26th ANNUAL FAMILY LAW CONFERENCE

Hosted by
Louisiana State University

ELECTRONIC EVIDENCE
A PROFESSOR WARREN L. MENGIS APPROACH

By: Kenneth P. Haines
Weems, Schimpf, Haines,
Shemwell & Moore (APLC)
912 Kings Highway
Shreveport, LA 71104

Brd. Cert. Appellate Practice (2017)
Brd. Cert. Family Law (2004)
Certified by: The Louisiana
Board of Legal Specialization

I. BACKGROUND

When I was a law student at LSU, circa 1986-1989, the most influential people on my legal education were Adjunct Professor Mike Rubin and Professors Tom Galligan and Warren Mengis. I name these men because they all taught me something that stayed with me my entire legal career.

Mike Rubin taught me, "Think most clearly for a **PAYING** client."[1] Tom Galligan taught me that a legal education can be fun.[2] Warren Mengis taught me something most students don't have the good fortune of learning in law school: that is, how to practice law.

Warren Mengis practiced law with "his good friend and law partner of some 32 years, Luther Cole," before becoming a law professor at LSU in 1982.[3] As Chancellor Jack Weiss said upon Professor Mengis's passing in 2011, "Warren Mengis was one of the most popular teachers ever to grace the

---

[1]Professor Rubin would often suggest the answer to a security devices question with the caveat that he, "Reserved the right to think more clearly for a paying client."

[2]Professor Galligan used jokes and funny stories to make legal points in class. I cannot recall a day where he ever came to class without a smile on his face or in a foul mood. He was more than once voted the favorite professor of the student body.

[3]Anyone who ever sat in Professor Mengis's class cannot count the number of times Professor Mengis mentioned his 32 years of practicing law with Luther Cole.

halls of our law school."[4]

Professor Mengis taught me Louisiana Civil Procedure, Successions and Donations, and Ethics. In his classes is where I first learned where legal theory and everyday practicality met. Professor Mengis was the practitioner's law professor. If you had him for procedure, you know that he taught the subject literally and down to its finest points.

For instance, who could ever forget Professor Mengis's description of the procedure involved in discovering written materials, "You dictate your Request for Production of Documents or Subpoena Duces Tecum, hand it to your secretary, print it out, staple a blue back on it, put that in the brief case and to court I got business." Remember also that the procedure for preventing the discovery of written materials is, as Professor Mengis taught, "You dictate your Motion for Protective Order or Motion to Quash, "hand it to your secretary, print it out, staple a blue back on it, put that in the brief case and to court I got business."[5]

When I was asked to present this topic by my friend, Clint Bowers, he

---

[4]http://www.law.lsu.edu/news/2011/12/07/professor-warren-mengis-the-peoples-professor

[5]On almost no occasion, would Professor Mengis fail to use his ending catch phrase, "to court I got business." In some instances, he would further opine that "there is nothing quite so satisfying in the practice of law as a paying client or closed file."

sent me two books as assistance in presenting the subject.[6] Considering that one of the books was a text used for teaching the subject to law students and the other a 209 page study on the subject of electronic evidence, I decided that I needed to more narrowly tailor the topic.

Pondering the topic and wondering about an interesting presentation, I thought of my old law professor, Warren Mengis. Obviously, electronic evidence and all of its forms that exist today, did not exist in 1986, or 1989 for that matter.[7] So, I could not have learned from Professor Mengis his practical approach to electronic evidence; but, if such evidence were a thing in 1986-1989, the good professor would have most assuredly presented in the manner I use today. With that backdrop, I present the topic, Electronic Evidence, A Professor Warren L. Mengis Approach.

---

[6]Shira A. Scheindlin & Daniel J. Capra, Electronic Discovery and Digital Evidence (3rd Ed. 2015); Timothy J. Conlon & Aaron Hughes, Electronic Evidence for Family Lawyers (1st Ed. 2017).

