or trial. A governmental entity may use a warrant, administrative subpoena, grand jury subpoena, or trial subpoena to obtain information directly from the online service. A private party does not have the same ability to use such subpoenas.

2. Your Client's Own Social Media

Attorneys should have a frank discussion with clients, as early as the first meeting, about what social media the client uses. This can be helpful to anticipate what evidence may be used against your client, and also to help your client avoid creating new problems in the future.

It is important for attorneys to be conscious not to tell a client to destroy any social media evidence. In a personal injury case, after the defendant sent a request for production of social media information, a Virginia lawyer instructed a paralegal to tell his plaintiff client to clean up his Facebook page. The attorney was assessed $722,000 in legal fees and a five-year suspension of his law license.

An attorney can advise a client to use privacy settings, however an attorney must not advise a client to destroy or remove social media evidence. The data can be made private so long as it is preserved and, if requested, is produced.

An attorney can also advise a client to avoid creating new harmful posts, photos, and evidence that may be used against that client!

3. Spoliation Letters

As discussed above, private parties cannot obtain user content directly from service providers. However, if there is any other party or witness that may have relevant information, it can be a good idea to send a spoliation letter, putting the person on notice that they have a duty to preserve evidence and not delete it. If a party can prove that evidence was spoliated, the party may be entitled to a presumption that the destroyed evidence was unfavorable to the spoliator. Under Texas law, the trial court must determine whether the destroyer had a duty to preserve the evidence. It is much easier to prove this element if you have explicitly put the person on notice of the litigation and requested that they preserve specific categories of relevant evidence.

4. Discovery Requests

Electronic information is subject to discovery requests just as traditional paper documents. There are some pitfalls that an attorney should be careful to avoid. If a request is too general, the receiving party may not understand that specific electronic information is responsive. If you are looking for something

specific, go ahead and spell it out. For example, if you want a party to download and produce his Twitter archive, set forth the instructions in the discovery request. It is all too common for a blanket request to not include ESI requests.

If the request is too general, there may be a significant charge for the production of the data.

You have the right to request and obtain electronic information in native format. A digital photograph file may contain significantly more information than a printout of a photo, including date and time, GPS location, and more.

### E. Illegal Ways to Obtain Data

Although it is beyond the scope of this paper, attorneys should be aware that certain means of collecting electronic evidence are illegal and inadmissible. For more information, please see the other papers on the topic written by Judge Miskel, available from the State Bar of Texas or on emilymiskel.com.

1. Wiretapping

Federal and Texas wiretapping laws are "one-party consent" laws. That means that a person can record any conversation she is part of. However, it is illegal to record or intercept communications of others without their consent. For example, you cannot place a bug in a car or room to record conversations that occur when you are not there.

New technology is creating opportunity for wiretapping issues. Apps such as Auto Forward Spy, Spyera, and more, allow a person to intercept and monitor cell phone conversations. Using these apps can be a crime, and the evidence is inadmissible. Further, there can be civil and criminal penalties against attorneys for using or disclosing information that was obtained through wiretapping. Be very cautious about wiretapped evidence.

2. Intercepting Communications

The apps mentioned above also allow a person to gain full access to text messages, call logs, browser history, and more. While this information may not be considered wiretapping, it may also be prohibited by the Stored Communications Act, the Computer Fraud and Abuse Act, and other state and federal laws.

3. GPS Monitoring

Apps also frequently allow for GPS monitoring. Texas Penal Code § 16.06 makes it an offense to install a tracking device on a motor vehicle owned or leased by another person. However, the law may not apply to tracking apps on cell phones.

4. Illegally-Obtained Data not Admissible in Criminal Trials

Texas Code of Criminal Procedure § 38.23 prohibits illegally-obtained evidence from being admitted in a criminal trial. However, illegally-obtained evidence is admissible in civil trials. Attorneys should be aware that there may be a consequence to any associated civil cases that the client may have, including custody cases or other cases where civil liability is an issue.

The federal and Texas wiretapping laws have a strict exclusionary rule. If any evidence is obtained through wiretapping, that evidence plus any fruit of the poisonous tree cannot be used for any purpose at any proceeding, including civil proceedings.

## III. ANALYZING DATA.

Many times production can be produced and received electronically and should be parsed and looked at in an efficient electronic manner. Computer tools to parse this data. But the massive data requested – and sometimes received – may invite the hiring of a third party expert to be the one who conducts the data parsing or even authenticates it.

### A. Faked and Forged Evidence

As discussed below, electronic evidence is not assumed to be more or less reliable than traditional documentary evidence. Documents, letters, and photos have always been capable of forgery or misleading editing. While there is no presumption or higher burden for admissibility for electronic evidence, the fact remains that all evidence may be faked. As discussed in the *Tienda* case below, once the party introducing the evidence makes a threshold showing of admissibility, questions about the legitimacy of the evidence go to its weight and credibility, not admissibility. Attorneys and courts should not be overly skeptical of internet evidence, but should retain a willingness to consider evidence that a particular document has been faked.

1. Fake A Baby

While troubling, there are now providers online capable of faking "spoof" medical records. "Fake a Baby," found online at www.fakeababy.com, sells fake ultrasounds, fake sonograms, fake pregnancy tests, fake DNA tests and even fake pregnancy bellies. The company maintains that its purpose is novelty-only and has been responsive to discovery requests.

2. Cell Phone/Text Spoofing

Cell phone spoofing allows a caller to create a fake or "spoofed" number to send SMS messages from, or make and receive calls.

The concept can be legitimate, as when attorneys use a Google Voice number to make cell phone calls or

send texts from a different number that will not display their personal cell phone number to clients. However, call and text spoofing can be used maliciously.

The FTC is increasingly receiving complaints that fraudulent telemarketers and debt collectors are making calls from innocent phone numbers. The owners of the actual phone numbers only find out that telemarketers and debt collectors are using their number when they begin to receive irate calls from victims.

Swatting is another dangerous trend. A person will call 9-1-1 from a spoofed number to report a phony dangerous situation such as a bomb threat, hostage situation, etc., at the house of the hoax's victim. SWAT teams will respond accordingly, leading to a potentially deadly situation for the victim.

Spoofing can also be used for malicious harassment and other illegitimate purposes. The caller ID and phone records of the recipient of the spoofed call will actually reflect the faked number, so spoofing can be hard to catch.

Under Tex. Penal Code § 33.07, online impersonation can be a misdemeanor or even a felony.

3. Fake Document Services

Several websites are offering services to allow financial documents to be forged, in whole or in part. For example, one party used the Replace Your Docs service (http://www.replaceyourdocs.com/) to alter his existing cell phone and credit card statements to remove objectionable contact numbers and charges. The website advertises the following services:

- Fake Documents – fake bank statements and utility bills, which can be used for proof of address. The service can add your own transactions, names, dates and addresses to documents and advertises "unlimited modifications and changes until you are satisfied."
- Document Editing Service - edit any existing document with the details you provide.
- Payroll Service - all figures calculated for you based on net/gross salary, which can be used as proof of income.
- Output options - digital copy emailed the same day in PDF format, printed copy delivered between 2-3 days

It would be unreasonably difficult to try to subpoena phone and financial statements directly from the provider in all cases. The main takeaway from this paper should be that you should have an appropriate level of skepticism. If you or your client has a gut feeling that documents have been forged, don't automatically discount it. It may be worth the money to subpoena documents to spot-check the records you're getting.

4. Disappearing Text Apps

Dozens of apps exist to make messages more private, such as SnapChat, Secret, and Cyber Dust. These messaging apps allow users to send and receive communications and photos that will be destroyed within minutes. The apps also disables the ability to forward or take screenshots of messages.

Although this can provide increased privacy for users, it may cause them to destroy relevant evidence in litigation and be subject to spoliation penalties. It is wise for attorneys to have frank discussions with clients about their use of social media and apps.

**B. Computer Software Analysis**

Evidence that is merely stored in a computer does not require forensic expert testimony for admissibility, However, evidence that is computer processed would require some testimony that the processing yields a reliable result. If computer processed evidence is important, there must be a competent witness who can show, among other things, chain of custody and that the process is reliable.

**C. Encryption**

Encryption is increasingly important, even in an everyday law practice. Although it is outside the scope of this paper, standards of practice for handling private health information under HIPAA and SB300 may require attorneys to be storing and transmitting such information in encrypted format. It is not currently required that attorney/client emails be encrypted or protected, but that topic comes up fairly frequently in attorney periodicals and may become a requirement as encryption becomes more commonplace.

Encryption takes the plain-text information on a device or storage drive and uses a computer algorithm to generate nonsense cypher text. Only by possessing the key (password) can the encrypted text be read. Attorneys are generally perceived to fear computers and new technology, so I don't expect that the average attorney looks forward to learning about and using encryption. However, it is professionally and personally useful, and it is relatively easy to use.

There are many consumer-level encryption tools. For example, Apple devices now use encryption as a standard feature. It is also possible to use encryption on Android devices. The Electronic Freedom Foundation provides a lot of information on their website for using encryption on your phone, USB drives, email, and more: https://ssd.eff.org/

This paper addressed forensic cell phone imaging above, and it is important to note that data cannot be forensically retrieved from encrypted cell phones without the password.

## IV. AUTHENTICATION & IDENTIFICATION.

The requirement of authentication or identification is a condition precedent to admissibility. This requirement is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.[12] Unless the evidence sought to be admitted is self-authenticating under Tex. R. Evid. 902, extrinsic evidence must be adduced prior to its admission. Rule 901(b) contains a non-exclusive list of illustrations of authentication that comply with the rule. A frequently-cited federal case, *Lorraine v. Markel Am. Insur. Co.*, has become an authority on the application of the rules of evidence to electronically-stored information (ESI).[13] This section quotes extensively from the case, including selections relevant to authenticating ESI:

### A. Admitting Electronic Evidence Under Existing Rules.

While electronic evidence and online communications feel like a new and unique area in evidence, they are evaluated under the same familiar rules judges have always used. State and federal courts have rejected calls to abandon the existing rules of evidence when evaluating electronic evidence. For example, a Pennsylvania court addressed the authentication required to introduce transcripts of instant message conversations:

> Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of [the rules of evidence and case law]....We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.[14]

While judges are right to be skeptical of electronic evidence, judges can forget that the same concerns are present with any type of evidence.

