ELECTRONICALLY STORED INFORMATION A-Z: ACQUIRE, EVALUATE, ADMIT

KENNETH G. RAGGIO
Raggio & Raggio, PLLC
3316 Oak Grove Avenue
Dallas, TX 75204
(214) 880-7500
kenneth@raggiolaw.com

EMILY MISKEL
KoonsFuller, PC
5700 W. Plano Pkwy., Suite 2200
Plano, Texas 75093
(972) 769-2727
emily@koonsfuller.com

State Bar of Texas
41st ANNUAL
ADVANCED FAMILY LAW COURSE
August 3-6, 2015
San Antonio

CHAPTER 51

TABLE OF CONTENTS

ELECTRONICALLY STORED INFORMATION A-Z: ACQUIRE, EVALUATE, AND ADMIT.

I. INTRODUCTION.

Increasingly, attorneys and judges are on the front lines of using modern, electronic evidence. 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 endeavors to provide a practical guide to obtaining, using, and admitting modern evidence.

II. THE STANDARD OF CARE RE: ESI.

A. ABA Model Rule 1.1

Client-Lawyer Relationship
Rule 1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment 8 reads as follows:

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (**Bold** Emphasis added)

B. Competence Required in Social Media.

Not surprisingly, states have started to adopt some specific ethical rules dealing with cloud computing and other items dealing specifically with electronic storage or transmission of data. Of particular interest right now is the North Carolina 2014 Formal Ethics Opinion 5 dealing with a duty for the lawyer to counsel with the client about social media.

The opinion states:

"Lawyers must provide competent and diligent representation to clients. Rule 1.1 and Rule 1.3. To the extent relevant and material to a client's legal matter, **competent representation includes knowledge of social media and an understanding of how it will impact the client's case including the client's credibility**. If a client's postings on social media might impact the client's legal matter, the lawyer must advise the client of the legal ramifications of existing postings, future postings, and third party comments. Advice should be given before and after the law suit is filed." (Emphasis added)

The opinion also deals with advising clients on removing social media posts and spoliation:

"..., in general, relevant social media postings must be preserved....

"The lawyer therefore should examine the law on spoliation and obstruction of justice and determine whether removing existing postings would be a violation of the law."

Even though this opinion is from North Carolina, the Ethics opinion may have been prompted by the famous Allied Concrete Co. v. Lester, 736 SE 2d 699 (VA 2013).

C. Is Texas Far Behind?

D. NB: Don't Forget Your Duty to Also Preserve Client Confidences.

California has dealt with protecting client confidentiality in a sweeping way in Formal Opinion Interim 11 – 0044. This opinion is in the context were a lawyer (who truly did not understand the breadth of a production request for ESI) agreed to a discovery order requiring production of his client's ESI, and found out how ineffective a "clawback" of data would be. And how little a Judge wants to get into the middle of a discovery dispute, no matter what the cause. Relevant language includes:

"A fundamental duty of an attorney is '[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.' [cite omitted] 'Secrets' includes 'information, other than that protected by the attorney-client privilege, that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client.' [cite omitted] Both 'secrets' and 'confidences' are protected communications. [cite omitted] 'A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1) without the informed consent of the client.'

"Similarly, an attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and client which are sought in discovery. [cite omitted] In a civil discovery setting, while the holder of the privilege is not required to take strenuous or 'Herculean efforts' to resist

disclosure in order to preserve the privilege, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure only if the attorney and client act reasonably to protect that privilege in the first instance. [cite omitted] A lack of reasonable care to protect against the disclosure of privileged and protected information when producing ESI can be deemed a waiver of the attorney-client privilege. See Kilopass Technology Inc. v. Sidense Corp. (N.D. Cal. 2012) 2012 WL 1534065 at *2-3 (attorney-client privilege deemed waived as to privileged documents released through e-discovery because screening procedures employed were unreasonable). [cite omitted]

"Accordingly, the reasonableness of an attorney's actions to ensure both that secrets and confidences, as well as privileged information, of a client remain confidential and that the attorney's handling of a client's information does not result in a waiver of any confidence, privilege, or protection, is a fundamental part of an attorney's duty of competence. Cal. State Bar Formal Opn. No. 2010-179. [Emphasis added]

III. ACQUIRING DATA.

One of the pleasures one can find in a divorce or other family law case is finding proof of a party's own words proving that such 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.

Clearly the most fertile field for out of court statements that may have a damning influence in a family law case is social media postings. Not surprisingly, tools have been developed to make the collection of such data easier and with built in robustness to answer authenticity and chain of custody challenges.

A. No Reasonable Expectation of Privacy.

In terms of use in a family law proceeding, there is no expectation of privacy with social media postings and messages even if there are restrictions on who can see the Facebook, Linked In, MySpace, Twitter, or other social media entries for a party. That horse has left the barn. So the tools that aggregate such postings will survive that feeble challenge, if made.

B. X-1 Social Discovery Software.

X-1 is software 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. But the software can be set up to track many "persons of interest" (the other party in a divorce or custody case?) and preserve the data in a way that is intended to be easily authenticated and therefore admissible in legal proceedings.

C. Archive Social.

Archive Social is a social media archiving solution for record keeping 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 Linked In in a manner that complies with subpoenaed requests for information. So the company employing a spouse in your case may be able to give you some relevant information gleaned internally. (Which is one reason we always tell our clients to NEVER use the Company email for any communications.)

D. 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 on line content including social media and provided a comprehensive fully searchable archive of online data.

E. 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.

F. Celebrite Touch.

Celebrite Touch Can download EVERYTHING on a Smart Phone. Celebrite Touch is the latest version of a machine that was initially used by the cell phone providers to transfer contacts and other data between a user's old and new cell phone. Not surprisingly, this tool has made its way into our realm, most commonly with the court ordered "capture" of a phone at the courthouse during a hearing, followed by 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 the courts are delegating 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.

G. The Poor Man's Way to Preserve Facebook Data.

It is important that the client understands the power of settings in Facebook, and that the client actually uses them. Instruct the account holder (client) to go into "Settings" of their Facebook account and navigate to the "Backup" screens/menus. Here the account holder can preserve, at that point in time, the complete history and the entire content of a Facebook account holder's account with all posts, time lines, and everything in the account. So it is preserved before it is "hacked" or bogus postings appear. Go to Home, Settings, then Click "Download a copy of your Facebook data," enter your password, and you will eventually be sent a link with the archive of your Facebook. Similarly one can get their Twitter archive.

It takes about and hour or so to complete the process. Although information from the download is abundant, it may not include 100% of a person's Facebook account. If a person uses a mobile device/application to access their Facebook page, some of those postings may not show up in the archived page, depending on the application. Additionally, it will not reveal any information that has been deleted from an account, even if that information was recently deleted. It is important to find out what application your client or the opposing party uses to access their social media sites.

H. All of the Above Applies to YOUR Client as Well as the Opposing Party.

I. The ESI Audit Letter

The ESI audit letter – really intended for your client – is something that should be sent out to your client even before the client retains you. (In fact, it is a good practice to have it filled out even before your initial consultation, if it is your practice to have a prospective client fill out forms.) It certainly should be completed early in the case so that there can be a frank discussion of do's and don'ts during the case or prior to the institution of the case if litigation is known or should be known to be imminent. And by definition, a consultation qualifies.

The audit letter suggests ways to minimize the continued generation of electronic evidence that could be unfavorable to your client, but also at the same time suggest avenues for collection of ESI from the other party that could be useful.

J. Acquiring Data from the Other Side

Normal request for Production, specifically including ESI requests ("including data in its native electronic form") is the normal way of getting the data. But there are other methods of legal self-help.

Using the data trolling software tools above, absent being produced by the other side, it is not really acquiring it from the other side. Using such tools can help to be a check and balance on the truth-telling or completeness of production that is made, when made by the other side. Also, there could be use if there is potential spoliation or deletion of evidence that is later produced but that was first acquired through using the previously mentioned trolling software.

1. Beware of Data Your Client Presents

You have a duty to evaluate the data YOUR client produces to you, especially recordings or other data that conceivably could have been taken or made in a way frowned upon by many state or federal statutes, starting with the Federal Wiretap Act and Federal Electronic Communications Privacy Act.

Even though case law provides a glimmer of limited extract for such a mess (see *Pollock v Pollock*, 154 F.3d 601, (6th Cir.1998), the trend is toward privacy and exclusion of such evidence (see *Collins v Collins*, 904 S.W.2d 792 (Houston [1st Dist.] 1995).