[7]On August 6, 1991, the World Wide Web became publicly available when its creator, Tim Berners-Lee, posted a short summary of the project on the alt.hypertext newsgroup. Later, in 1993 the first web browser, MOSAIC, was introduced and made available free to the public. Bryant, Martin, *20 Years Ago Today the World Wide Web Opened to the Public*. https://www.thenextweb.com (Aug. 6, 2011); Grossman, David, *On this Day 25 Years Ago, the Web Became Public Domain*. https://www.popularmechanics.com (April 30, 2018).

II. INVENTORY THE PLACES TO FIND DIGITAL FILES

As you can see, Professor Mengis generally started his "how to" with dictation of a motion. In today's world, we don't start with dictation or a motion but instead with gaining an understanding of where we might find or where the other side will look for electronic evidence. The first place to look for electronic evidence is on the memory of the device on which it is stored.

Step 1: Inventory the Hardware: You don't know, so you must find out what devices are in play with the client, the opposition, and if they have children, do they have devices? What kind of devices do they have?

Common devices are of course, home computers, laptop computers, i-Pads or notebooks, i-Pods or hand held MP3 players and smart phones. Less common but other places to look include plug and play memory cards, thumb drives, hard drives, GPS devices, cameras, door bells, etc. Anywhere a digital memory can be found.

You must also know who owns or controls the device. Is the computer a family system or does it belong to one spouse's employer? Are the phones on an individual, business or family plan.

Step 2: What Social Media is in Play?: It is fair to say that since the 1990's nothing has more changed the social fabric of the world than social media. We need to know which platforms our clients use, which ones the other spouse uses and which ones the kids are using. As we have all likely learned, these sites are filled with pictures, communications, statements, insights and evidence, good and bad, for us and our opponent. We can learn what might be in play before we go to court or learn in court what we wished we had learned earlier. Have an idea what is in play sooner rather than later.

Since Nasir Ahmed first proposed the discrete cosine transform (DCT) compression technique in 1973,[8] the platforms and avenues by which people communicate and socialize have been ever growing.[9] Common platforms today include, but are certainly not limited to, Classmates (1995), Linked-In (2003), Facebook (2004), Pinterest (2010), Instagram (2010), Snapchat (2011), Tinder (2012), Vine (2013), TikTok (2017) and Parler (2020).[10]

---

[8]Ahmed, Nasir (January 1991). *How I Came Up With the Discreet Cosine Transform*, Digital Signal Processing 1, 4-5.

[9]Ahmed's algorithm became the most widely used data compression system on social media, enabling the practical transmission and streaming of digital media. It is the basis for most media compression standards such as JPEG, MPEG, Dolby Digital and MP3. Lea, William (1994), *Video on demand*. Research Paper 94/68. House of Commons Library.

[10]Parler has already been shut down on most service providers.

Don't forget to think about varying ways of delivering messages. In addition to the traditional e-mail and text message, communications can be sent via, Yahoo Messenger,[11] AOL Instant Messenger,[12] Facebook Instant Messenger, etc. Most of the social media sites have a function allowing transmission of an electronic message to someone else using the service.

Step 3: Keep It Ethical and Legal: In this step you have a couple of questions to ask. If the client brings you the evidence, then the question which must be asked is, "How was it obtained?" If the information has to be obtained then use proper methodology to obtain it.

When we ask the question, "How was the information obtained?", we are generally thinking about two things: a. staying out of jail and b. being able to actually use the evidence in court. Professor Mengis would never subscribe to discovery methods that would either send you or the client to jail or be ineffective for later use.

Information gathered through "Spyware" is not legally obtained. The term "Spyware" can be deceiving, but generally refers to software or devices

---

[11]Was shut down July 17, 2018.