### B. Electronically Stored Information (ESI).

A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. This is not a particularly high barrier to overcome. For example, in *United States v. Safavian*, the court analyzed the admissibility of e-mail, noting, 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 only that there is sufficient evidence that the jury ultimately might do so.

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. 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. Obviously, there is no "one size fits all" approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges.

### C. Tienda v. State (Tex. Crim. App. 2012)

The Texas Court of Criminal Appeals released a 2012 opinion that dealt extensively with authenticating social media evidence. At the trial court level, the State introduced printouts of a MySpace profile allegedly belonging to the defendant and implicating him in a shooting. The issue of whether the MySpace pages were sufficiently authenticated by circumstantial evidence was appealed all the way to the Court of Criminal Appeals, which addressed the issue very specifically:

> Rule 901(a) of the Rules of Evidence defines authentication as a "condition precedent" to admissibility of evidence that requires the

[12] Tex. R. Evid. 901.

[13] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D.Md. 2007) (memo. op.).

[14] *In Re F.P.*, 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005).

> proponent to make a threshold showing that would be "sufficient to support a finding that the matter in question is what its proponent claims." Whether the proponent has crossed this threshold as required by Rule 901 is one of the preliminary questions of admissibility contemplated by Rule 104(a). The trial court should admit proffered evidence "upon, or subject to the introduction of evidence sufficient to support a finding of" authenticity. The ultimate question whether an item of evidence is what its proponent claims then becomes a question for the fact-finder—the jury, in a jury trial. In performing its Rule 104 gate-keeping function, the trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic. [15]

There is no specific procedure for authenticating each piece of electronic evidence; rather the means of authentication will depend on the facts of the case:

> Evidence may be authenticated in a number of ways, including by direct testimony from a witness with personal knowledge, by comparison with other authenticated evidence, or by circumstantial evidence. Courts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted and/or stored information, including information found on social networking web sites, the rules of evidence already in place for determining authenticity are at least generally "adequate to the task." Widely regarded as the watershed opinion with respect to the admissibility of various forms of electronically stored and/or transmitted information is *Lorraine v. Markel American Insurance Co.* There the federal magistrate judge observed that "any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances." Rather, as with the authentication of any kind of proffered evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case. [16]

The *Tienda* court reviewed the caselaw from other jurisdictions to list some methods by which electronic evidence had been authenticated:

> Like our own courts of appeals here in Texas, jurisdictions across the country have recognized that electronic evidence may be authenticated in a number of different ways consistent with Federal Rule 901 and its various state analogs. Printouts of emails, internet chat room dialogues, and cellular phone text messages have all been admitted into evidence when found to be sufficiently linked to the purported author so as to justify submission to the jury for its ultimate determination of authenticity. Such prima facie authentication has taken various forms. In some cases, the purported sender actually admitted to authorship, either in whole or in part, or was seen composing it. In others, the business records of an internet service provider or a cell phone company have shown that the message originated with the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have had access to the computer or cell phone. Sometimes the communication has contained information that only the purported sender could be expected to know. Sometimes the purported sender has responded to an exchange of electronic communications in such a way as to indicate circumstantially that he was in fact the author of the particular communication, the authentication of which is in issue. And sometimes other circumstances, peculiar to the facts of the particular case, have sufficed to establish at least a prima facie showing of authentication. [17]

The *Tienda* court also acknowledged that some courts have held electronic evidence to a higher standard of authentication than other forms of evidence:

---

[15] *Tienda v. State*, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) (internal citations omitted).

[16] *Id*.

[17] *Id*.

> However, mindful that the provenance of such electronic writings can sometimes be open to question—computers can be hacked, protected passwords can be compromised, and cell phones can be purloined—courts in other cases have held that not even the prima facie demonstration required to submit the issue of authentication to the jury has been satisfied. That an email on its face purports to come from a certain person's email address, that the respondent in an internet chat room dialogue purports to identify himself, or that a text message emanates from a cell phone number assigned to the purported author—none of these circumstances, without more, has typically been regarded as sufficient to support a finding of authenticity.[18]

In the *Tienda* case, the Court of Criminal Appeals found that the State presented sufficient circumstantial evidence to authenticate the MySpace pages and postings as those of the defendant:

> This combination of facts—(1) the numerous photographs of the appellant with his unique arm, body, and neck tattoos, as well as his distinctive eyeglasses and earring; (2) the reference to [the victim's] death and the music from his funeral; (3) the references to the appellant's [gang]; and (4) the messages referring to … the [MySpace] user having been on a monitor for a year (coupled with the photograph of the appellant lounging in a chair displaying an ankle monitor) sent from the MySpace pages … is sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the appellant. This is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them.[19]

The Court acknowledged the possibility that someone could have forged the pages to set up the defendant, but held that that issue was one for the fact-finder, not for the court as an authentication prerequisite:

> 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 [the victim's] murder and the circumstances of that shooting, was aware of the music played at [the victim'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.

The *Tienda* court also distinguished a previous Maryland decision which had listed three methods for authenticating internet postings:

> The Maryland Court of Appeals recognized that such postings may readily be authenticated, explicitly identifying three non-exclusive methods. First, the proponent could present the testimony of a witness with knowledge; or, in other words, "ask the purported creator if she indeed created the profile and also if she added the posting in question." That may not be possible where, as here, the State offers the evidence to be authenticated and the purported author is the defendant. Second, the proponent could offer the results of an examination of the internet history or hard drive of the person who is claimed to have created the profile in question to determine whether that person's personal computer was used to originate the evidence at issue. Or, third, the proponent could produce information that would link the profile to the alleged person from the appropriate employee of the social networking website corporation. The State of Maryland failed to take advantage of any of these methods in *Griffin*. And it is true that the State of Texas has likewise failed to utilize any of them in the appellant's case. Nevertheless, as we have explained, there are far more circumstantial indicia of authenticity in this case than in *Griffin*—enough, we think, to support a prima facie case that would justify admitting the evidence and submitting the ultimate question of authenticity to the jury.

[18] *Id*.
[19] *Id*.

**Practice Tip:** While caselaw on authenticating and admitting electronic evidence is still developing, practitioners may need to rely on cases from other jurisdictions. Research will show that authentication issues concerning many forms of electronic evidence and social media have been presented to the Court and unpublished opinions have been issued. Though no legal weight can be given to them, they can be used as a good frame of reference for argument purposes if authentication or admissibility becomes an issue.

However, a practitioner should always attempt to admit the evidence, even if caselaw from other jurisdictions appears to be against it. Texas law has sometimes followed, but sometimes distinguished federal law and the law of other states, so there's nothing to lose by at least attempting to authenticate the evidence, using as much circumstantial evidence as possible.

### D. Email

There are many ways in which e-mail evidence may be authenticated. An e-mail is properly authenticated if its appearance, contents, substance, or other distinctive characteristics, taken in conjunction with circumstances, support a finding that the document is what its proponent claims.[20] One well respected commentator has observed: [21]

> [E]-mail messages may be authenticated by direct or circumstantial evidence. An e-mail message's distinctive characteristics, including its 'contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances' may be sufficient for authentication. Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an email message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender's listed e-mail address. The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message. However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.

Courts also have approved the authentication of e-mail by the above described methods. *See, e.g.*:

- *Siddiqui*, 235 F.3d at 1322–23 (E-mail may be authenticated entirely by circumstantial evidence, including its distinctive characteristics);
- *Safavian*, 435 F.Supp.2d at 40 (recognizing that e-mail may be authenticated by distinctive characteristics 901(b)(4), or by comparison of exemplars with other e-mails that already have been authenticated 901(b)(3));
- *Rambus*, 348 F.Supp.2d 698 (Email that qualifies as business record may be self-authenticating under 902(11));
- *In re F.P.*, 878 A.2d at 94 (E-mail may be authenticated by direct or circumstantial evidence).

The most frequent ways to authenticate email evidence are:

- 901(b)(1) (person with personal knowledge),
- 901(b)(3) (expert testimony or comparison with authenticated exemplar),
- 901(b)(4) (distinctive characteristics, including circumstantial evidence),
- 902(7) (trade inscriptions), and
- 902(11) (certified copies of business record).

**Texas Note:** An email can be authenticated by testimony that the witness was familiar with the sender's e-mail address and that she had received the e-mails in question from him.[22] Another court enumerated several characteristics to consider when determining whether an e-mail has been properly authenticated, including:

(1) consistency with the e-mail address on another e-mail sent by the defendant;
(2) the author's awareness through the e-mail of the details of defendant's conduct;

[20] *Manuel v. State*, No. 12-09-00454-CR. (Tex.App.—Tyler 2011).

[21] *Lorraine*, 241 F.R.D. at 554-55.

[22] *Shea v. State*, 167 S.W.3d 98, 105 (Tex.App.—Waco 2005, pet. ref'd).

(3) the e-mail's inclusion of similar requests that the defendant had made by phone during the time period; and
(4) the e-mail's reference to the author by the defendant's nickname.[23]

### E. Reply-Letter Doctrine

Several Texas cases have held that the reply-letter doctrine for authenticating letters applies to email and other messages. Under this traditional doctrine, a letter received in the due course of mail purportedly in answer to another letter is prima facie genuine and admissible without further proof of authenticity.[24] A reply letter needs no further authentication because it is unlikely that anyone other than the purported writer would know of and respond to the contents of the earlier letter addressed to him.[25] An e-mail is sufficiently authenticated when a person responds to an e-mail that was sent to the person's e-mail address.[26] This rule has been applied to other types of messages by analogy. A New York case held that the reply-letter doctrine applied to instant messages, where the person sent an instant message to a screen name and received a reply, the content in the reply supported the conclusion that the message was sent by defendant, and no evidence was admitted to show that anyone else had motive or opportunity to impersonate defendant by using his screen name.[27]

### F. Text Messages.

Text messages can be authenticated by applying the same factors as emails.[28]

**Recent Texas Case:[29]** Printouts of emails, internet chat room dialogues, and cell phone text messages can all be admitted into evidence when found to be sufficiently linked to the purported author so as to justify submission to the jury for its ultimate determination of authenticity.