2. Specific Discovery Requests

A specific discovery request which some may view as being too global and some as too specific, could include a request for social media as below:

A complete copy of each of your social media profiles and all entries posted, including but not limited to Facebook, MySpace, Twitter, Instagram, LinkedIn Meetme, or any other dating/social website.

See the Appendix for the detail required for production in a "Federal" case. We, as civilian divorce lawyers, are under the same standard as the Feds in having the responsibility to request relevant data. This is true even if we do not have the "federal" resources to analyze it once received. So a caveat: consider being as narrow as you feel comfortable in making a discovery request, as the needle in the haystack could be buried under 50 haystacks instead of one.

3. Requesting Hard Drives or Information

One of the biggest mistake attorneys make is to treat ESI like it is completely different than the paper documents we typically request. In our new "paperless" world, everything people use to keep in their filing cabinet is now staying on the computer. Therefore, requesting said items on the computer does not require a different set of rules. However, there are some aspects of collecting electronic data which are different than collecting paper evidence. You must ensure that you have taken the proper steps in requesting the ESI. As the Supreme Court enunciated in *In re Weekley Homes,*

L.P., 295 S.W.3d 309 (Tex. 2009), a proper 196.4 discovery dispute should look something like this:

Step 1: Requesting party must make a "specific request for electronic information."

Step 2: The responding party must object if the information cannot be obtained by reasonable means in the form requested.

Step 3: Either side may request a hearing, but the burden remains on the responding party to offer evidence to prove that the information is not available by reasonable means in the form requested.

Step 4 (optional): The trial court may order additional discovery such as testing, sampling or depositions to determine the reasonability of the request.

Step 5: If the responding party fails to meet their burden, the court may order discovery but is still limited by Tex. R. Civ. P. 192.4.

Step 6: If the responding party meets their burden, the burden shifts to the requesting party to prove that the "benefits of ordering production outweigh the costs."

Step 7: If the court order production of "not reasonably-available information" the court must also order the requesting party to pay the expenses of the extraordinary steps.

4. Capturing Cell Phone Data

The Cellebrite Touch previously mentioned is the gold standard. But use of the results requires a careful chain of custody including "capture" of the phone to be analysed.

5. The Federal Case Standard is Also Our Standard

The Appendix from a Federal Case Management Order shows the detail and levels of production requests. Even though most of our cases don't have complexity – or budget – for such, we technically are under the same duty to request (and produce requested ESI) in a fashion not dissimilar from the Appendix.

6. Tracking Devices

It is all too easy for an "owner" to put a tracking device – a magnetic GPS – onto the bottom of an automobile; or a helpful, soon to be ex-spouse, giving their spouse a new iPhone, with tracking software installed and activated on it.

For such tracking devices to be legal, and potentially produce admissible data, there must be at least a colorable claim of ownership of the vehicle/phone to which the tracking device is attached; otherwise, there is the distinct possibility of violation of privacy and other laws that are covered in other presentations. But be aware that the person that utilizes those devices may be interested only in the use of the information, not in its formal use in a Court proceeding. Be aware of your client trumpeting information for which the source appears suspect or unexplained. It would be far better to incur the cost of traditional surveillance to try to get this type of evidence, as such a method would have the fact witness who would be able to offer testimony to support authenticity and admission.

a) Pinger
b) Find my Phone
c) Burner

K. Acquiring from 3rd Parties

It is really no different than a request from any third party, but be aware if you make a global request, there may be a significant charge for the production of the data.

As mentioned, subpoenas are a way to reach the records, if the record holder is within the reach of the subpoena. Otherwise, deposition of written questions – just as you would use for a far away pension fund – would be the next level of acquisition.

IV. ANALYZING DATA.

Many times production data when requested electronically is received electronically and should be parsed and looked at in an efficient electronic manner. Even simple searches, even if data produced in a searchable .pdf can help winnow down the initial universe of what may be relevant and useful in a case. This varies significantly from the old method of receiving documents in hard copy and really having to go through in a manual fashion to look at data for possible relevance.

There are computer tools to parse this data. But the massive data requested – and presumably received – almost always invites the hiring of a third party expert to be the one who conducts the data parsing. Such an expert can be appointed as a discovery master to actually take control of the data to resolve any privilege claims, and to segregate the data that meets certain criteria to all within the purview of the case. In some cases, such could be a quick and efficient way to get to the data in a way where both sides are not having to do the same work twice.

A. Traditional.

B. Computer Software Analysis & [Potential] Testifying Expert.

There are many software tools, but most are "run" by someone who, at time of attempted admission, must show competency, chain of custody, and the process used. The Appendix shows instructions of how emails could/ should be produced, among many other species of ESI. Most production shown is to be produced by a computer-friendly tool.

V. DATA SECURITY TIPS.

A. Nelson-Simek Practical Security Tips.

In their article, Preventing Law Firm Data Breaches, Nelson and Simek discussed security basics that every lawyer should know, including:

- Have a strong password of at least 12 characters. A strong 12-character password takes roughly 17 years to crack.
- Don't use the same password everywhere.
- Change your passwords regularly.
- Do not have a file named "passwords" on your computer.
- Change the defaults. Whether you are configuring a wireless router or installing a server operating system, make sure you change any default values.
- Laptops should be protected with whole disk encryption; no exceptions.
- Backup media should be encrypted. If you use an online backup service, make sure the data is encrypted in transit and while being stored. Also, be sure that employees of the backup vendor do not have access to decrypt keys.
- Thumb drives should be encrypted.
- Keep your server in a locked rack in a locked closet or room. Physical security is essential.
- Most smartphones write some amount of data to the phone. Opening a client document may write it to the smart-phone. The iPhone is data rich. Make sure you have a PIN for your phone. This is a fundamental protection. Don't use "swiping" to protect your phone as thieves can discern the swipe the vast majority of the time due to the oils from your fingers. Also make sure that you can wipe the data remotely if you lose your phone.
- Solos and small firms should use a single integrated product to deal with spam, viruses and malware.
- Wireless networks should be set up with the proper security. First and foremost, encryption should be enabled on the wireless device. Whether using Wired Equivalent Privacy (WEP) 128-bit or WPA encryption, make sure that all communications are secure. WEP is weaker and can be cracked. The only wireless encryption standards that have not been cracked (yet) are WPA with the AES (Advanced Encryption Standard) or WPA2.
- Make sure all critical patches are applied. This may be the job of your IT provider, but too often this is not done.
- If software is no longer being supported, its security may be in jeopardy. Upgrade to a supported version to ensure that it is secure.
- Control access.
- Using cloud providers for software applications is fine, provided that you made reasonable inquiry into their security. Read the terms of service carefully and check your state for current ethics opinions on this subject.
- Be wary of social media applications, as they are now frequently invaded by cybercriminals. Giving another application access to your credentials for Facebook, as an example, could result in your account being hijacked. And even though Facebook now sends all hyperlinks through Websense first (a vast improvement), be wary of clicking on them.
- Consider whether you need cyber insurance to protect against the possible consequences of a breach. Most insurance policies do not cover the cost of investigating a breach, taking remedial steps or notifying those who are affected.
- Dispose of anything that holds data, including a digital copier, securely. For computers, you can use a free product like DBAN to securely wipe the data.
- Use wireless hot spots with great care. Do not enter any credit card information or login credentials prior to seeing the https: in the URL.
- For remote access, use a VPN or other encrypted connection.

See Sharon D. Nelson and John W. Simek, Preventing Law Firm Data Breaches, Texas Bar Journal, May 2012, p 364.

B. Ken’s Tips

Telling your client what is required or prudent, reminds you of the universe of what’s out there to be produced by or procured from the other side:

1. Educate your client from the beginning consultation about vigilance to protect their data and communications.
2. Don't forget to mention their duty not to delete information or social media postings.
3. Regularly remind clients of their continuing duty to preserve.
4. Make clients aware of how easy it is to "mine" data from their social media postings.
5. Get client's written consent to email communications.
6. Suggest that a client do an "audit" or "sweep" of their electronic devices – phones, computers, and even vehicles.
7. Get a grip on passwords, password retention, and password changes.
8. Turn it off when not using it. Or at least log off.
9. Have regular IT audits of your internal data security and backup systems.
10. Encrypt.
11. Fill out the Audit letter.
12. Follow the advice you give.
13. Assume the other side is as well versed as you are in ESI and security measures.

Data security for your data, for your client’s data, and for the data you receive in a case is paramount.

Awareness of the ways data security and privacy can be breached, either on the lawyers' side or on the client's side helps prevent same. Hopefully, this realization and action on it will lessen the chance for a breach of privacy.