[12]Remember "You Got Mail?" See the motion picture, *When Harry Met Sally*.

used to gather data surreptitiously.[13]

Professor Mengis would candidly say that there is a difference in "copying" and "intercepting." Copying may be permissible, intercepting is illegal.[14] Copying gets you what is on a device at a moment in time. An interception broadcasts, records or preserves for later retrieval the activity on the device as it occurs.[15] Interception runs afoul of the federal wiretapping and state of Louisiana wiretapping law.[16]

Professor Mengis would definitely say at this juncture to "hire an expert" in the collection of your electronic data. Not only do the forensic imaging devices they use gather all of the information, it helps preserve the chain of custody of the information you are trying to use. Keep in mind that it is very easy to delete portions of a text message and give an impression that is not

---

[13]Timothy J. Conlon & Aaron Hughes, Electronic Evidence for Family Law Attorneys, p. 28.

[14]*White v. White*, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001), copying stored emails on hard drive of a family computer after transmission was not violation of wiretap act; *O'Brien v. O'Brien*, 899 So. 2d 1133, 1137 (Fla. Dist. Ct. App. 2005), wife illegally obtained husband's conversations with another woman as they played "Yahoo Dominoes" online, because Spyware that wife installed intercepted the communication contemporaneously with transmission.

[15]Conlon, supra at p. 70.

[16]*O'Brien*, supra; *Klumb v. Goan*, 884 F. Supp. 2d 644 (E.D. Tenn. 2012), device that copied an email and rerouted it back through the Internet to a third party's email address constituted wiretapping.

depicted in the whole conversation.

Watch out for "Keyloggers!" Professor Mengis had uncanny "street smarts" and a good nose for nefarious conduct. Does the other side just know too much about your case? Would only you and the client know the content of a conversation? If yes, there is a good chance the client is communicating with you on a computer where a key logger has been installed.

These devices are readily available and are designed to broadcast activity on one computer to another. One device, "LightLogger" touts its ability to monitor the messages your child sends to others.[17] While monitoring your child's messages is a lawful activity, the device can easily be used for illegal activity.

Be careful about video and audio recordings. Louisiana is of course a single party consent state,[18] but beware the device installed to record conversations or activities that do not involve a party. Also know that the Federal Wiretapping Act does not prohibit silent video surveillance.[19]

Something that was not around in Professor Warren Mengis's day was

---

[17] http://www.hwsuite.com/keylogger/benefits

[18] See, La. R.S. 14:322; La. R.S. 15:1303 C.(4)

[19] 18 U.S.C. § 2511; Rebecca v. Lyon, *Hidden Home Videos: Surreptitious Video Surveillance*, 89(2) Chi.-Kent L. Rev. 877 (2014)

GPS tracking. The United States Supreme Court has weighed in on this issue.[20] A Justice of the Peace in Louisiana was suspended for six months without pay on a finding that placing a GPS tracking device on a community vehicle amounted to criminal stalking.[21]

Louisiana has a variety of criminal laws related to computer hacking and misuse of cellular data.[22] For instance, La. R.S. 14:222.3 makes it a low grade felony ($3,000.00 fine and 2 years with or without hard labor) to "possess a cellular tracking device or to use a cellular tracking device for the purpose of collecting, intercepting, accessing, transferring, or forwarding the data transmitted or received by the communications device, or stored on the communications device of another without the consent of a party to the communication and by intentionally deceptive means."

Exceptions are: "the owner of a motor vehicle, including the owner of a vehicle available for rent, who has consented to the use of the tracking device

---

[20]*United States v. Jones*, 132 S.Ct. 945 (2012), finding that government's installation of a GPS device on a target's vehicle constituted a search.

[21]*In re Sachse*, 2017-2008 (La. 3/13/2008), 240 So. 3d 170

[22]See generally, La. R.S. 14:73.1 through 14:73.12, Computer Related Crime and La. R.S. 14:222.2 (Cellular telephone counterfeiting) and La. R.S. 14:222.3 (Unlawful use of a cellular tracking device.)

with respect to that vehicle;"[23] "a parent or legal guardian of a minor child whose location or movements are being tracked by the parent or legal guardian;"[24] "ascertaining or attempting to ascertain the location of any telecommunications device that is part of a plan and that has been lost or stolen."[25] Do note, when the parents of the minor child are living separate and apart or are divorced from one another, this exception shall apply only if both parents consent to the tracking of the minor child's location and movements, unless one parent has been granted sole custody, in which case consent of the non-custodial parent shall not be required.[26]

In summary, take the practical step of determining how information was obtained. It could save both you and your client from facing a criminal charge and allow later use of the electronic evidence obtained.