**Recent Texas Case:[30]** Authentication of text messages does not erect a particularly high hurdle, and that hurdle may be cleared by circumstantial evidence.

**Recent Texas Case:[31]** A creative argument to the authentication of text messages was made when the defendant argued that text messages in a "group text" that identified the defendant only as "me" was not sufficient to identify defendant as the owner/sender of the messages.

The defendant (Jones) argued the authenticity of information (text messages) from his mobile telephone; however, the State offered evidence from the phone as information and content that was within defendant's control by showing circumstantial evidence connecting Jones to the phone at the time of the arrest. This included Jones's possession and use of the phone, identification of phone numbers suggesting Jones used the phone, photographs showing a shipping label addressed to him at a restaurant where he worked, and text messages regarding bank transactions consistent with bank receipts found in his car.

**Recent Texas Case:[32]** The defendant argued that the State failed to authenticate a text message because the witness did not see the text message arrive from the defendant's phone, nor could the witness testify the texts were sent by the defendant's recognizable telephone number. The court held that the witness did testify he knew when his mother received text messages from the defendant. Because he was better with technology, he saved the texts on the phone. The witness then pulled out his mother's phone and pulled up the text message for the attorneys to review. The court held that "Given the low threshold for authentication under Rule 901(b)(1), we conclude [the witness's] testimony was sufficient that a reasonable fact finder could properly determine that the text message was what it claimed to be—a text message from [the defendant]."

**Recent Texas Case:** A witness was permitted to testify about the contents of text messages the victim received from the accused and the emotional effect the texts had on the victim.[33]

---

[23] *Massimo v. State*, 144 S.W.3d 210, 215 (Tex.App.—Fort Worth 2004, no pet.).
[24] *Varkonyi v. State*, 276 S.W.3d 27, 35 (Tex.App.—El Paso 2008, pet. ref'd).
[25] *Id*.
[26] *Manuel v. State*, No. 12-09-00454-CR. (Tex.App.—Tyler 2011).
[27] *People v. Pierre*, 838 N.Y.S.2d 546, 548-49 (N.Y. App. Div. 2007)
[28] *Manuel v. State*, No. 12-09-00454-CR. (Tex.App.—Tyler 2011).
[29] *Longoria v. State*, No. 08-13-00083-CR (Tex. App.—El Paso Dec. 15, 2015)
[30] *Cook v. State*, 460 S.W.3d 703 (Tex. App.—Eastland, 2015 no pet.)
[31] *Jones v. State*, 466 S.W.3d 252 (Tex. App.—Houston [1st Dist.] 2015, no pet.)
[32] *Montoya v. State*, No. 05-10-01468-CR (Tex.App.—Dallas Mar. 30, 2012) (memo. op.).
[33] *Gardner v. State*, 306 S.W.3d 274 (Tex. Crim. App. 2009).

**Recent Texas Case:** [34] In a recent case, a defendant raised an authenticity objection, that just because text messages were found on a phone in his possession did not mean he sent or received them. The court overruled the authenticity objection (but upheld a hearsay objection), stating in part:

> This court is sympathetic with Appellant's position in trying to find law directly on point, given the speed with which technology has changed. To guide parties in raising and preserving such issues, courts are going to have to determine at some point whether a cell phone is akin to a computer, a file cabinet, a personal notebook or diary, or something else, and the rules of evidence should be modernized. But Appellant does not challenge the technology. Nor does he challenge the rule 901 predicate required for the authentication or identification of most electronic devices.

**G. Internet Website Postings.**

When determining the admissibility of exhibits containing representations of the contents of website postings of a party, the issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting.[35] *See*:

- *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir.2000) (excluding evidence of website postings because proponent failed to show that sponsoring organization actually posted the statements, as opposed to a third party);
- *St. Luke's*, 2006 WL 1320242 (plaintiff failed to authenticate exhibits of defendant's website postings because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website);
- *Wady*, 216 F.Supp.2d 1060.

Cases that have dealt specifically with the admission of Facebook postings include:

- *State v. Eleck*, No. AC 31581, 2011 Conn. App. LEXIS 427, at *17-18 (Conn. App. Ct. Aug. 9, 2011) (showing that messages came from particular Facebook account insufficient to authenticate messages without further "foundational proof");
- *Commonwealth v. Purdy*, 459 Mass. 442, 450-51, 945 N.E.2d 372 (2011) (holding that e-mail sent from Facebook account bearing defendant's name not sufficiently authenticated without additional "confirming circumstances").

One commentator has observed ''[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly.

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

The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

- 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?''

Counsel attempting to authenticate exhibits containing information from internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation.

The authentication rules most likely to apply, singly or in combination, are:

- 901(b)(1) (witness with personal knowledge)
- 901(b)(3) (expert testimony)
- 901(b)(4) (distinctive characteristics),
- 901(b)(7) (public records),
- 901(b)(9) (system or process capable of producing a reliable result), and
- 902(5) (official publications).

[34] *Black v. State*, No. 02-10-00283-CR (Tex.App.—Fort Worth 2012).
[35] *Lorraine*, 241 F.R.D. at 555-56.

**Recent Texas Case:**[36] A court addressed the concerns of third-party posts on social media/websites and the lack of foundation which is at issue in the *Dering* case.

In *Dering*, the evidence was insufficient to support a finding of authenticity because circumstantial evidence is necessary to properly authenticate social media posts. The Facebook posts in this case were not made by Appellant or sent by Appellant to anyone. Appellant had nothing to do with the creation or the content of the posts other than serve as the subject of the posts. The original post was created by a third party who did not testify. There was no evidence of the authenticity of who the purported author was of any of the Facebook posts.

**Recent Texas Case:** A court excluded, as unauthenticated, a writing and recording from a company's website. Counsel attested that the writing and recording were true and correct copies obtained from the company website. The court held that the statements did not establish that the website was actually that of the company. Further, the affiant did not state that he recognized the voice on the recording and that the voice excerpts captured from the website were actually those of the speaker.

### H. Tinder and Other Online Personals

Online dating websites (Match, eHarmony, OkCupid, PlentyOfFish) and dating apps (Tinder, Grindr) are increasingly being used as evidence. The following cases address the authentication of online personals and messaging applications.

**Recent Texas Case:**[37] The Texas Court of Criminal Appeals has suggested that when determining the admissibility of text messages, instant messages, chats and the similar forms of electronic communication courts must be especially cognizant that such matters may sometimes be authenticated by distinctive characteristics found within the writings themselves and by comparative reference from those characteristics to other circumstances shown to exist by the evidence presented at trial. Conversations and events that precede or follow the communications at issue, when identified or referred to within the written communication, can provide contextual evidence demonstrating the authenticity of such communications.

**Recent Texas Case:** One case addressed an online personal ad, and found that it was not necessary for authentication to show that the person placed the ad, only that the exhibit was an authentic copy of the actual online ad.[38] Whether the party placed the ad did not go to the authenticity of the exhibit, but rather to the underlying issues in the case.

**Recent Texas Case:** Mother objected to the admission of provocative photographs of her, allegedly posted to an adult website. On appeal, the court held that the objection had not been preserved because, although she objected at trial that the photos were not of her, she failed to object to their authentication as pictures that were posted on an adult website.[39]

### I. Facebook.

Since the *Tienda* decision, several Texas courts have evaluated Facebook evidence. The recent *Campbell*[40] decision stated:

The content of the messages themselves purport to be messages sent from a Facebook account bearing the defendant's name to an account bearing the victim's name. While this fact alone is insufficient to authenticate the defendant as the author, when combined with other circumstantial evidence, the record may support a finding by a rational jury that the messages were authored and sent by the defendant.

Turning to the Facebook messages themselves, the messages contain internal characteristics that tend to connect the defendant as the author. First, the unique speech pattern presented in the messages is consistent with the speech pattern that the defendant, a native of Jamaica, used in testifying at trial. Second, the messages reference the incident and potential charges, which at the time the messages were sent, few people would have known about. Thus, the contents of the messages provide circumstantial evidence supporting the trial court's ruling.

Further, the undisputed testimony provides circumstantial evidence tending to connect the defendant to the messages. The undisputed testimony yields the following: (1) the defendant had a Facebook account; (2) only he and the victim ever had access to his Facebook account; and (3) the victim received the messages bearing the defendant's name. This evidence suggests that only the defendant or the victim could have authored the messages received in the victim's Facebook account. In addition, the victim told the jury that she could not access the defendant's account, and therefore, she did not send the messages to herself. While this evidence certainly does not conclusively establish that the defendant authored the messages-in fact, the defendant insisted that he did not — the State

[36] *Dering v. State*, 465 S.W.3d 668 (Tex. App.—Eastland 2015, no pet.)

[37] *Butler v. State*, 459 S.W.3d 595 (Tex. Crim. App. 2015)

[38] *Musgrove v. State*, No. 03-09-00163-CR (Tex.App.—Austin 2009) (memo. op.).

[39] *In Re J.A.S.*, No. 11-09-00176-CV (Tex.App.—Eastland January 13, 2011) (memo. op.).

[40] *Campbell v. State*, 382 S.W.3d 545, 551-53 (Tex. App.-Austin 2012, no pet.)

was not required to rule out all possibilities inconsistent with authenticity or prove beyond any doubt that the evidence is what it purports to be. So long as the authenticity of the proffered evidence was at least within the zone of reasonable disagreement, the jury was entitled to weigh the credibility of these witnesses and decide who was telling the truth.

**Recent Texas Case:**[41] In an unpublished opinion, the Beaumont Court of Appeals addressed the authenticity of facebook messages/chats.