VI. 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.[1]

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

VII. 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.[2] 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).[3] This section quotes extensively from the case, including selections relevant to authenticating ESI:

A. 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.

B. 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 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

[1] *In Re F.P.*, 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005).
[2] Tex. R. Evid. 901.
[3] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D.Md. 2007) (memo. op.).

> 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. [4]

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.[5]

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.[6]

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

> 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.[7]

---

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

[5] *Id*.

[6] *Id*.

[7] *Id*.

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.[8]

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.

Practice Tip: While caselaw on authenticating and admitting electronic evidence is still developing, practitioners may need to rely on cases from other jurisdictions. 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.

C. 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.[9] One well respected commentator has observed: [10]

> [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

[8] *Id*.

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

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

> 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.[11] 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;

(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.[12]

D. 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.[13] 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.[14] An e-mail is sufficiently authenticated when a person responds to an e-mail that was sent to the person's e-mail address.[15] 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.[16]

E. Text Messages.

Text messages can be authenticated by applying the same factors as emails.[17]

---

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

[12] *Massimo v. State*, 144 S.W.3d 210, 215 (Tex.App.—Fort Worth 2004, no pet.).

[13] *Varkonyi v. State*, 276 S.W.3d 27, 35 (Tex.App.—El Paso 2008, pet. ref'd).

[14] *Id*.

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

[16] *People v. Pierre*, 838 N.Y.S.2d 546, 548-49 (N.Y. App. Div. 2007)

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

Recent Texas Case:[18] 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.[19]

Recent Texas Case: 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.[20] 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.

F. 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.[21] *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?''

[18] *Montoya v. State*, No. 05-10-01468-CR (Tex.App.—Dallas Mar. 30, 2012) (memo. op.).

[19] *Gardner v. State*, 306 S.W.3d 274 (Tex. Crim. App. 2009).

[20] *Black v. State*, No. 02-10-00283-CR (Tex.App.—Fort Worth 2012).

[21] *Lorraine*, 241 F.R.D. at 555-56.

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).

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.

G. Tinder and Other Online Personals

Online dating websites (Match, eHarmony, OkCupid, PlentyOfFish) and dating apps (Tinder, Grindr) are increasingly being used by our family law clients. The following cases address the authentication of online personals.

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.[22] 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.[23]

H. Facebook.

Since the *Tienda* decision, several Texas courts have evaluated Facebook evidence. The recent *Campbell*[24] 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 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.

I. 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.[25]

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

[22] *Musgrove v. State*, No. 03-09-00163-CR (Tex.App.—Austin 2009) (memo. op.).
[23] *In Re J.A.S.*, No. 11-09-00176-CV (Tex.App.—Eastland January 13, 2011) (memo. op.).
[24] *Campbell v. State*, 382 S.W.3d 545, 551-53 (Tex. App.-Austin 2012, no pet.)
[25] *Lorraine*, 241 F.R.D. at 556.

(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.*,[26] 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*,[27] 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*,[28] 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).

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*[29] case discusses the use of Kik chat evidence, but unfortunately does not go into detail on how the evidence was authenticated or admitted.

J. Stored versus Processed Data

In general, electronic documents or records that are merely *stored* in a computer raise no computer-specific authentication issues.[30] 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.

K. 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.[31] 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. That said, although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional ''hard copy'' records. 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*,[32] 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

[26] 878 A.2d at 93–94.
[27] 152 F.3d at 1249.
[28] 200 F.3d at 629–31.
[29] *Smallwood v. State*, No. 02-13-00532-CR (Tex.App.—Fort Worth 2015).
[30] *Lorraine*, 241 F.R.D. at 543 (emph. added).
[31] *Lorraine*, 241 F.R.D. at 556-59.
[32] 263 F.3d at 1180–81.

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*,[33] 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 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

[33] 336 B.R. 437.

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. However, it also is plain that commentators and courts increasingly recognize the special characteristics of electronically stored records, and there appears to be a growing awareness, as expressed in the Manual for Complex Litigation, 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. Further, although ''it may be better to be lucky than good,'' as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.

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).

L. 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.[34] 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 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.[35] 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.[36] 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.[37]

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

[34] *Lorraine*, 241 F.R.D. at 561-62.
[35] *See* Tex.R. Evid. 901(b)(9).
[36] *Reavis v. State*, 84 S.W.3d 716, 719-20 (Tex.App.-Fort Worth 2002, no pet.).
[37] *Reavis v. State*, 84 S.W.3d 716, 719-20 (Tex.App.-Fort Worth 2002, no pet.).

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.[38]

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.[39] 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.

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*,[40] 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.

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).

M. 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

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

[39] *Brown v. State*, No. 12-11-00027-CR (Tex.App.—Tyler Sept. 7, 2011) (memo op.).

[40] 268 Conn. 781, 847 A.2d 921, 950–52 (2004).

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.[41] However, a recording can be properly authenticated even when the witness cannot identify every voice in the recording.[42]

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.[43]

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.

N. 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.[44] 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.

VIII. 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.[45] 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.[46]

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.[47] 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.[48] The defendant objected, citing the Best Evidence Rule. The Court 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.

IX. 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

---

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

[42] *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.).

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

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

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

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

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

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

additional evidence at the appropriate time. Judge Bonnie Sudderth explains:[49]

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.)

X. 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.[50] (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.[51] Hearsay is inadmissible unless otherwise permitted by the rules or by statute.[52]

Put more simply, any out-of-court statement, whether by the witness or another person, is hearsay 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.[53] 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.[54]

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.[55] However, all hearsay exceptions require a showing of trustworthiness.[56]

A. Unreflective Statements.

Evidence obtained from email, text messaging, or social networking sites, such as Facebook, MySpace, or Twitter, is often relevant in family law 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

[49] 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/

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

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

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

[53] Tex. R. Evid. 802.

[54] *See, Miranda v. State*, 813 S.W.2d 724, 735 (Tex.App.— San Antonio 1991, pet ref'd).

[55] *Fischer v. State*, 252 S.W.3d 375, 379 (Tex.Crim.App. 2008).

[56] *Robinson v. Harkins & Co.*, 711 S.W.2d 619, 621 (Tex.1986).

communication is particularly prone to candid statements of the declarant's state of mind, feelings, emotions, and motives.[57] 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.[58] Unlike the excited-utterance exception, the rationale for this exception stems from the statement's contemporaneity, not its spontaneity.[59] 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.[60] The *Fischer*[61] 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.[62] The excited-utterance exception is broader than the present-sense-impression exception.[63] 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.[64] The *Goodman*[65] 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 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.[66] 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.[67] 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).[68] However, a statement is inadmissible if it is a statement of memory or belief offered to prove the fact remembered or believed.[69] 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.[70]

---

[57] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 570 (D.Md. 2007) (memo. op.).
[58] Tex. R. Evid. 803(1) (emph. added).
[59] *Rabbani v. State*, 847 S.W.2d 555, 560 (Tex.Crim.App. 1992).
[60] *Id*.
[61] *Fischer v. State*, 252 S.W.3d 375, 381 (Tex.Crim.App. 2008).
[62] Tex. R. Evid. 803(2).
[63] *McCarty v. State*, 257 S.W.3d 238, 240 (Tex.Crim.App. 2008).
[64] *Id*.
[65] *Goodman v. State*, 302 S.W.3d 462, 472 (Tex.App.—Texarkana 2009, pet. ref'd).
[66] Tex. R. Evid. 803(3).
[67] *Garcia v. State*, 246 S.W.3d 121, 132 (Tex.App.—San Antonio 2007, pet. ref'd).
[68] *Id*.
[69] Tex. R. Evid. 803(3).
[70] *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)).

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.[71] 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.[72] 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.[73]

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.[74] 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 affidavit. Courts have admitted check registers, medical bills and receipts, and cancelled checks in this way.[75] 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.[76] 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).[77] 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.[78] 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.[79]

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.[80] 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.[81] 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.[82]

---

[71] Tex. R. Evid. 803(5).

[72] *Johnson v. State*, 967 S.W.2d 410, 416 (Tex.Crim.App. 1998).

[73] *Id*.

[74] Tex. R. Evid. 803(6).

[75] *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.).

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

[77] *Id*.

[78] *Id*.

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

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

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

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

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.'"[83]

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-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.[84] A few ethics opinions have held that mining metadata is not unethical.[85] 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.[86]

The exemption for admissions by a party-opponent is extremely useful in overcoming a hearsay objection to texts, emails, Facebook wall posts, etc. The

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

[84] 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.