III. OBTAINING AND PRESERVING EVIDENCE:

Once we know where to look, we need to use all available discovery techniques to get the information. As Professor Mengis would say in procedure class, "You need it, get it. But understand there are financial limits.

---

[23]La. R.S. 14:222.3 C.(4)

[24]La. R.S. 14:222.3 C.(7)(a)

[25]La. R.S. 14:222.3 C.(16)

[26]La. R.S. 14:222.3C.(7)(b)

Not sure what you got? Hire an expert."[27]

First thing, put the other side on notice that they should stop deleting data and preserve the evidence for trial. Generally, courts look at the issue of duty to preserve evidence from the context of "pending or reasonably foreseeable litigation."[28] A person engaged in conduct that might be harmful to the marriage is definitely going to be deleting as they go.

Grab the evidence available on "open" sources. This would include looking at readily available posts to social media accounts or electronic files created that are generally available to the public. I, myself, do not personally understand things such as the "dark web," but there are methods of researching these publicly available information sources and determining things relevant to your case. If you don't know how to do it, hire an expert.

Look at public forums. There are forums on the internet that cover almost every conceivable interest known to man. These can range from owners of certain automobiles or motorcycles, to dating service ratings, to fetish sites. Obviously, review the parties' pages on the various social media platforms.

---

[27]Professor Mengis delighted in the minute steps of using the law to obtain a practical result. This was literally how he viewed procedure. What are the physical steps taken to accomplish a desired consequence. He would walk a class through the actual process he would use in his private practice of law with Luther Cole.

[28]*West v. Goodyear Tire and Rubber Co.*, 167 F.3d 776 (2nd Cir. 1999); *Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423 (2nd Cir. 2001).

Look at cached information. This is information on previous versions of a page or site that has been held in storage. Big search engines like Google and Bing allow you to attach "cache" to your search. Can't figure it out, hire an expert.

Use the standard discovery methods available in the code. Requests for production of documents. Get access to the computers, hand held devices and phones where you need to obtain information. Have an expert retrieve the information so that there are no chain of custody issues.

IV. HAVING DIGITAL FILES ADMITTED INTO EVIDENCE:

The last part of the Mengis method is of course to actually use the evidence in court. He might describe the process something like this, "First, you take an exhibit sticker and place it on the back of the document.[29] Next, you have your file clerk make copies (one for your opponent, one for the judge, one for yourself and use the original to file into evidence).[30] Then, you get a 'red rope' out of your supplies and place the exhibits in there in the order you

---

[29]There is no doubt in my mind that Professor Mengis would include the minute step of placing an evidence sticker on the exhibit. He would further detail that the sticker should go on the back so as not to "obscure" any part of the document.

[30]Professor Mengis would **never** engage in the task of making copies. That is not what a real lawyer would do. Delegation was big in his practice.

plan to use them.[31] If your file is not too big, put it in the brief case and to court I got business."[32]

Ask yourself the question and plan, "How am I going to get the Judge to look at this evidence?" That literally means to determine if you need a computer; will you need to play audio or video; are you going to use paper copies, photos, etc.; does the court have the wiring and hardware in place for you to use the devices you intend to use to demonstrate your evidence? Many courthouses are old and do not have the ability to deal with modern technology. Be prepared to go pre-historic to show your evidence.

The next part of the process is thinking about the mechanical process of getting the exhibit admitted. Professor Mengis would detail the process something like, "First, you have to lay the foundation for the exhibit. Next, prepare to counter any objections to the evidence such as the hearsay rule, relevancy, or claim of privilege. Once you have accomplished that part, don't forget to 'offer, introduce and file' your exhibit into evidence." "Last," Professor Mengis would say, "if the judge does not accept the exhibit, make sure to "proffer" the exhibit, so that when you get up on appeal, those judges

---

[31]I credit even knowing there was a thing called a "red rope" to Professor Mengis. In his class is the first time I ever heard that term for an expandable file.