In *Bullman*, defendant (Bullman) contends the trial court abused its discretion in admitting into evidence Facebook records from Bullman's Facebook account, which included various dialogues between Bullman and E.D., the child he allegedly molested. Bullman argues the records were not properly authenticated and contained inadmissible hearsay. To satisfy the authentication requirement, the evidence must produce evidence to support a finding that the item is what the proponent claims it is. Two concerns: (1) the account could be fictitious, and (2) another person may gain access to someone's account by obtaining their username and password. The victim, E.D., identified the Facebook message printouts as messages she received from the defendant, and she denied she sent the messages to herself through the defendant's account. The victim also denied having the defendant's password on the day the message was sent. The court concluded the State only had to present prima facie evidence such that a reasonable jury could have found the Facebook messages were created by the defendant.

### J. Chat Room Content.

Many of the same foundational issues encountered when authenticating website evidence apply with equal force to internet chat room content; however, the fact that chat room messages are posted by third parties, often using ''screen names'' means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host.[42]

One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

(1) evidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
(2) evidence that, when a meeting with the person using the screen name was arranged, the individual showed up;
(3) evidence that the person using the screen name identified himself as the person in the chat room conversation;
(4) evidence that the individual had in his possession information given to the person using the screen name; or
(5) evidence from the hard drive of the individual's computer showing use of the same screen name.

Courts also have recognized that exhibits of chat room conversations may be authenticated circumstantially.

For example, in *In re F.P.*,[43] the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts.

Similarly, in *United States v. Simpson*,[44] the court held that there was ample circumstantial evidence to authenticate printouts of the content of chat room discussions between the defendant and an undercover detective, including use of the e-mail name of the defendant, the presence of the defendant's correct address in the messages, and notes seized at the defendant's home containing the address, e-mail address and telephone number given by the undercover officer.

Likewise, in *United States v. Tank*,[45] the court found sufficient circumstantial facts to authenticate chat room conversations, despite the fact that certain portions of the text of the messages in which the defendant had participated had been deleted. There, the court found the testimony regarding the limited nature of the deletions by the member of the chat room club who had made the deletions, circumstantial evidence connecting the defendant to the chat room, including the use of the defendant's screen name in the messages, were sufficient to authenticate the messages.

Based on the foregoing cases, the rules most likely to be used to authenticate chat room and text messages, alone or in combination, appear to be:

- 901(b)(1) (witness with personal knowledge) and
- 901(b)(4) (circumstantial evidence of distinctive characteristics).

---

[41] *Bullman v. State*, No. 09-14-00196-CR (Tex. App.—Beaumont, April 13, 2016)
[42] *Lorraine*, 241 F.R.D. at 556.
[43] 878 A.2d at 93–94.
[44] 152 F.3d at 1249.
[45] 200 F.3d at 629–31.

**Recent Texas Case:**[46] A detective was an actual party to a chat room conversation and identified the State's chat log. Appellant admitted to the detectives he chatted online with a 15-year old girl, and that chat log was a true representation of that conversation. The chat log is what it is proclaimed to be: a chat log between a detective and Appellant. Prima facia authentication was found when the purported sender actually admitted to authorship or was seen composing it. Printouts of emails, internet chat room dialogues, and cell phone text messages can all be admitted into evidence when found to be sufficiently linked to the purported author so as to justify submission to the jury for its ultimate determination of authenticity.

**Recent Texas Case:** Although chat rooms per se are not as common as they used to be, chat apps are surging in popularity. Chat apps include Kik, WhatsApp, and more. The 2015 *Smallwood*[47] case discusses the use of Kik chat evidence, but unfortunately does not go into detail on how the evidence was authenticated or admitted.

### K. Stored versus Processed Data

In general, electronic documents or records that are merely *stored* in a computer raise no computer-specific authentication issues.[48] 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 stages 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.

### L. Computer Stored Records and Data.

Given the widespread use of computers, there is an almost limitless variety of records that are stored in or generated by computers.[49] As one commentator has observed ''[m]any kinds of computer records and computer- generated information are introduced as real evidence or used as litigation aids at trials. They range from computer printouts of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements.''

The least complex admissibility issues are associated with electronically stored records. In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. Two cases illustrate the contrast between the more lenient approach to admissibility of computer records and the more demanding one:

In *United States v. Meienberg,*[50] the defendant challenged on appeal the admission into evidence of printouts of computerized records of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records. The Tenth Circuit disagreed, stating: ''Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility.'' *See also*:

- *Kassimu,* 2006 WL 1880335 (To authenticate computer records as business records did not require the maker, or even a custodian of the record, only a witness qualified to explain the record keeping system of the organization to confirm that the requirements of Rule 803(6) had been met, and the inability of a witness to attest to the accuracy of the information entered into the computer did not preclude admissibility);
- *Sea–Land Serv., Inc. v. Lozen Int'l,* 285 F.3d 808 (9th Cir.2002) (ruling that trial court properly considered electronically generated bill of lading as an exhibit to a summary judgment motion. The only foundation that was required was that the record was produced from the same electronic information that was generated contemporaneously when the parties entered into their contact. The court did not require evidence that the records were reliable or accurate).

In contrast, in the case of *In re Vee Vinhnee,*[51] the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. The court noted that ''it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground.'' The court further observed that: ''The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between

[46] *Longoria v. State*, No. 08-13-00083-CR (Tex. App.—El Paso Dec. 15, 2015).

[47] *Smallwood v. State*, No. 02-13-00532-CR (Tex.App.—Fort Worth 2015).

[48] *Lorraine*, 241 F.R.D. at 543 (emph. added).

[49] *Lorraine*, 241 F.R.D. at 556-59.

[50] 263 F.3d at 1180–81.

[51] 336 B.R. 437.

when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created. Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.'' The court reasoned that, for paperless electronic records: ''The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.'' In order to meet the heightened demands for authenticating electronic business records, the court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried, viewing electronic records as a form of scientific evidence:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Although the position taken by the court in *In re Vee Vinhnee* appears to be the most demanding requirement for authenticating computer stored records, other courts also have recognized a need to demonstrate the accuracy of these records. *See, e.g.*:

- *State v. Dunn*, 7 S.W.3d 427, 432 (Mo.Ct.App.2000) (Admissibility of computer-generated records ''should be determined on the basis of the reliability and accuracy of the process involved.'');
- *State v. Hall*, 976 S.W.2d 121, 147 (Tenn. 1998) (''[T]he admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.'').

As the foregoing cases illustrate, there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed. Further, it would not be surprising to find that, to date, more courts have tended towards the lenient rather than the demanding approach. The Manual for Complex Litigation states that courts ''should consider the accuracy and reliability of computerized evidence'' in ruling on its admissibility. Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required.

The methods of authentication most likely to be appropriate for computerized records are:

- 901(b)(1) (witness with personal knowledge),
- 901(b)(3) (expert testimony),
- 901(b)(4) (distinctive characteristics), and
- 901(b)(9) (system or process capable of producing a reliable result).

**M. Digital Photographs and Videos.**

Photographs have been authenticated for decades under Rule 901(b)(1) by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately represents the scene.[52] Calling the photographer or offering expert testimony about how a camera works almost never has been required for traditional film photographs. Today, however, the vast majority of photographs taken, and offered as exhibits at trial, are digital photographs, which are not made from film, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered. Indeed, unlike photographs made from film, digital photographs may be "enhanced." Digital image enhancement consists of

[52] *Lorraine*, 241 F.R.D. at 561-62.

removing, inserting, or highlighting an aspect of the photograph that the technician wants to change.

Some examples graphically illustrate the authentication issues associated with digital enhancement of photographs: Suppose that in a civil case, a shadow on a 35 mm photograph obscures the name of the manufacturer of an offending product. The plaintiff might offer an enhanced image, magically stripping the shadow to reveal the defendant's name. Or suppose that a critical issue is the visibility of a highway hazard. A civil defendant might offer an enhanced image of the stretch of highway to persuade the jury that the plaintiff should have perceived the danger ahead before reaching it. In many criminal trials, the prosecutor offers an 'improved', digitally enhanced image of fingerprints discovered at the crime scene. The digital image reveals incriminating points of similarity that the jury otherwise would never would have seen.

There are three distinct types of digital photographs that should be considered with respect to authentication analysis: original digital images, digitally converted images, and digitally enhanced images.

1. Original Digital Photograph.

An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it. If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under Rule 201.

Further, even if no witness can testify from personal knowledge that the photo or video accurately depicts the scene, the "silent witness" analysis allows a photo or video to be authenticated by showing a process or system that produces an accurate result.[53] Testimony that showed how the tape was put in the camera, how the camera was activated, the removal of the tape immediately after the offense, the chain of custody, and how the film was developed was sufficient to support the trial court's decision to admit the evidence.[54] Photos taken by an ATM were properly authenticated on even less evidence--mere testimony of a bank employee familiar with the operation of the camera and the fact that the time and date were indicated on the evidence were sufficient to authenticate the photos.[55]

**Recent Texas Case:**[56] A court discussed at great length admissibility of a video when the sponsoring witness was not present and did not witness the events in the video.

Defendant, Standmire, contended the trial court erred in admitting a video recording from the jail surveillance camera, because the sponsoring witness for the exhibit did not have sufficient knowledge to authenticate the exhibit. More specifically, the guard sponsoring the video did not see the assault take place and because he could not show the recording process accurately produced the resulting video, no one with personal knowledge could testify that the images on the exhibit were an accurate portrayal of what occurred. There are at least two ways to authenticate photographic evidence including videos: (1) the photo or video is an accurate representation of the object or scene in question, where the sponsoring witness is not required to be the person operating the camera or video equipment, and (2) testimony that the process or system that produced the photo or video is reliable, where there is most often no witness that was present at the scene or event depicted in the photograph or video. To authenticate such photographic or video evidence, the sponsoring witness usually (1) describes the type of system used for recording and whether it was working properly, (2) testifies whether he reviewed the video/photos, (3) testifies whether he removed the video or device that stores the photos, and (4) testifies whether the video or photos have been altered or tampered with. If the sponsoring witness was present when the photos/video was taken, it is unnecessary for them to testify regarding the reliability of the system.