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

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

Massimo[87] 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 family case held that statements by a party on his MySpace page were non-hearsay as admissions by a party-opponent.[88]

XI. 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*[89] 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.[90]

An adverse party is entitled to have the writing produced at the hearing, to inspect it, to cross-examine the witness thereon, and to introduce in evidence those portions which relate to the testimony of the witness.[91]

Practice Note: Use of an otherwise privileged writing to refresh a party's memory will constitute a waiver of that privilege.[92]

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.[93] 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.[94] If the impeachment evidence meets a hearsay exception or exemption, however, it may be admitted as probative evidence.

The *Michael*[95] 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).[96]

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.

---

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

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

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

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

[91] Tex. R. Evid. 613.

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

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

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

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

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

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.[97] 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.[98]

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.[99] If reputation or opinion testimony is admitted, evidence of specific instances of conduct is permitted on cross-examination.

While the use of character evidence in civil cases is limited by the rules of evidence, in family law, several important exceptions make the use of character evidence relevant and commonly-used. In custody cases, evidence of the prior conduct of a parent is regularly presented to show that future behavior is likely to be in conformity. One termination case has drawn a relevant distinction: The evidence regarding the father's prior criminal behavior, convictions, and imprisonment was not offered to prove conduct in conformity or to impeach his credibility as a witness. Instead, it was relevant and probative to whether he engaged in a course of conduct that endangered the child.[100] A modification case held that, while evidence of past misconduct or neglect may not of itself be sufficient to show present unfitness in a suit affecting the parent-child relationship, such evidence is permissible as an inference that a person's future conduct may be measured by her past conduct as related to the same or similar situation.[101] Another modification case held that a parent's prior conduct can give rise to a material and substantial change in circumstances of the child.[102]

XII. 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

[97] *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).

[98] Tex. R. Evid. 406.

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

[100] *In re JTG*, 121 SW3d 117, 133 (Tex.App.--Fort Worth 2003, no pet.).

[101] *Kirby v. Chapman*, 917 S.W.2d 902, 911 (Tex.App.—Fort Worth 1996, no pet.).

[102] *In re ALE*, 279 S.W.3d 424 (Tex. App.--Houston [14th Dist.] 2009, no pet.).

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[103] ("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).

XIII.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. For example, social study evaluators are being handed printouts of a spouse's online activity. 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 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.[104] 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.[105] The pre-rules case of *Moore*,[106] held that such testimony was limited to show the foundation of the opinion. In *Birchfield*,[107] 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 issue can often come up with social workers assigned to custody cases. In their testimony, they should not be able to restate what third parties have said, unless that statement fits one of the hearsay exceptions.[108] 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.

---

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

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

[105] *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).

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

[107] 747 S.W.2d at 365.

[108] *Rosendorf v. Blackmon*, 800 S.W.2d 377, 380 (Tex.App.–Corpus Christi 1990, no writ); *D.M.B. v. R.L.B*., 798 S.W.2d 399, 402 (Tex.App. – Amarillo 1990, no writ).

C. Jury Trials

Courts have also placed limits on expert testimony in jury cases. For example, in *Ochs*,[109] 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.[110] Social studies are generally inadmissible hearsay before a jury, although the worker is competent to testify as a witness.[111] A court should not exclude the testimony of a social worker merely because that witness is not court-appointed.[112]

XIV. 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.[113]

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.[114]

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.[115] Demonstrative evidence that summarizes or even emphasizes the testimony is admissible if the underlying testimony has been admitted, or is subsequently admitted into evidence.[116] Admission of charts and diagrams which summarize a witness' testimony is within the discretion of the court.[117] Even if exhibits contain excerpts from witness' testimony and are admitted, the trial court must permit them to be taken into the jury room.[118]

XV. CONCLUSION

Obtaining and processing electronic information can be the most difficult part or working with these new resources. Attorneys should creatively think about the best way to obtain evidence and how the discovery rules can be applied to your client, an opposing party, or a third party.

Once electronic evidence is obtained, attorneys and judges are still working with the same familiar rules of evidence. Do not be intimidated just because evidence is electronic in nature. A judge who is familiar with how the rules of evidence apply to electronic evidence can successfully rule on the admission of even the newest technologies.

XVI. APPENDIX

1. ESI Audit Letter

2. ESI Presentation Letter

3. "Federal" ESI production request from DOJ

---

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

[110] *Id.* at 957.

[111] *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.

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

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

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

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

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

[117] *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).

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

RAGGIO & RAGGIO, PLLC

RAGGIO FAMILY LAW

INFORMATION REGARDING
SOCIAL NETWORKING AND ELECTRONICS

Because the Internet could be a source of much public information about yourself, we need to know what presence, if any, you have there. Just "Googling" a name often provides valuable information and is permissible.

Also, all of us now have much reliance upon, and information contained in, electronic devices such as computers, tablets, cell phones, and digital cameras. To properly advise you, we need to know the following:

1. Do you have a profile on a social network like Facebook, Twitter, Linked-in, MySpace, Google Plus, etc.? **[Y] [N]**
   a. Is it in your name? **[Y] [N]**
   b. If not in you name, what is the name associated with the profile? . . . . . .
   c. How many such profiles do you have? . . . . . .
   d. Are they open to the public? **[Y] [N]**
   e. What is posted? . . . . . .
   . . . . . .
   f. When was your most recent deletion or change to each of your social media sites?.. . . . . .
   . . . . . .
   g. Where else do you post your communications?.. . . . . .
   h. Have you commented on articles, blogs, or pictures on other people's social media sites? **[Y] [N]**
   i. Do you use social media software (such as X1 Social Discovery software or Archive Social software) that collects and makes a record of all entries and data (or "mines" everything) that is currently on or has been on your social media site, or would do the same on someone else's social media site? **[Y] [N]**

2. Do you have your own website? **[Y] [N]**
   a. If so, what is the site(s) name? . . . . . .
   b. How long have you had it? . . . . . .
   c. When did you first launch the site? . . . . . .
   d. When was your site last changed? . . . . . .

3. Do you have a blog? **[Y] [N]**
   a. If so, what is the name? . . . . . .
   b. What do you post there? . . . . . .
   . . . . . .

4. Do you post material on YouTube? **[Y] [N]**

3316 OAK GROVE AVENUE, DALLAS, TEXAS 75204 | 214 880-7500 | FAX 214 880-7506 | WWW.RAGGIOLAW.COM | KENNETH@RAGGIOLAW.COM

APPENDIX 1

a. If so, what exactly to you post? .. . .
. . . . . .
. . . . . .

5. Do you buy or sell on eBay, Craigslist, or similar services? **[Y] [N]**

6. Do you, or does your cell phone, make, accept, or send:
   a. Text messages? **[Y] [N]**
   b. Emails? **[Y] [N]**
   c. Video recordings? **[Y] [N]**
   d. Audio records? **[Y] [N]**
   e. Internet browsing inquiries? **[Y] [N]**

7. On your cell phone, do you have software, such as SpoofCall or CallerID Faker, that can change the caller ID that a recipient of a call sees? **[Y] [N]**

8. Do you send or receive text messages from your cell phone? **[Y] [N]**

9. Do you use software (such as Xpire or CyberDust) that erases or deletes text message after they have been read, or after a specific time period? **[Y] [N]**

10. Have you recently lost or replaced your cell phone? **[Y] [N]**
    a. If so, what happened to the "old" phone?. . . . . .

11. Do you upload anything from your cell phone to the internet, such as posting a photo or comment to Facebook? **[Y] [N]**

12. Do you email from a computer, Blackberry, iPhone, iPad, iPod, iTouch, tablet, or other smart phone? **[Y] [N]**
    a. List all email addresses you have used: . . . . . .
    . . . . . .
    . . . . . .
    . . . . . .
    . . . . . .

    b. Do you use: *(include user names)*
    Skype? **[Y] [N]** Google +? **[Y] [N]**
    Gchat? **[Y] [N]** FaceTime? **[Y] [N]**
    Instant Message? **[Y] [N]** Or any other? **[Y] [N]**

    c. Do you use email encryption software? **[Y] [N]**
    If so, what do you use?.. . . . . .

13. Do you use file sharing, file storage or peer-to-peer programs? **[Y] [N]**
    a. If so, which ones? . . . . . .

14. Do you share a computer, cell phone, or other electronic device? **[Y] [N]**
    a. If so, with whom?

15. How do you keep track of your passwords for computers, cell phones, and other devices?. . . . . .
    . . . . . .

16. How often do you change "key" passwords?.. . . . . .

17. Who possibly has access to your computers, phones, and other devices by knowing, or guessing, your passwords?. . . . . .
    . . . . . .