[32]Professor Mengis liked to go to court with a brief case. I suspect he would have frowned at the idea of having to use boxes of materials.

might figure it out."

Let's break down Professor Mengis's lesson. First is authentication.

When we think about electronic evidence, authentication is often where the battle is won or lost, because if the evidence can be authenticated its relevancy is almost always evident from the thing itself. Questions to ask, "Was the Facebook post created by a party?" "Did the email come from the person the claimant says it did?" Was the text message sent by the person the witness says sent it?"

According to Article 901 of the Code of Evidence, the requirement of authentication or identification as a condition precedent to admissibility is satisfied by **evidence sufficient to support a finding that the matter in question is what its proponent claims**.[33] The article then provides "illustrations" of authentication of identification that conforms to the rule.[34]

The illustrations provided include: 1. Testimony of a witness with knowledge that the matter is what it is claimed to be; 2. Nonexpert opinion on handwriting based on familiarity not acquired for purposes of litigation; 3. Comparison by trier or expert witness of specimens which have been authenticated; 4. Distinctive characteristics taken in conjunction with

---

[33]La. Code Evid. art. 901 A.

[34]La. Code Evid. art. 901 B.

circumstances; 5. Voice identification whether heard firsthand or by transmission or recording, by opinion; 6. Telephone conversations by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business; 7. Public records or reports; 8. Ancient documents or data compilation that is in such condition that no suspicion surrounds its authenticity, was in a place where it would likely be if authentic and had been in existence 30 years or more at the time it is offered; 9. Process or system used to produce an accurate result; and 10. Methods provided by legislation, "Act of Congress or Act of the Louisiana Legislature."

The 2016 case of *State v. Smith*, is a good study of admitting "social media" evidence.[35] Finding that Louisiana courts have dispensed "limited guidance" on the subject of admitting social media evidence,[36] the court provides a historic context to the issue from other states.[37] Citing, *Sublet v.*

---

[35]*State v. Smith*, 2015-1359 (La. App. 4th Cir. 4/20/2016), 192 So. 3d 836

[36]*State v. Smith*, at 840

[37]Discussed in the historic references are: *Griffin v. State*, 419 Md. 343, 19 A.3d 415 (2011), (finds that identifying date of birth and face in a photograph on a screenshot of a MySpace page that purports to reflect the creator and author of the post is insufficient authentication ... the mere fact that digital evidence exists on the internet does not, by itself, lead to the conclusion that it was created by the defendant). Compare, *Tienda v. State*, 353 S.W.3d 633 (Tex. Crim. App. 2012), equating social media post authentication to that of emails, text messages or internet chat rooms, i.e. whether the message can be sufficiently tied or linked to the author to justify submission to the trier of fact to determine authenticity.

State, 442 Md. 632, 113 A.3d 695 (2015),[38] three acceptable methods were identified for authenticating social media evidence. First, ask the purported creator if they created the profile and if they added the post in question. Second, search the computer of the person who allegedly created the profile and post and determine if that computer was used to create the profile and post. Third, obtain information directly from the social networking website.

In *Archaga v Johnson*, the Fifth Circuit Court of Appeal said that authentication of a document is sufficient when a reasonable trier of fact could find that the evidence is what the proponent claims it to be.[39] In this case, Archaga (an accountant) agreed to help bring multiple years of unfiled tax returns current for Johnson. Johnson (a husband and wife law firm) disputed that the parties had an "oral agreement" for the payment of accounting services.

The accountant used a combination of text messages and emails to prove an agreement and that allowed the court to award $30,000 on the oral agreement. On appeal, Johnson claimed the text messages and emails were not "authenticated."