**Recent Texas Case:** A court found the following testimony sufficient to authenticate a video: a witness, who was not present at the time of the incident, described the store's multiplex recording system and its computer systems; he detailed how he was able to link the encoding on the receipts to the time and date that the account was opened, to the transactions in question, to the cashier, to the terminal, and finally to the video camera that recorded the transactions; and he testified that he had personally copied the relevant recordings from the multiplex to the videotape. He further testified that he had viewed the video on the multiplex system, viewed it on the tape on the day that he made the tape, and then viewed it again on the day prior to his testimony and that it fairly and accurately represented what it purported to show. The witness testified that no alterations or deletions were made to the videotape.[57]

[53] *See* Tex.R. Evid. 901(b)(9).

[54] *Reavis v. State*, 84 S.W.3d 716, 719-20 (Tex.App.-Fort Worth 2002, no pet.).

[55] *Reavis v. State*, 84 S.W.3d 716, 719-20 (Tex.App.-Fort Worth 2002, no pet.).

[56] *Standmire v. State*, 475 S.W.3d 336 (Tex. App.—Waco 2014, pet. denied).

[57] *Thierry v. State*, 288 S.W.3d 80 (Tex.App.--Houston [1st Dist.] 2009, pet. ref'd).

**Recent Texas Case:** Interestingly, a witness may authenticate a photograph without knowing where it was taken, when it was taken, or by whom it was taken, as long as the witness can testify that the photograph accurately represents what it purports to represent.[58] This holds true for any photograph, not just digital photographs.

2. Digitally Converted Images.

For digitally converted images, authentication requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images, Rules 901(b)(1) and 901(b)(9)-the latter rule implicating expert testimony under Rule 702. Alternatively, if there is a witness familiar with the scene depicted who can testify to the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion.

**Recent Texas Case:[59]** The State sought to introduce still images captured from a surveillance video, and Defendant, Anderson, objected that the photographs had not been properly authenticated. Evidence can be authenticated through comparison by the trier of fact or by an expert witness with specimens that have been found by the court to be genuine. Here, the parties stipulated to the genuineness of the surveillance video when the stipulated to its admissibility. The jury was presented with the video, which was admitted by stipulation, and the jury determined the photographs were the same images contained in the video; therefore, the record supports finding the still photographs were sufficiently authenticated.

3. Digitally Enhanced Images.

For digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified. In such a case, there will need to be proof, permissible under Rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under Rule 702. Recently, one state court has given particular scrutiny to how this should be done.

In *State v. Swinton*,[60] the defendant was convicted of murder in part based on evidence of computer enhanced images prepared using the Adobe Photoshop software. The images showed a superimposition of the defendant's teeth over digital photographs of bite marks taken from the victim's body. At trial, the state called the forensic odontologist (bite mark expert) to testify that the defendant was the source of the bite marks on the victim. However, the defendant testified that he was not familiar with how the Adobe Photoshop made the overlay photographs, which involved a multi-step process in which a wax mold of the defendant's teeth was digitally photographed and scanned into the computer to then be superimposed on the photo of the victim. The trial court admitted the exhibits over objection, but the state appellate court reversed, finding that the defendant had not been afforded a chance to challenge the scientific or technical process by which the exhibits had been prepared. The court stated that to authenticate the exhibits would require a sponsoring witness who could testify, adequately and truthfully, as to exactly what the jury was looking at, and the defendant had a right to cross-examine the witness concerning the evidence. Because the witness called by the state to authenticate the exhibits lacked the computer expertise to do so, the defendant was deprived of the right to cross examine him.

Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a means to authenticate digitally enhanced photographs under Rule 901(b)(9):

(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.

[58] *Brown v. State*, No. 12-11-00027-CR (Tex.App.—Tyler Sept. 7, 2011) (memo op.).
[59] *Anderson v. State*, 461 S.W.3d 674 (Tex. App.—Texarkana 2015, no pet.).
[60] 268 Conn. 781, 847 A.2d 921, 950–52 (2004).

The author recognized that this is an extensive foundation, and whether it will be adopted by courts in the future remains to be seen. However, it is probable that courts will require authentication of digitally-enhanced photographs by adequate testimony that a photograph is the product of a system or process that produces accurate and reliable results under Rule 901(b)(9).

### N. Voicemail or Other Audio Recordings.

Rule 901(b)(5) provides that a voice recording may be identified by opinion based upon hearing the voice at anytime under circumstances connecting it with the alleged speaker. One Texas court has found that a voicemail was not properly authenticated when a witness testified that she recognized the voice as a party's but did not identify the recording or explain the circumstances in which it was made.[61] However, a recording can be properly authenticated even when the witness cannot identify every voice in the recording.[62]

**Recent Texas Case:** One recent case lists three methods that can be used to authenticate a voicemail: (1) through the testimony of a witness with knowledge that a matter is what it is claimed to be; (2) by opinion based upon hearing the voice at anytime under circumstances connecting it with the alleged speaker; or (3) the identity of a caller can be demonstrated by self-identification coupled with additional circumstances, such as the context and timing of the call, the contents of the statement, and disclosure of knowledge of facts known peculiarly to the speaker.[63]

**Practice Tip:** A video is typically authenticated by a witness who can testify either that the scene is accurately depicted, or that the recording was made by a reliable method. However, if your witness merely recognizes the people in the video but cannot testify about the scene or how the video was made, you may try admitting solely the audio portion. Your witness can testify that she recognizes some or all of the voices, and the other requirements for authenticating a video would not apply.

### O. Conclusion on Authenticating ESI.

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced.[64] Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in Rules 901 and 902, as well as consider requesting a stipulation from opposing counsel, or filing a request for admission of the genuineness of the evidence. With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

An attorney could also ask authenticating questions about ESI during a deposition. An attorney could have the deponent log into various sites during the deposition and testify to the contents. In theory, this would be no different than having a deponent produce a diary and go through it.

## V. BEST EVIDENCE RULE.

The Best Evidence Rule states that, to prove the content of a writing, recording, or photograph, the *original* writing, recording, or photograph is required except as otherwise provided.[65] The purpose of the best evidence rule is to produce the best obtainable evidence, and if a document cannot as a practical matter be produced because of its loss or destruction, then the production of the original is excused.[66]

Under Tex. R. Evid. 1001(c), if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original. An Indiana court, for example, found that internet chat room communications that a party cut and pasted into a word processing document were still originals.[67] In the predicate for introducing a computer printout, asking whether the exhibit reflects the data accurately may help to overcome an objection under the Best Evidence Rule.

**Recent Texas Case:** In a case where the trial court was not equipped to play minicassettes, the State transferred a recording to a CD, and offered the duplicate into evidence instead.[68] The defendant objected, citing the Best Evidence Rule. The Court

---

[61] *Miller v. State*, 208 S.W.3d 554, 566 (Tex.App.—Austin 2006, pet. ref'd).

[62] *See e.g.*, *Jones v. State*, 80 S.W.3d 686 (Tex. App.-Houston [1st Dist.] 2002); *Rios v. State*, No. 10-08-00408-CR (Tex.App.—Waco Nov. 10, 2009) (memo. op.).

[63] *Goodrich v. State*, No. 09-10-00167-CR (Tex.App.—Beaumont Apr. 13, 2011) (memo. op.).

[64] *Lorraine*, 241 F.R.D. at 562.

[65] Tex. R. Evid. 1002 (emph. added).

[66] *Jurek v. Couch-Jurek*, 296 S.W.3d 864, 871 (Tex.App.--El Paso 2009, no pet.).

[67] *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002).

[68] *Milton v. State*, No. 14-10-00696-CR (Tex.App.—Houston [14th Dist.] Sept. 20, 2011) (memo op.).

stated that a duplicate is admissible to the same extent as an original unless a question is raised as to the authenticity of the original. Stated another way, a duplicate is inadmissible if reasonable jurors might differ as to whether the original is what it is claimed to be. In this case, the defendant primarily challenged the authenticity of the duplicate CD, rather than the original. He also objected that the chain of custody was never documented between the officer's possession of the minicassette to its transfer onto a CD. The officer testified the copy was an exact duplicate, and the defendant never questioned the authenticity of the original, so the best evidence rule objection was overruled.

## VI. RULE OF OPTIONAL COMPLETENESS.

Frequently when one party attempts to introduce one part of a lengthy set of electronic data or recordings, the other party objects to the introduction on the grounds of "optional completeness." Optional completeness is not a method for excluding evidence, but rather a way to give the other side the opportunity to introduce additional evidence at the appropriate time. Judge Bonnie Sudderth explains:[69]

Texas Rules of Evidence 107, the Rule of Optional Completeness, provides:

> "When part of an act, declaration, conversation, writing or recorded statement is given in evidence by one party, the whole on the same subject may be inquired into by the other, and any other act, declaration, writing or recorded statement which is necessary to make it fully understood or to explain the same may also be given in evidence…"

Contrary to popular belief and practice, nothing in Rule 107, the rule of optional completeness, provides for a right to have the additional statement placed into evidence immediately. It simply provides that such evidence is admissible. And, while most judges would liberally permit a contemporaneous offer of the additional statement, it would not be error for a judge to require that such evidence be placed into evidence when the objecting party cross-examines or re-directs the witness, as with any other piece of additional evidence.

Rule 106, Remainder of or Related Writings or Recorded Statements provides:

> "When a writing or recorded statement or part thereof is introduced by a party, an adverse party may at that time introduce any other part or any other writing or recorded statement which ought in fairness to be considered contemporaneously with it… "

So, even though the rule of optional completeness does not contemplate a contemporaneous offer, the evidence may be admissible contemporaneously under Rule 106. Even under Rule 106, there is no guaranteed right to have every sentence read to completion, or any deposition answer fully read contemporaneously with an initial offer.

Rule 106 provides for contemporaneous admission of evidence only when, in fairness, it ought to be considered contemporaneously with the portion previously admitted. In other words, contemporaneous admission operates only to prevent unfairness. Whether fairness necessitates a contemporaneous offer under the circumstances is a factual determination to be made by the trial court and reviewed under an abuse of discretion standard.