18. Has your email, cell phone, or computer been "hacked" before? **[Y] [N]**

19. On what media do you store files or photos?

PC	**[Y] [N]**	Mac	**[Y] [N]**
Laptop	**[Y] [N]**	PDA	**[Y] [N]**
DVD	**[Y] [N]**	CD	**[Y] [N]**
Compact Flash or SD/microSD cards	**[Y] [N]**		
Flash drives	**[Y] [N]**	Portable hard drive	**[Y] [N]**
Thumb drives	**[Y] [N]**		

20. Do you back up your files to, or keep files on, an internet site such as DropBox, iCloud, Microsoft SkyDrive, Box, Mozy, or a similar Cloud based resource? **[Y] [N]**
    a. If so, which ones?. . . . . .
    . . . . . .

21. Is there a physical backup of any of your data anywhere else? **[Y] [N]**
    a. Where? . . . . . .

22. Do you store, keep, or maintain any adult material on your call phone or any other electronic device? **[Y] [N]**
    a. If so, on what device(s) do you store this material?.. . . . . .
    . . . . . .

23. Do you understand that you have a duty to preserve and not to delete any data or documents that could be relevant to your potential or actual family law case? **[Y] [N]**

If you have questions about any of these inquiries, please discuss them with one of us. But please respond to the questions quickly and return to us.

_____ _____

Client Name Date Returned

3316 OAK GROVE AVENUE, DALLAS, TEXAS 75204 | 214 880-7500 | FAX 214 880-7506 | WWW.RAGGIOLAW.COM | KENNETH@RAGGIOLAW.COM

APPENDIX 1

GRIER H. RAGGIO (1988)
LOUISE B. RAGGIO (2011)
THOMAS L. RAGGIO*+
KENNETH G. RAGGIO*+
GRIER H. RAGGIO, JR.*
BARBARA G. VAN DUYNE
JEFFREY T. RAGGIO (2014)

Law Offices of
RAGGIO & RAGGIO, P.L.L.C.
3316 OAK GROVE AVENUE
DALLAS, TEXAS 75204
214/880-7500

FAX: 214/880-7506
Website: http://www.raggiolaw.com

*FELLOW
AMERICAN ACADEMY OF
MATRIMONIAL LAWYERS

+CERTIFIED SPECIALISTS
FAMILY LAW
TEXAS BOARD OF
LEGAL SPECIALIZATION

July 6, 2015

The Best Client
Anywhere in Texas

RE: IMOMO ____; Cause No. _____

Dear :

Recent changes in the law require that you now protect from change and destruction all electronically stored information (ESI) during your case. This means that until your case is over and you are told otherwise by me, you must not delete any email, text messages or voice-mails. If you are using Quick Books, Microsoft Money or other accounting software at home, you cannot delete those files. Frankly if in doubt, keep it.

If you suffer a hardware failure such as a hard drive that stops working, it is imperative that you let my office know so we can notify the opposing counsel. You will need to keep that broken hard drive until I tell you that you can dispose of it. This is also true for your cell phone. If you decide to replace your phone (or a computer or laptop or tablet), you cannot turn in your old one, and you must keep the old one safe until your case is over and I tell you it is now okay to get rid of your old phone.

This rule of keeping old, broken or inoperable hardware also applies to:

iPods or any music player,
iPads or any computer tablet,
thumb drives and portable hard drives,
GPS devices, handheld or built into your car,
Security systems that record video or audio,
Digital audio recorders,
Media used to hold your digital photos, even the ones on your cell phone. This includes CD's, DVD's, flash drives, SD drives, Compact Flash Drives or any type of device used to hold the digital photo, video or audio.

If you have any question, before you delete anything, before you through anything away, call the office and speak to me. The penalties the court can impose on you for what the court deems to be the destruction of evidence or potential evidence can be very severe. This includes the court prohibiting you from presenting certain evidence yourself, deciding issues without any input from you or making you pay for the recreation of the lost or damaged ESI.

APPENDIX 2

ESI Hold
Page 2

You are likely wondering why any of this is necessary. The answer is simply that now the law requires it and it is my duty to make sure you are informed of your responsibilities to protect and preserve all electronically stored information while your case is pending.

Do not take this responsibility lightly as the court takes it very seriously. If you have any questions at all, please call me and I will be happy to answer them for you.

Sincerely,

Raggio & Raggio, P.L.L.C.

_____

I, _____, acknowledge receipt of this letter and the instructions have been explained to me.

Date: _____ _____
Client Name

APPENDIX 3

N. Scott Sacks, Attorney (D.C. Bar No. 913087)
Jessica N. Butler-Arkow, Attorney (D.C. Bar No. 430022)
Anna T. Pletcher, Attorney (California Bar No. 239730)
Adam Severt, Attorney (Member, Maryland Bar, numbers not assigned)
Ryan Struve, Attorney (D.C. Bar No. 495406)
Shane Wagman, Attorney (California Bar No. 283503)
United States Department of Justice
Antitrust Division
450 Fifth Street NW, Suite 7100
Washington, DC 20530
Telephone: 202-307-6200
Facsimile: 202-616-8544
Email: scott.sacks@usdoj.gov

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

EBAY INC.

Defendant.

Case No. 12-CV-05869-EJD

ATTACHMENT B TO JOINT CASE MANAGEMENT STATEMENT AND [PROPOSED] ORDER: DOJ STANDARD SPECIFICATIONS FOR PRODUCTION OF ESI

U.S. Department of Justice Antitrust Division
Standard Specifications for
Production of ESI and/or Hard Copy as Images and Text

Introduction:

This document describes the standard specifications and procedures for making an image-based production to the Antitrust Division in the form of load files**.**

- To ensure the efficient processing and review of any electronic production, Division legal, economic, and technical staff need to resolve the details prior to production, and preferably before you or your vendor begin to gather and process responsive documents.
- Care should be taken to ensure that all responsive data and metadata are preserved in the collection process.
- These are not Unicode compliant specifications and do not cover production of translations. Please contact Division staff if either of these is anticipated.

A. Categories of Documents

Discussion regarding the details of an electronic production should focus on seven categories of documents: (1) email and other electronic messages (*e.g.,* instant messaging), (2) other electronic documents, (3) hard copy documents, (4) shared resources, (5) databases, (6) audio and video data, and (7) foreign-language materials. General requirements for each category of document are outlined below. For information regarding document-specific metadata and bibliographic information (identifying information), please refer to the enclosed Metadata Table of Requested Fields.

1. Email, Attachments, and Other Electronic Messages

Email and other electronic messages (*e.g*., instant messages (IMs)) should be produced as image files with related searchable text, metadata and bibliographic information. Depending on how the company's systems represent names in email messages or IMs, we may require a table of names or contact lists from custodians.

Email repositories, also known as email databases (*e.g*., Outlook .PST, Lotus .NSF), can contain a variety of items, including messages, calendars, contacts, tasks, etc. For purposes of production, responsive items should include the "Email" metadata/database fields outlined in the Metadata Table, including but not limited to all parent items (mail, calendar, contacts, tasks, notes, etc.) and child files (attachments of files to email or other items), with the parent/child relationship preserved. Similar items found and collected outside an email repository (*e.g*., .MSG, .EML, .HTM, .MHT) should be produced in the same manner.

Each IM conversation should be produced as one document.

A. Attachments. Pay special attention to the PARENTID and ATTACHMENTIDS fields, which are used to track email families. While this example relates to email families, all attachment relationships for all responsive documents are to be produced in this format.

EXAMPLE: Consider ABC-JD-00000001 a 10-page parent email, with records ABC-JD-00000011 to ABC-JD-00000015, ABC-JD-00000016 to ABC-JD-00000020, and ABC-JD-00000021 to ABC-JD-00000025 as its attachments. Fields should be populated exactly as follows using the semicolon as the multi-entry delimiter for ATTACHMENTIDS:

BEGDOC#	ENDDOC#	PARENTID	ATTACHMENTIDS	FAMILYRANGE
ABC-JD-00000001	ABC-JD-00000010		ABC-JD-00000011; ABC-JD-00000016; ABC-JD-00000021	ABC-JD-00000001 – ABC-JD-00000025
ABC-JD-00000011	ABC-JD-00000015	ABC-JD-00000001		ABC-JD-00000001 – ABC-JD-00000025
ABC-JD-00000016	ABC-JD-00000020	ABC-JD-00000001		ABC-JD-00000001 – ABC-JD-00000025
ABC-JD-00000021	ABC-JD-00000025	ABC-JD-00000001		ABC-JD-00000001 – ABC-JD-00000025

2. Electronic Documents

Electronic documents include word-processing documents, spreadsheets, presentations, and all other electronic documents not specifically discussed elsewhere. Production of these items should include image files with related searchable text, metadata, and bibliographic information. All passwords and encryption must be removed from electronic documents prior to production. Please note the following:

A. Spreadsheets
Spreadsheets should be produced in native format (*e.g.*, as .XLSX files), with searchable text for the entire document, metadata, and bibliographic information. **Provide only a single image of the first page of the spreadsheet or provide a single placeholder image. The placeholder image must contain at a minimum the BEGDOC#, FILENAME, and FILEPATH.** The Bates range for a spreadsheet should be a single number (*e.g.*, ABC-JD-00000001 – ABC-JD-00000001). The linked native file name should match the BEGDOC#/DOCID with the appropriate file extension.