---

[38] *Sublet v. State*, 442 Md. 632, 113 A.3d 695 (2014)

[39] *Archaga v. Johnson*, 19-85 (La. App. 5th Cir. 10/16/2019), 280 So. 3d 331

Relyng on *State v. Hayden*,[40] the 5th Circuit found that text messages and emails could be authenticated by the recipient of the texts.[41] Archaga, the recipient with personal knowledge of the facts surrounding the communications, properly authenticated them. Similar holdings are available in virtually all of the other circuits.[42]

In *State v. Gray*, Youtube videos, a/k/a electronic evidence, was properly authenticated and admitted over defendant's objection, when the investigating police officer testified that the video depicted what it was purported to be, i.e. a video of the defendant's gang activity in a park.[43] This evidence was allowed despite the the fact that the police officer did not know who made, posted, or the time that the recording was made. What the officer could say was the defendant was depicted in the video doing what is shown in the video.

As mentioned, once authenticated, most electronic evidence is going to

---

[40]*State v. Hayden*, 17-234 (La. App. 5th Cir. 12/20/2017), 235 So. 3d 1293

[41]*Archaga* at 341.

[42]See, *State v. Smith*, 2015-1359 (La. App. 4th Cir. 4/20/2016), 192 So. 3d 836, (authentication of social media evidence standard is reasonable fact finder can find that the proffered evidence is what it purports to be); *State v. Harris*, 52,541 (La. App. 2d Cir. 2/27/2019), 266 So. 3d 953, (copies of text messages authenticated by recipient); *State v. Benedict*, 04-742 (La. App. 3d Cir. 11/10/2004), 887 So. 2d 649 (screen shots of texts deemed admissible when authenticated by a witness with knowledge of the item depicted).

[43]*State v. Gray*, 2016-1195 (La. App. 4th Cir. 6/28/2017), 2017 WL 3426021

speak for itself as to its relevancy and if the party is the creator or subject of the posting. Hearsay should be easily overcome as well. In some instances, all you may be trying to do is merely show that the post was made and not necessarily prove that the statement contained in the post is true. That approach would overcome a hearsay objection as well.

V. THE BEST FOR LAST:

If I were going to add one final thought to handling electronic evidence, which obviously I am doing just that, I'd be remiss to not mention my "Go To" authority and source of helpfulness in this field. When in doubt and not trusting your own research or instincts, CALL PROFESSOR SALLY BROWN RICHARDSON.[44]

I can think of no greater compliment to pay Professor Richardson than to compare her insights on electronic evidence to what I believe Professor Mengis would have had. More than once in dealing with my own conundrums involving electronic evidence, I have picked up the phone and called her, emailed her and asked her to assist me. Never has she failed to return my call, write me back and help me find an answer. You will find no one more helpful

---

[44]Professor Sally Richardson at Tulane University is a 2009 honors graduate of the Paul M. Hebert Law Center, Louisiana State University. Her presentations at this very seminar have been more than once helpful to my practice, as well as, she has graciously responded to emails and returned my phone calls.

on the subject, I guarantee.[45]

To summarize Electronic Evidence using the Mengis Approach:

1. Know what hardware and social media sources are in play.

2. Obtain the evidence legally and by ethical means.

3. Consult a Millennial or Zoomer[46] and/or use an expert to help you when dealing with electronic evidence.[47]

4. Plan for court to have a means to present the evidence and authenticate it.

5. When in doubt call Professor Richardson.

---

[45]The Cajun humorist, Justin Wilson, would often utter, "I guarantee" during a story. I expected Professor Mengis to use the word, but alas, he never did.

[46]A Millennial (Gen Y) or Zoomer (Gen Z) are individuals either born into a world with social media (Gen Z) or grew up watching its evolution (Gen Y). They are so adept at navigating the world of social media that they are known by the coined phrase, "tech natives."

[47]Before incurring the cost of an IT expert, I find Millennials and Zoomers to be very helpful in this field as these generations of Americans have grown up during the digital age and know the ins and outs of cell phones and social media platforms. If you are like me, you have two sons, one from each generation, as consultants.