Furthermore, case law suggests that even when fairness predominates in favor of a contemporaneous offer, Rule 106 does not actually mandate it. Because Rule 106 was not written in mandatory terms, it would not be error for a court to require (as with Rule 107) that such evidence be placed into evidence at the time when opposing counsel is directing the witness. *Gilmore v. State*, 744 S.W.2d 630 (Tex. App. — Dallas 1987). ("Rule 106 is a narrow modification of the doctrine of optional completeness, controlling the time an adversary can introduce certain kinds of remainder evidence, [but] the language of the rule is a permissive grant and not a requirement." *Id*. at 631.)

## VII. HEARSAY ISSUES IN ELECTRONIC EVIDENCE.

Hearsay is a 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.[70] (See "Non-Assertive Statement," below, for a discussion of whether testimony is even a "statement" at all.) The "matter asserted" includes any matter explicitly asserted, and any matter implied by a statement, if the probative value of the statement as offered flows from declarant's belief as to the matter.[71] Hearsay is inadmissible unless otherwise permitted by the rules or by statute.[72]

Put more simply, any out-of-court statement, whether by the witness or another person, is hearsay

[69] From Judge Bonnie Sudderth, Law Blog on the Texas Rules of Evidence, "The Rule of Optional Completeness," available at: https://judgebonniesudderth.wordpress.com/2011/06/09/the-rule-of-optional-completeness/

[70] Tex. R. Evid. 801(d).

[71] Tex. R. Evid. 801(c).

[72] Tex. R. Evid. 802; *see* Tex. R. Evid. 801(e), 803, 804.

and is inadmissible to support the truth of a claim, unless permitted by another rule. However, otherwise inadmissible hearsay admitted without objection should not be denied probative value merely because it is hearsay.[73] If it can be shown that a statement is non-hearsay or that it falls within a hearsay exception, the statement can be admissible as probative evidence.[74]

The twenty-four hearsay exceptions listed in Texas Rule 803 may be roughly categorized into three categories: unreflective statements, reliable documents, and reputation evidence. The rationale for all of the exceptions is that, over time, experience has shown that these types of statements are generally reliable and trustworthy.[75] However, all hearsay exceptions require a showing of trustworthiness.[76]

**A. Unreflective Statements.**

Evidence obtained from email, text messaging, or social networking sites, such as Facebook, MySpace, or Twitter, is often relevant in criminal cases. The evidence may be non-hearsay to the extent that it is an admission by a party-opponent, but there may be times where statements by others are relevant. Of the hearsay exceptions, 803(1)-(3) can be especially useful in admitting these types of evidence. Those are the exceptions for present sense impression, excited utterance, and then-existing condition. Electronic communication is particularly prone to candid statements of the declarant's state of mind, feelings, emotions, and motives.[77] Further, such messages are often sent while events are unfolding. The logic of the existing exceptions can be applied to admit even new forms of communication.

1. Present Sense Impression.

A statement describing or explaining an event made *while* the declarant was perceiving the event or *immediately* thereafter.[78] Unlike the excited-utterance exception, the rationale for this exception stems from the statement's contemporaneity, not its spontaneity.[79] The present sense impression exception to the hearsay rule is based upon the premise that the contemporaneity of the event and the declaration ensures reliability of the statement. The rationale underlying the present sense impression is that: (1) the statement is safe from any error of the defect of memory of the declarant because of its contemporaneous nature, (2) there is little or no time for a calculated misstatement, and (3) the statement will usually be made to another (the witness who reports it) who would have an equal opportunity to observe and therefore check a misstatement.[80] The *Fischer*[81] case states the following: The rule is predicated on the notion that the utterance is a reflex product of immediate sensual impressions, unaided by retrospective mental processes. It is instinctive, rather than deliberate. If the declarant has had time to reflect upon the event and the conditions he observed, this lack of contemporaneity diminishes the reliability of the statements and renders them inadmissible under the rule. Once reflective narratives, calculated statements, deliberate opinions, conclusions, or conscious thinking-it-through statements enter the picture, the present sense impression exception no longer allows their admission. Thinking about it destroys the unreflective nature required of a present sense impression.

2. Excited Utterance.

A statement relating to a startling event or condition made while the declarant was under stress or excitement caused by event or condition.[82] The excited-utterance exception is broader than the present-sense-impression exception.[83] While a present-sense-impression statement must be made while the declarant was perceiving the event or condition, or immediately thereafter, under the excited-utterance exception, the startling event may trigger a spontaneous statement that relates to a much earlier incident.[84] The *Goodman*[85] case states the following: For the excited-utterance exception to apply, three conditions must be met: (1) the statement must be a product of a startling occurrence that produces a state of nervous excitement in the declarant and renders the utterance spontaneous and unreflecting, (2) the state of excitement must still so dominate the declarant's mind that there is no time or opportunity to contrive or misrepresent, and (3) the statement must relate to the circumstances of the occurrence preceding it. The critical factor in determining when a statement is an excited utterance under Rule 803(2) is whether the declarant was still

[73] Tex. R. Evid. 802.
[74] *See, Miranda v. State*, 813 S.W.2d 724, 735 (Tex.App.—San Antonio 1991, pet ref'd).
[75] *Fischer v. State*, 252 S.W.3d 375, 379 (Tex.Crim.App. 2008).
[76] *Robinson v. Harkins & Co.*, 711 S.W.2d 619, 621 (Tex.1986).
[77] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 570 (D.Md. 2007) (memo. op.).
[78] Tex. R. Evid. 803(1) (emph. added).
[79] *Rabbani v. State*, 847 S.W.2d 555, 560 (Tex.Crim.App. 1992).
[80] *Id*.
[81] *Fischer v. State*, 252 S.W.3d 375, 381 (Tex.Crim.App. 2008).
[82] Tex. R. Evid. 803(2).
[83] *McCarty v. State*, 257 S.W.3d 238, 240 (Tex.Crim.App. 2008).
[84] *Id*.
[85] *Goodman v. State*, 302 S.W.3d 462, 472 (Tex.App.—Texarkana 2009, pet. ref'd).

dominated by the emotions, excitement, fear, or pain of the event. The time elapsed between the occurrence of the event and the utterance is only one factor considered in determining the admissibility of the hearsay statement.

3. Then Existing Mental, Emotional, or Physical Condition.

A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, or bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will.[86] Texas courts have held that the type of statement contemplated by this rule includes a statement that on its face expresses or exemplifies the declarant's state of mind—such as fear, hate, love, and pain.[87] For example, a person's statement regarding her emotional response to a particular person qualifies as a statement of then-existing state of emotion under Rule 803(3).[88] However, a statement is inadmissible if it is a statement of memory or belief offered to prove the fact remembered or believed.[89] One federal court offers the following explanation of Rule 803(3)'s "exception to the exception": Case law makes it clear that a witness may testify to a declarant saying "I am scared," but not "I am scared because the defendant threatened me." The first statement indicates an actual state of mind or condition, while the second statement expresses belief about why the declarant is frightened. The phrase "because the defendant threatened me" is expressly outside the state-of-mind exception because the explanation for the fear expresses a belief different from the state of mind of being afraid.[90]

**B. Reliable Documents.**

The second category of hearsay exceptions, reliable documents, can also include a variety of computer- or internet-stored data. Anything from online flight schedules, to personal financial records, to emails could potentially be admitted under these existing hearsay exceptions.

1. Recorded Recollection.

A memorandum or record concerning a matter about which a witness once had personal knowledge but now has insufficient recollection to enable the witness to testify fully and accurately, shown to have been made or adopted by the witness when the matter was fresh in the witness' memory and to reflect that knowledge correctly, unless the circumstances of preparation cast doubt on the document's trustworthiness. If admitted, the memorandum or record may be read into evidence but may not itself be received as an exhibit unless offered by an adverse party.[91] For a statement to be admissible under Rule 803(5): (1) the witness must have had firsthand knowledge of the event, (2) the statement must be an original memorandum made at or near the time of the event while the witness had a clear and accurate memory of it, (3) the witness must lack a present recollection of the event, and (4) the witness must vouch for the accuracy of the written memorandum.[92] To meet the fourth element, the witness may testify that she presently remembers recording the fact correctly or remembers recognizing the writing as accurate when she read it at an earlier time. But if her present memory is less effective, it is sufficient if the witness testifies that she knows the memorandum is correct because of a habit or practice to record matters accurately or to check them for accuracy. At the extreme, it is even sufficient if the individual testifies to recognizing her signature on the statement and believes the statement is correct because she would not have signed it if she had not believed it true at the time.[93]

2. Records of Regularly Conducted Activity.

A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by affidavit that complies with Rule 902(10), unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. "Business" as used in this paragraph includes any and every kind of regular organized activity whether conducted for profit or not.[94] For example, if a spouse keeps financial records as part of a regularly organized activity, the records can be admitted under this exception with the spouse as the sponsoring witness, without a business records

[86] Tex. R. Evid. 803(3).
[87] *Garcia v. State*, 246 S.W.3d 121, 132 (Tex.App.—San Antonio 2007, pet. ref'd).
[88] *Id*.
[89] Tex. R. Evid. 803(3).
[90] *Delapaz v. State*, 228 S.W.3d 183, 207 (Tex.App.—Dallas 2007, pet. ref'd) (citing *United States v. Ledford*, 443 F.3d 702, 709 (10th Cir. 2005)).
[91] Tex. R. Evid. 803(5).
[92] *Johnson v. State*, 967 S.W.2d 410, 416 (Tex.Crim.App. 1998).
[93] *Id*.
[94] Tex. R. Evid. 803(6).

affidavit. Courts have admitted check registers, medical bills and receipts, and cancelled checks in this way.[95] The predicate for admissibility under the business records exception is established if the party offering the evidence establishes that the records were generated pursuant to a course of regularly conducted business activity and that the records were created by or from information transmitted by a person with knowledge, at or near the time of the event.[96] Business records that have been created by one entity, but which have become another entity's primary record of the underlying transaction may be admissible pursuant to Rule 803(6).[97] Although Rule 803(6) does not require the predicate witness to be the record's creator or have personal knowledge of the content of the record, the witness must have personal knowledge of the manner in which the records were prepared.[98] In order for a compilation of records to be admitted, there must be a showing that the authenticating witness or another person compiling the records had personal knowledge of the accuracy of the statements in the documents.[99]

3. Market Reports, Commercial Publications.

Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations.[100] Where it is proven that publications of market prices or statistical compilations are generally recognized as reliable and regularly used in a trade or specialized activity by persons so engaged, such publications are admissible for the truth of the matter published.[101] A variety of potentially-relevant commercial data published online can be admissible under this exception.