B. Presentations
Presentations should be produced in full slide image format along with speaker notes (which should follow the full images of the slides) with related searchable text, metadata, and bibliographic information. Presentations should also be produced in native format (*e.g.*, as .PPT files). The linked native file name should match the BEGDOC#/DOCID with the appropriate file extension.

C. Hidden Text
All hidden text (*e.g.*, track changes, hidden columns, hidden slides, mark-ups, notes) shall be expanded and rendered in the extracted text file. For files that cannot be expanded linked native files shall be produced with the image files.

D. Embedded Files

All embedded objects (*e.g.,* graphical files, Word documents, Excel spreadsheets, .wav files) that are found within a file shall be produced so as to maintain the integrity of the source document as a single document. For purposes of production the embedded files shall remain embedded as part of the original source document. Hyperlinked files must be produced as separate, attached documents. Any objects that cannot be rendered to images and extracted text (*e.g.,* .wav, .avi files) must be produced as separate extracted files treated as attachments to the original file.

E. Image-Only Files
All image-only files (non-searchable .PDFs, multi-page TIFFs, Snipping Tool screenshots, etc., as well as all other images that contain text) shall be produced with associated OCR text, metadata, and bibliographic information.

F. Proprietary File Types and Non-PC or Non-Windows Based Systems
Proprietary file types, such as those generated by financial or graphic design software, should be discussed with the Division in advance of production to determine the optimal format of production.

File types from non-PC or non-Windows bases systems (*e.g.,* Apple, UNIX, LINUX systems), should be discussed with the Division in advance of production to determine the optimal format of production.

G. Archive File Types
Archive file types (*e.g.,* .zip, .rar) must be uncompressed for processing. Each file contained within an archive file should be produced as a child to the parent archive file. If the archive file is itself an attachment, that parent/child relationship must also be preserved.

3. Hard-Copy (or Paper) Documents

Hard-copy documents are to be produced as black-and-white image files, except where noted below, with related searchable OCR text and bibliographic information. Special attention should be paid to ensure that hard-copy documents are produced as they are kept, reflecting attachment relationships between documents and information about the file folders within which each document is found. In addition, multi-page documents must be produced as single documents (*i.e.*, properly unitized) and not as several single-page documents. Where color is required to interpret the document, such as hard copy photos, and certain charts, that image must be produced in color. These color images are to be produced as .jpg format. Hard-copy photographs should be produced as color .jpg, if originally in color, or grayscale .tif files if originally in black-and-white.

4. Shared Resources

Shared Resources should be produced as separate custodians if responsive custodians have access to them or if they contain responsive documents. The name of the group having access would be used as the custodian name, *i.e.* Marketing Execs or Accounting Dept. The company will separately provide a brief description of each shared resource that includes a list of the custodians who have access to that shared resource.

5. Database Productions

Production of enterprise databases are not addressed in these specifications and must be discussed with the appropriate government legal and technical staff to determine the optimal production format; these will usually fall outside the scope of an image-based production. Care must be taken to ensure that all responsive databases and their metadata are preserved.

6. Audio/Video Data

These specifications do not address the production of audio/video data. Care must be taken to ensure that all responsive audio/video data and their metadata are preserved. These data types may be stored in audio or video recordings, voicemail text messaging, and related/similar technologies. However, such data, logs, metadata, or other files related thereto, as well as other less common but similar data types, should only be produced after consultation with and written consent of the Division as to the format for the production of such data.

7. Foreign-Language Materials

Foreign language materials should be produced in accord with the specifications set forth in the Division's Guidelines on Production of Translations and, if appropriate, the Division's Specifications for Unicode Productions. Both are available upon request.

B. De-duplication

Before doing any de-duplication, provide the Division with a written description of the method used to de-duplicate (including which elements are compared and what hash codes are used), and what is considered a duplicate. Then confirm that your approach is acceptable to the Division. The Division does not allow de-duplication of hard-copy documents, or that of "loose" electronic documents (*e.g.,* presentation slides located on the custodian's C: drive) against email attachment versions of those same documents. The integrity of any produced email and any related "document family" must be maintained except as limited by any claim of privilege. De-duplication should occur both vertically within each custodian and horizontally across custodians. Vertical de-duplication is crucial when a production includes electronic documents from back-up tapes. Horizontal de-duplication must be done in a way that preserves (and produces) information on blind copy (Bcc) recipients of emails and other custodians whose files contain the duplicates that will be eliminated from the production.

1. Custodian Append File

A Custodian Append file is to be produced when de-duplicating ACROSS custodians (*i.e.,* horizontal de-duplication) and data is produced on a rolling basis. The file must be provided on an incremental basis **starting with the second submission;** as more custodians are discovered for previously produced documents, this file is updated with **only the new** custodian information. The Custodian Append File is a two-field delimited file consisting of the DOCIDs of the previously delivered document and the **new** custodian names for the duplicates of those records that would otherwise have been produced in the subsequent (new) submissions.

These specifications do not allow for near de-duplication or email threading. These formats must be discussed separately with the Division and written consent obtained prior to the use of such techniques for production.

C. Document Numbering

Documents must be uniquely and sequentially Bates-numbered across the entire production, with an endorsement burned into each image. Each Bates number shall be of a consistent length, include leading zeros in the number, and unique for each produced page. Bates numbers should contain no more than three segments. For example, a company identifier, a middle segment identifying the custodian, and a sequential page counter with connecting hyphens. The number of digits in the numeric portion of the format should not change in subsequent productions, nor should spaces, hyphens, or other separators be added or deleted. Under no circumstances should bates numbers contain embedded spaces , slashes (/), backslashes (\), carats (^), underscores (_), ampersands (&), hash marks (#), plus signs (+), percent signs (%), dollar signs ($), exclamation marks (!), pipes (|), any character used as a delimiter in the metadata load files, or any character not allowed in Windows file-naming convention (,\ / : * ? " < > | ~ @ ^). Bates numbers may contain hyphens (-).

D. Privilege Designations

Documents redacted pursuant to any claim of privilege will be designated "Redacted" in the EPROPERTIES field as described in the Metadata Table. Appropriately redacted searchable text (OCR of the redacted images is acceptable), metadata, and bibliographic information must also be provided. All documents that are part of a document family that includes a document withheld pursuant to any claim of privilege will be designated "Family Member of Privileged Doc" in the EPROPERTIES field as described in the Metadata Fields table for all other documents in its family. Placeholder images with BEGDOC#, FILENAME, FILEPATH and reason withheld (*e.g.,* "Privileged") should be provided in place of the document images of the privileged document.

E. Sample

Before beginning production, a sample production covering files of all types, including emails and attachments, loose files including spreadsheets and presentations, redacted documents, etc., must be provided to the Division. The sample size should be between 500 to 1000 records to be large enough to be representative and small enough to review quickly. The Division will take a few business days to evaluate the sample and provide feedback. If there are any problems, corrected samples will need to be resubmitted until the Division can confirm the problems are resolved.

F. Load File Set/Volume Configuration

Each production must have a unique PHYSICALMEDIA name associated with it. This PHYSICALMEDIA name must also appear on the physical label. The PHYSICALMEDIA naming scheme should start with a 2 or 3 letter prefix (identifying your company) followed by a 3-digit counter (*e.g.,* ABC001). Each separate volume delivered on that media must also have a separate VOLUMENAME associated with it. On the root of the media, the top level folder(s) must be named for the volume(s). VOLUMENAME(s) should also be indicated on the physical label of the media. The volume naming scheme should be

based on the PHYSICALMEDIA name followed by a hyphen, followed by a 3-digit counter (*e.g.*, ABC001-001). Load file volumes should be as large as practical but not contain more than 100,000 records each. The VOLUMENAME should increase sequentially across all productions on the same PHYSICALMEDIA.

Under the VOLUMENAME folder, the production should be organized in 4 subfolders:
1. DOCLINK (contains linked native files , may contain subfolders, with no more than 5,000 files per folder)
2. IMAGES (may contain subfolders, with no more than 5,000 image files per folder)
3. FULLTEXT (may contain subfolders, with document-level text files)
4. LOADFILES (should contain the metadata, DII, OPT, LST, and custodian append files)

G. Deliverables

A cover letter spreadsheet must be delivered with each submission and should provide statistical information about the volume(s) and media produced. **Provide this in hard copy format and electronically on the deliverable media**. A sample is included in this PDF.