### C. Statements That Are Not Hearsay.

Evidence constitutes hearsay only if it is (1) an assertive statement (2) by an out-of-court declarant (3) offered to prove the truth of the assertion.[102]

1. Computer Generated "Statements."

"Cases involving electronic evidence often raise the issue of whether electronic writings constitute 'statements' under Rule 801(a). Where the writings are non-assertive, or not made by a 'person,' courts have held that they do not constitute hearsay, as they are not 'statements.'"[103]

While there may be authentication issues relating to computer-generated text or computer-processed data, several federal cases have held that such information is not hearsay:

- *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.2003) ("[N]either the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by "a person," so nothing "said" by a machine is hearsay'");
- *Safavian*, 435 F.Supp.2d at 44 (holding that portions of e-mail communications that make imperative statements instructing defendant what to do, or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay);
- *Telewizja Polska USA*, 2004 WL 2367740 (finding that images and text posted on website offered to show what the website looked like on a particular day were not "statements" and therefore fell outside the reach of the hearsay rule);
- *Perfect 10*, 213 F.Supp.2d at 1155 (finding that images and text taken from website of defendant not hearsay, "to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all—and thus fall outside the ambit of the hearsay rule.");
- *United States v. Rollins*, rev'd on other grounds 2004 WL 26780, at *9 (A.F.Ct.Crim.App. Dec.24, 2003)("Computer generated records are not hearsay: the role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system itself, relative to its proper functioning and accuracy.");
- *State v. Dunn*, 7 S.W.3d 427, 432 (Mo.Ct.App.2000) ("Because records of this type [computer generated telephone records] are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-

[95] *See Sabatino v. Curtiss Nat'l Bank*, 415 F.2d 632, 634 (5th Cir. 1969); *In re M.M.S. and I.M.S.*, 256 S.W.3d 470, 477 (Tex.App.—Dallas 2008, no pet.); *Strahan v. Strahan*, 2003 WL 22723432 *8 (Tex.App.—Houston [1st Dist.] 2003) (memo op.).

[96] *Martinez v. Midland Credit Management, Inc.*, 250 S.W.3d 481, 485 (Tex.App.—El Paso 2008, no pet).

[97] *Id*.

[98] *Id*.

[99] *In re EAK*, 192 SW3d 133, 143 (Tex.App.--Houston [14th Dist.] 2006, no pet.).

[100] Tex. R. Evid. 803(17).

[101] *Patel v. Kuciemba*, 82 S.W.3d 589, 594 (Tex.App.—Corpus Christi 2002, pet. denied).

[102] Edward J. Imwinkelreid, *Evidentiary Foundations*, 7th ed., §10.01, p. 407 (2008).

[103] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 564-65 (D.Md. 2007) (memo. op.).

examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the reliability and accuracy of the process involved.");

- *State v. Hall*, 976 S.W.2d 121, 147 (Tenn.1998) (reviewing the admissibility of computer generated records and holding "[t]he role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.").

2. Metadata

Metadata is the computer-generated data about a file, including date, time, past saves, edit information, etc. It would likely be considered a non-statement under the above logic, and therefore non-hearsay. It remains important to properly satisfy authentication requirements. A higher authentication standard may apply, since it is computer-processed data, rather than merely computer-stored data.

However, since metadata is normally hidden and usually not intended to be reviewed, several states have issued ethics opinions concluding that it is unethical to mine inadvertently-produced metadata.[104] A few ethics opinions have held that mining metadata is not unethical.[105] Texas does not yet have an ethics opinion directly on point.

See the Appendix for how metadata is handled in a "federal" case.

3. Admissions by a Party-Opponent.

The statement is offered against a party and is: (A) the party's own statement in either an individual or representative capacity; (B) a statement of which the party has manifested an adoption or belief in its truth; (C) a statement by a person authorized by the party to make a statement concerning the subject; (D) a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship; ***or*** (E) a statement by a co-conspirator of a party during the course and in furtherance of the conspiracy.[106]

The exemption for admissions by a party-opponent is extremely useful in overcoming a hearsay objection to texts, emails, Facebook wall posts, etc. The *Massimo*[107] case has a description of the authentication of a party's emails as well as a discussion of whether the emails meet the hearsay exemption for admission by party opponent or the hearsay exception for a statement against interest. A recent Texas case held that statements by a party on his MySpace page were non-hearsay as admissions by a party-opponent.[108]

## VIII. WITNESSES.

Online evidence can also be useful in managing a witness.

### A. Writing Used to Refresh Memory.

Social networking or other electronic communications can be a useful record of events or a witness's thoughts. If a witness's memory fails, a writing, including an electronic communication, may be used to refresh the witness's memory.

There is often confusion about the difference between a recorded recollection under the hearsay exception of Rule 803(5) and a writing used to refresh memory under Rule 613. The *Welch*[109] case discusses the distinction: A witness testifies from present recollection what he remembers presently about the facts in the case. When that present recollection fails, the witness may refresh his memory by reviewing a memorandum made when his memory was fresh. After reviewing the memorandum, the witness must testify either his memory is refreshed or his memory is not refreshed. If his memory is refreshed, the witness continues to testify and the memorandum is not received as evidence. However, if the witness states that his memory is not refreshed, but has identified the memorandum and guarantees the correctness, then the memorandum is admitted as past recollection recorded. Where the memorandum, statement or writing is used to refresh the present recollection of the witness and it does, then the memorandum does not become part of the evidence, for *it is not the paper that is evidence*, but the recollection of the witness.[110]

An adverse party is entitled to have the writing produced at the hearing, to inspect it, to cross-examine

---

[104] NY. Comm. On Prof'l Ethics, Op. 749 (1002); Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006); Ala. State Bar office of the Gen. Counsel, Op. No. 2007-02 (2007); D.C. Bar, Op. 341.

[105] Md. State Bar Ass'n, Comm. on Ethics, Op. 2007-092 (2006); ABA Formal Op. 06-442.

[106] Tex. R. Evid. 801(e)(2).

[107] *Massimo v. State*, 144 SW3d 210, 215-17 (Tex.App.--Fort Worth 2004, no pet.).

[108] *In re TT*, 228 SW3d 312, 316-17 (Tex.App.--Houston [14th Dist.] 2007, pet. denied).

[109] *Welch v. State*, 576 S.W.2d 638, 641 (Tex.Crim.App. 1979).

[110] *Wood v. State*, 511 S.W.2d 37, 43 (Tex.Crim.App. 1974) (emph. added).

the witness thereon, and to introduce in evidence those portions which relate to the testimony of the witness.[111]

**Practice Note:** Use of an otherwise privileged writing to refresh a party's memory will constitute a waiver of that privilege.[112]

**B. Impeachment.**

Electronic communications can be some of the most useful tools for impeachment. Impeachment evidence is generally hearsay and does not have probative value.[113] Prior inconsistent statements offered to impeach the witness's credibility do not constitute hearsay because they are not offered for the truth of the matter asserted.[114] If the impeachment evidence meets a hearsay exception or exemption, however, it may be admitted as probative evidence.

The *Michael*[115] case gives an excellent summary of the means of impeachment: There are five major forms of impeachment: two are specific, and three are nonspecific. Specific impeachment is an attack on the accuracy of the specific testimony (i.e., the witness may normally be a truthteller, but she is wrong about X), while non-specific impeachment is an attack on the witness generally (the witness is a liar, therefore she is wrong about X). The two specific forms of impeachment are impeachment by prior inconsistent statements and impeachment by another witness. The three non-specific forms of impeachment are impeachment through bias or motive or interest, impeachment by highlighting testimonial defects, and impeachment by general credibility or lack of truthfulness. Electronic evidence can be useful for providing specific impeachment (previous statements by the witness) as well as non-specific impeachment (photos of the witness in situations that reflect poorly on the witness's credibility).

1. Prior Inconsistent Statement.

In examining a witness concerning a prior inconsistent statement made by the witness, whether oral or written, and *before* further cross-examination concerning, or extrinsic evidence of such statement may be allowed, the witness must be told the contents of such statement and the time and place and the person to whom it was made, and must be afforded an opportunity to explain or deny such statement. If written, the writing need not be shown to the witness at that time, but on request the same shall be shown to opposing counsel. If the witness unequivocally admits having made such statement, extrinsic evidence of same shall not be admitted. This provision does not apply to admissions of a party-opponent as defined in Rule 801(e)(2).[116]

If a proper predicate is not laid, the inconsistent statement may be excluded and further cross-examination on the subject blocked. However, if the witness is the opposing party, no confrontation is required, and no opportunity to explain need be given.

2. Impeaching Hearsay Statements

The credibility of hearsay statements can be impeached just as if the statements were uttered by a witness. If an opponent successfully uses online communications from a third party, an attorney can put on evidence to impeach the credibility of the out-of-court declarant. Tex. R. Evid. 806 provides that when a hearsay statement, or a non-hearsay statement defined by Rule 801(e), has been admitted in evidence, the credibility of the out-of-court declarant may be attacked. Evidence of a statement or conduct by the declarant at any time may be offered to impeach the out-of-court declarant. There is no requirement that the declarant be afforded an opportunity to deny or explain. If the credibility of the out-of-court declarant is attacked, it may be supported by any evidence which would be admissible if the declarant had testified as a witness. If the party against whom a hearsay statement has been admitted then calls the declarant as a witness, the party is entitled to examine the declarant on the statement as if under cross-examination.

**C. Character Evidence.**

Social networking evidence can be especially useful for providing character evidence or evidence of a party's prior conduct.

Evidence about prior instances of conduct used to show that a person acted in conformity on a particular occasion is generally inadmissible.[117] However, under 404(b), such evidence may be admissible for other purposes, such as showing proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident. Further, evidence of a person's habit or routine practice, whether corroborated or not and regardless of the presence of eyewitnesses, is relevant to prove that the conduct of the person on a particular occasion was in conformity with the habit or routine practice.[118]

---

[111] Tex. R. Evid. 613.

[112] *City of Denison v. Grisham*, 716 S.W. 2d 121, 123 (Tex.App.— Dallas 1986, orig proceeding)

[113] *Lewis v. Merrill*, 295 S.W.2d 920, 923 (Tex.Civ.App. 1956).

[114] *See Flores v. State*, 48 S.W.3d 397, 404 (Tex.App.—Waco 2001, pet. ref'd).

[115] *Michael v. State*, 235 S.W.3d 723, 726 (Tex.Crim.App. 2007).

[116] Tex. R. Evid. 613(a) (emph. added).

[117] *See*, *Burton v. Kirby*, 775 S.W.2d 834, 837 (Tex.App.–Austin 1989, no writ); *Penwell v. Barrett*, 724 S.W.2d 902, 907 (Tex.App.—San Antonio 1987, no writ).

[118] Tex. R. Evid. 406.

Although evidence of specific acts is limited, character evidence through testimony of a person's reputation or by testimony in the form of an opinion is admissible.[119] If reputation or opinion testimony is admitted, evidence of specific instances of conduct is permitted on cross-examination.

## IX. UNFAIR PREJUDICE.

If an attorney trying to keep a piece of evidence out has failed to block the evidence based on relevance, authenticity, hearsay, or the original writing rule, the final step is the requirement to balance evidence's probative value against the potential for unfair prejudice, or other harm, under Rule 403. This rule states: Although relevant, evidence may be excluded 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, or needless presentation of cumulative evidence.

Although Rule 403 may be used in combination with any other rule of evidence to assess the admissibility of electronic evidence, courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in the following circumstances:

**Offensive language.** When the evidence would contain offensive or highly derogatory language that may provoke an emotional response.

> *Monotype Corp.*, 43 F. 3d at 450 (Finding that trial court properly excluded an email from a Microsoft employee under Rule 403 that contained a "highly derogatory and offensive description of ... [another company's] type director.").

**Computer Animations.** When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation.

> *Friend v. Time Manufacturing Co.*, 2006 WL 2135807 at * 7 (D. Ariz. 2006)("Therefore, the question is simply whether the animation accurately demonstrates the scene of the accident, and whether the 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.").

> *State v. Sayles*, 662 N.W. 2d 1, 11 (Iowa, 2003) (Appellate court found no error in trial court's admission of computer animation slides showing effects of shaken infant syndrome, finding that trial court properly considered state version of Rule 403, and admitted evidence with a cautionary instruction that the evidence was only an illustration, not a re-creation of the actual crime).

**Summaries.** When considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 1006.

> *Weinstein*[120] ("Summary evidence is subject to the balancing test under Rule 403 that weighs the probative value of evidence against its prejudicial effect.").

**Reliability and Accuracy.** In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence.

> *St. Clair v. Johnny's Oyster and Shrimp Inc.*, 76 F. Supp. 2d 773 (S.D. Tx. 1999) (Court expressed extreme skepticism regarding the reliability and accuracy of information posted on the internet, referring to it variously as "voodoo information". Although the court did not specifically refer to Rule 403, the possibility of unfair prejudice associated with the admissibility of unreliable or inaccurate information, as well as for confusion of the jury, makes Rule 403 a likely candidate for exclusion of such evidence).

## X. EXPERT TESTIMONY AND OPINIONS.

### A. Basis of Expert Testimony and Opinions.

Increasingly, parties are bringing electronic evidence directly to experts, including Facebook posts, Twitter "tweets," online photo albums, and other relevant social networking posts. To determine how this evidence affects an expert's work, attorneys should look back at the rules regarding expert testimony.

### B. Factors Relied Upon.

The general rule is that, once properly qualified, an expert can base his or her opinion on just about anything remotely relevant to the issue he or she is called to testify about—including evidence of online

[119] Tex. R. Evid. 405(a).

[120] JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 1006.08[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997).

activity. Tex. R. Evid. 703 permits an expert to rely on the following to base his opinion:

**Personal Knowledge.** This would include such observations as statements made by the parties, testing results, etc.

**Facts/Data Made Known to the Expert at or Before the Hearing.** Many mental health professional rely and may rely on other evidence presented by others, deposition testimony and reports of other experts.

**Inadmissible Evidence, if Relied on by Others.** The reliance on tests, trade journals, other medical reports, etc. has not created much controversy in regard to expert opinions.[121] However, a problem may arise when the expert begins to recount a hearsay conversation he has had with another. Tex. R. Evid. 703 implies that this type of testimony is permissible, but the case law indicates that there are limits. A trial court may permit the expert to state that his or her opinion was based in part on what another had related, but should not permit the expert to disclose what was actually said.[122] The pre-rules case of *Moore*,[123] held that such testimony was limited to show the foundation of the opinion. In *Birchfield*,[124] the Court held that "[o]rdinarily an expert witness should not be permitted to recount a hearsay conversation with a third party, even if that conversation forms part of the basis of his opinion." However, the *Birchfield* court permitted the testimony to stand based on the theory of invited error on the part of defendant's counsel. This principle can be used to block an expert from detailing what third parties have said in online communications, even if an attorney cannot prevent it from influencing the experts conclusion.

### C. Jury Trials

Courts have also placed limits on expert testimony in jury cases. For example, in *Ochs*,[125] the court held that a psychologist in a child abuse case was not permitted to testify before a jury as to the propensity of the child complainant to tell the truth regarding the alleged abuse. The court reasoned that such testimony invaded the province of the jury in regard to judging the credibility of the witness.[126] Social studies are generally inadmissible hearsay before a jury, although the worker is competent to testify as a witness.[127] A court should not exclude the testimony of a social worker merely because that witness is not court-appointed.[128]

## XI. DEMONSTRATIVE EVIDENCE.

There is often confusion about demonstrative evidence. Demonstrative evidence is used as an aid to the court in presenting information, but it is not admitted into evidence, and it cannot be taken back into the jury room along with the admitted evidence. Common examples of demonstrative evidence are PowerPoint slide shows, lists or drawings on a tablet, or other visual aids. An attorney can use courtroom demonstratives without authenticating or admitting them into evidence. For example, demonstrative evidence may be used during voir dire.[129]

Demonstrative evidence does not have to meet admissibility requirements under the rules of evidence. However, while a court has the discretion to permit counsel the use of visual aids, including charts, to assist in summarizing the evidence, the court also has the power to exclude such visual aids.[130]

If a demonstrative does meet the requirements for admissibility, an attorney may offer it into evidence. One court allowed the admission into evidence of a golf club that was alleged to be similar to one used in a crime.[131] Demonstrative evidence that summarizes or even emphasizes the testimony is admissible if the underlying testimony has been admitted, or is subsequently admitted into evidence.[132] Admission of charts and diagrams which summarize a witness' testimony is within the discretion of the court.[133] Even if exhibits contain excerpts from witness' testimony

---

[121] *See, Noriega v. Mireles*, 925 S.W.2d 261, 264-265 (Tex.App.— Corpus Christi 1996, writ denied).

[122] *First Southwest Lloyds Ins. Co. v. MacDowell*, 769 S.W.2d 954, 958 (Tex.App.—Texarkana 1989, writ denied). *In Sosa by and through Grant v. Koshy*, 961 S.W.2d 420, 427 Tex.App.— Houston [1st Dist.] 1997, review denied).

[123] *Moore v. Grantham*, 599 S.W.2d 287, 289 (Tex. 1980).

[124] 747 S.W.2d at 365.

[125] *Ochs v. Martinez*, 789 S.W.2d 949, 956 (Tex.App.–San Antonio 1990, writ denied)

[126] *Id.* at 957.

[127] *Rossen v. Rossen*, 792 S.W.2d 277, 278 (Tex.App.–Houston [1st Dist.] 1990, no writ); *see also, Chacon v. Chacon*, 978 S.W.2d 633, 638 (Tex.App.-El Paso 1998, no pet.). Under Tex. Fam. Code §§ 107.054-55, while a social study is made part of the record, it is subject to the rules of evidence in being presented to a jury.

[128] *See, Davis v. Davis*, 801 S.W.2d 22, 23 (Tex.App.— Corpus Christi 1990, no writ).

[129] *See Hanson v. State*, No. 07-07-0138-CR (Tex.App.— Amarillo Oct. 9, 2008, no pet.) (memo. op.).

[130] *See Hartin v. State*, No. 09-07-00547-CR (Tex.App.— Beaumonth Apr. 22, 2009, no pet.) (memo. op.).

[131] *See Lynch v. State*, No. 07-06-0104-CR (Tex.App.— Amarillo May 23, 2007, no pet.) (memo. op.).

[132] *North American Van Lines, Inc. v. Emmons*, 50 S.W.3d 103, 130 (Tex.App.—Beaumont 2001, pet. denied).

[133] *Speier v. Webster College*, 616 S.W.2d 617, 618 (Tex. 1981); *Uniroyal Goodrich Tire Co. v. Martinez*, 977S.W.2d 328, 342 (Tex. 1998).

and are admitted, the trial court must permit them to be taken into the jury room.[134]

## XII. CONCLUSION

Attorneys can be reluctant to delve into issues relating to electronic evidence. There is a perception that attorneys are incapable of being competent at technical issues. However, it is critical that attorneys zealously advocate for their cl]ients, and a part of that is learning to be comfortable working with electronic evidence that can be the most important and useful evidence in a case. Every attorney started as a beginner at one point, and there is no shame in being a beginner at electronic evidence—as long as you learn. Please do not shy away from electronic evidence. If you are capable of passing a bar exam, you are capable of understanding how to effectively use electronic evidence.

[134] *Houston Lighting & Power Co. v. Klein I.S.D.*, 739 S.W.2d 508, 519 (Tex.App.—Houston [14th Dist.] 1987, no writ).