The Division accepts electronic productions loaded onto hard drives, CD-ROMs, or DVD-ROMs; however, production on hard drives minimizes costs and delay and is preferable. Where the size of the production exceeds the capacity of a single DVD-ROM, hard drives should be used as the delivery medium. For each piece of media a unique identifier (PHYSICALMEDIA) must be provided and should also be physically visible *on the exterior* of the physical item.

If the media is encrypted, please supply the tool for decryption on the same media, and instructions for decryption. A separate email must be sent with the password to decrypt.

All documents produced in electronic format shall be scanned for, and free of, viruses. The Division will return any infected media for replacement, which may affect the timing of the company's compliance with the production request.

The Division does not accept load file productions via email or those that are posted on download sites (*e.g.,* FTP, secure server).

H. Zip File Table of Contents

The attached zip file contains this document and a sample load file set following the guidelines set forth above.

1. Sample Cover Letter Spreadsheet: Sample .xlsx file for providing statistics associated with each submission.
2. Sample DII Load File: Sample format for the image load file, Summation image link file.
3. Sample OPT Load File: Sample format for the image load file, Opticon image link file.
4. Sample FullText LST File: Sample control list for loading extracted/OCR text.
5. Sample Custodian Append File: This is to be produced only when de-duplicating ACROSS custodians (*i.e.,* horizontal deduplication) and rolling productions are being delivered. Provide on an incremental,

rolling basis **starting with the second submission.** As more custodians are discovered for previously produced documents, this file is populated with **only the new** custodian information.

6. Sample Metadata Load File. Sample delimited text metadata file.

IMAGE and TEXT FILE SPECIFICATIONS, & LOAD FILE CONFIGURATION

Please review carefully for revisions.

Image/Native File Specifications

- Black-and-white Group IV Single-Page TIFFs (300 DPI). Color images should be provided in .JPG format when color is necessary.
- Image file names should match the page identifier for that specific image and end with the .tif (or .jpg if needed) extension. Example: ACME-ABC-0003072.TIF
- File names cannot have embedded spaces, commas, underscores, ampersands, slashes, back slashes, hash marks, plus signs, percent signs, exclamation marks, any character used as a delimiter in the metadata load files, or any character not allowed in Windows file-naming convention. (, _ & \ / # + % ! : * ? " < > | ~ @ ^)
- Images for a given document must reside together in the same folder.
- The maximum number of image files should be limited to 5,000 per folder.
- Native file names should match the BEGDOC#/DOCID entry for that specific record and end with the appropriate file extension.
- The maximum number of native files in a subfolder should be limited to 5,000 per folder.
- Any encryption or password protection will be removed from all native format files produced.

Searchable Text File Specifications and Control List Configuration

- Extracted text should be provided with all records, except for documents that originated as hard copy or redacted documents.
    - For hard copy documents, please provide OCR text.
    - For redacted documents, provide OCR text for the redacted version.
- There should be a single extracted/OCR text file per document, in ASCII Text format only. This load file configuration is not for use with a Unicode based production.
- The name of the text file should be the same as the document's first page/Bates number, with a TXT extension: DOCID.TXT.
- There must be a carriage return and line feed (CRLF) no later than the 250th character of the **first** line of every text file.
- All soft and hard returns in the native electronic or image file should be replicated as a Carriage Return Line Feed (CRLF) in the text file (i.e. the lines of text in the file terminate with a CRLF in correlation with the appearance of the native electronic or rendered image file). Pay particular attention to not allow multi-line paragraphs of e-mails to be rendered as a single, extended line of text.
- Text files should include page breaks that correspond to the "pagination" of the image files.
- Place text files under a "FULLTEXT" folder and provide a Control List file for loading in the "LOADFILES" folder on the delivery media.

Metadata Load File Delimiters and Configuration

- Field Separator ¶ (ASCII 020)
- Text Qualifier þ (ASCII 254)
- Substitute Carriage Return or New Line in data ® (ASCII 174)
- Multi-value separator **(Do Not Follow with Space)** ; (ASCII 059)
- Date format YYYYMMDD (date type fields only)
- Time format HH:MM:SS in 24-hour format (*e.g.*, 04:32 pm formatted to 16:32:00 – Do not include AM, PM, or Timezone indicators).
- There should be one line for every record in the load file. A carriage return and line feed (CRLF) must appear at the end of each record and ONLY at the end of each record.
- The first row of each metadata load file should be a header row containing the field names. Field names must match Division Metadata Table field names.
- All requested fields should be present in the metadata load file whether data exists or not. Field order must remain consistent in subsequent productions.

Summation Image Load File (.dii) Configuration

- @T ImageTag Token - MUST be first token listed for a document record and MUST be identical to BEGDOC# and DOCID entries in Metadata load file.
- @D @I Image Path Tokens - Path to image files as they appear on the delivery media.
- Image Files – Individual file names or iterated listing of image filenames comprising the document. Note that iterated filenames CANNOT contain leading zeros inside the braces {}.
- Example using iteration for document ABC-JD-00030005 to ABC-JD-00030352:

  @T ABC-JD00030005
  @D @I\ABC002\Images\001\
  ABC-JD-0003000{5-9}.tif
  ABC-JD-000300{10-99}.tif
  ABC-JD-00030{100-352}.tif

Opticon Image Load File (.opt) Configuration – Page level comma-delimited file containing seven fields per line.
PageID,VolumeLabel,ImageFilePath,DocumentBreak,FolderBreak,BoxBreak,PageCount

- PageID – PageID of the item being loaded. MUST be identical to the image name (less the file extension).
- VolumeLabel – Optional. If used it is preferable that it match the VOLUMENAME assigned in the corresponding metadata load file.
- ImageFilePath – The path to the image from the root of the delivery media.
- DocumentBreak – The letter "Y" denotes the first page of a document. If this field is blank the page is not the first page of a document.
- FolderBreak – Leave empty
- BoxBreak – Leave empty
- PageCount – Optional
- Example - ABC-JD00030005,,\ABC002\Images\001\ ABC-JD-00030005.tif,Y,,,

METADATA TABLE OF REQUESTED FIELDS

Please review carefully as fields have been added or modified from ATR's last set of specifications.

A "**X**" indicates that the field should be populated in the load file produced. "Other ESI" includes non-email files, such as, but not limited to MS Office files, WordPerfect files, etc.

Field Name	Field Description	Field Type	Hard-Copy	Email	Other ESI	Calendar Items
COMPANIES	Company submitting data	Multi-Entry	X	X	X	X
PHYSICALMEDIA	The unique identifier on the physical piece of media (e.g., ABC001)	Note Text	X	X	X	X
VOLUMENAME	Production volume number (e.g., ABC001-001)	Note Text	X	X	X	X
CUSTODIAN	Custodian(s) / source(s) -- format: *Last, First* or *ABC Dept*	Multi-Entry	X	X	X	X
TIMEZONE	The TimeZone from which the native file was collected.	Note Text		X	X	X
SPEC#	Subpoena/request paragraph number to which the document is responsive	Multi-Entry	X	X	X	X
HASHMD5	Document MD5 hash value (used for deduplication or other processing)	Note Text		X	X	X
HASHSHA	Document SHA1 hash value (used for deduplication or other processing)	Note Text		X	X	X
SEARCHVALUES	List of search terms used to identify record as responsive (if used)	Multi-Entry	X	X	X	X
BEGDOC#	Start Bates (including prefix) -- No spaces or special characters	Note Text	X	X	X	X
ENDDOC#	End Bates (including prefix) -- No spaces or special characters	Note Text	X	X	X	X
DOCID	Must equal the value appearing in the BEGDOC# field and be UNIQUE	Note Text	X	X	X	X
NUMPAGES	Page count	Integer	X	X	X	X
PARENTID	Parent record's BEGDOC#, including prefix (populated ONLY in child records)	Note Text	X	X	X	X
ATTACHMENTIDS	Child document list: BEGDOC# of each child (populated ONLY in parent records)	Multi-Entry	X	X	X	X
FAMILYRANGE	Range of the BEGDOC# value of the parent record to the ENDDOC# value (including prefix) of the last child record (for example, ABC-JD-00001201 - ABC-JD-00001220); populated for all documents in the group. Empty if the record is NOT in family grouping	Note Text	X	X	X	X
EPROPERTIES	Indicate all that apply : Record Type: E-Doc, E-Doc Attachment, Email, Email Attachment, Hard Copy, Calendar Appt Other Notations: Translation of [DOCID of original], Translated as [DOCID of Translation] Privilege Notations: Redacted, Privileged, Family Member of Priv Doc	Multi-Entry	X	X	X	X
FOLDERLABEL	Email folder path (sample: Inbox\Active); or Hard Copy folder/binder title/label	Note Text	X	X		X
FROM	Author of the Email or Calendar item (as formatted on the original)	Note Text		X		X
TO	Recipients of the Email (as formatted on the original)	Multi-Entry		X		X
CC	Names of the individuals who were copied on the Email (as formatted on the original)	Multi-Entry		X		X
BCC	Names of the individuals who were blind-copied on the Email (as formatted on the original)	Multi-Entry		X		X
SUBJECT	Email or calendar subject	Note Text		X		X
DATE_HC	Date of hard copy documents, if coded. Format: YYYYMMDD.	Date	X			
DOCDATE	This is a multipurpose date field. Populate with: DATESAVED for E-Docs; DATESENT for Emails; DATEAPPTSTART for calendar appointments; DATE_HC for hard copy documents, if available. Format: YYYYMMDD.	Date	X	X	X	X
DATECREATED	Date electronic file was created. Format: YYYYMMDD.	Date			X	
DATESENT	Date the Email was sent. Format: YYYYMMDD.	Date		X		X
TIMESENT	Time Email was sent -- Format: HH:MM:SS (use 24 hour times, e.g., 13:32 for 1:32 pm; timezone indicators cannot be included)	Time		X		X
DATERECEIVED	Date Email was received. Format: YYYYMMDD.	Date		X		X
TIMERECEIVED	Time Email was received. Format: HH:MM:SS (use 24 hour times, e.g., 13:32 for 1:32 pm; timezone indicators cannot be included)	Time		X		X
HEADER	The internet header information for Email sent through the internet;	Note Text		X		
INTERNETMSGID	Globally unique identifier for a message which typically includes messageid and a domain name. Example: <0E6648D558F338179524D555@m1p.innovy.net	Note Text		X		X
MESSAGEID	Proprietary email database/mailstore/post office file associated with centrally managed enterprise email servers. Microsoft Outlook PST EntryID, the UniqueID (UNID) for Lotus Notes, equivalent value for other proprietary mailstore formats.	Note Text		X		X
INREPLYTOID	Internet message ID of the Email replied to	Note Text		X		
CONVERSATIONINDEX	Email Thread Identification	Note Text		X		X
IMPORTANCE	Email flag indicating priority level set for message	Note Text		X		X
DELIVRECEIPT	Delivery receipt request notification for Email messages	Note Text		X		X
READRECEIPT	Read Receipt request notification for Email messages	Note Text		X		X
SENSITIVITY	Sensitivity field from Email messages	Note Text		X		X
REVISION	Revision number extracted from metadata of native file	Note Text			X	

DATESAVED	Date native file was last modified. Format: YYYYMMDD.	Date			X	
DATEPRINTED	Date native file was printed (metadata derived from Word documents, etc.)	Date			X	
EORGANIZATION	Company field extracted from the metadata of a native file	Note Text			X	
EAUTHOR	Author field value extracted from the metadata of a native file	Note Text			X	
LAST AUTHOR	Last Saved By field value extracted from metadata of a native file	Note Text			X	
ESUBJECT	Subject field value extracted from metadata of a native file	Note Text			X	
FILESIZE	File size in Bytes (integer value only - do not include unit of measure or decimal places - e.g., 568)	Integer		X	X	X
FILENAME	File name of native file (E-Docs or attachments to Email)	Note Text		X	X	X
APPLICATION	Application used to create native file (e.g., Excel, Outlook, Word)	Note Text		X	X	X
FILEEXTENSION	File extension of native file	Fixed Length 5 chars		X	X	X
FILEPATH	File path to native file as it existed in original environment	Note Text		X	X	X
DOCLINK	File path location to the current native file location on the delivery medium	Note Text			X	
DATEAPPTSTART	Start date of calendar appointment. Format: YYYYMMDD.	Date				X
TIMEAPPTSTART	Start time of calendar appointment. Format: HH:MM:SS (use 24 hour times, e.g., 13:32 for 1:32 pm; timezone indicators cannot be included)	Time				X
DATEAPPTEND	End date of calendar appointment. Format: YYYYMMDD.	Date				X
TIMEAPPTEND	End time of calendar appointment. Format: HH:MM:SS (use 24 hour times, e.g., 13:32 for 1:32 pm; timezone indicators cannot be included)	Time				X

APPENDIX 3

Cover Letter Spreadsheet for ABC Company Production to DOJ											
Matter: ABC's Acquisition of XYZ											
Custodian	**Physical Media Name**	**Volume Name**	**Begin Bates Number**	**End Bates Number**	**Intentionally Left Blank**	**Number of Records**	**Number of Images**	**Number of Native Files**	**Number of Extracted/OCRed Text Files**	**Volume Size in GB**	**Date Produced**
Doe, John	ABC001	ABC001-001	ABC-00000001	ABC-00005825		258	5,825	13	258		
Doe, Jane	ABC001	ABC001-001	ABC-00005826	ABC-00009536		365	3,711	52	362		
TOTALS FOR THIS VOLUME						**623**	**9,536**	**65**	**621**	**0.50**	mm/dd/yyyy
Daniels, Jack	ABC001	ABC001-002	ABC-00009537	ABC-00015263		1,150	5,727	156	1,149		
Weiser, Bud	ABC001	ABC001-002	ABC-00015264	ABC-00018273		600	3,010	20	598		
TOTALS FOR THIS VOLUME						**1,750**	**8,737**	**176**	**1,750**	**1.39**	mm/dd/yyyy
Brown, Charlie	ABC002	ABC002-001	ABC-00018274	ABC-00025225		1,315	6,952	68	1,310	1.02	mm/dd/yyyy
Flintstone, Fred	ABC002	ABC002-002	ABC-00025226	ABC-00035625	ABC-00025698 - ABC-00025982	2,023	10,115	85	2,023	2.00	mm/dd/yyyy
GRAND TOTALS						**5,711**	**35,340**	**394**	**8,071**	**4.91**	
*** This spreadsheet can be provided on a current production-specific or a cumulative production basis, but the totals per *volume* must be provided**											
**** This spreadsheet does not reflect the sample production provided**											
***** Volume size is actually space used not total available space on the delivery media**											

APPENDIX 3

CHECKLIST TO ENSURE PROPER DELIVERY TO DOJ ANTITRUST

ACTION	CHECKED
Does the production format conform to DOJ Antitrust Image and Text File Specifications and Load File Configuration?	
DOCLINK folder – Does count of native files = cover letter spreadsheet and count of records where DOCLINK field is populated?	
IMAGES folder – Does count of image files = cover letter spreadsheet?	
Are all images single-page tiff files or jpeg if color is necessary?	
FULLTEXT folder – Does count of TXT files = cover letter spreadsheet and count of records in control list (LST) load file?	
LOADFILES folder – Are the metadata, DII, control list, and custodian append (if applicable) files all provided? Does count of records match across metadata, DII, and LST files for the same volume?	
Are images and native files of presentations and spreadsheets provided properly (per negotiation)?	
Are line returns in fulltext files implemented properly? Does each hard and soft return in the native files appear as a Carriage Return Line Feed (CRLF) in extracted text file?	
Are all fields listed in the Metadata Table formatted correctly?	
Are all requested fields present in the load file? Is any requested field empty for all records?	
Has the DocDate field been populated properly from Email, E-Doc and Calendar metadata dates.	
Is the metadata file properly formatted without extraneous delimiter or null characters? Have conflicts between delimiter characters also embedded in metadata been resolved?	
Are the PARENTID & ATTACHMENTIDS fields populated correctly? Is the PARENTID field only populated on child records? Is the ATTACHMENTIDS field only populated on parent records?	
Has your custodian append file been created on an "incremental" basis, so that only new custodians will be added to previously produced records? Custodians previously listed on records should NOT be included.	
Have all family members of documents withheld for privilege been properly flagged?	
Does your Bates-numbering scheme exclude the characters prohibited in the Document Numbering specifications?	
Does your file naming scheme exclude the characters prohibited in the Document Numbering specifications?	
Has each physical piece of media been labeled on the exterior with a unique identifier per the configuration specifications (PHYSICALMEDIA)?	
Have you specified the VOLUMENAME(s) as the root folder(s) on media?	
Have you submitted your cover letter spreadsheet electronically and in hard copy?	

APPENDIX 3