21st Century Discovery and Evidence: Electronically Stored Information

Richard R. Orsinger
richard@momnd.com
http://www.orsinger.com

McCurley, Orsinger, McCurley,
Nelson & Downing, L.L.P.

San Antonio Office:
1717 Tower Life Building
San Antonio, Texas 78205
(210) 225-5567
http://www.orsinger.com

and

Dallas Office:
5950 Sherry Lane, Suite 800
Dallas, Texas 75225
(214) 273-2400

New Frontiers in Marital Property Law 2010
October 28-29, 2010
Hyatt Regency Resort and Spa at Gainey Ranch
Scottsdale, AZ

Table of Contents

21st Century Discovery and Evidence: Electronically Stored Information

by

Richard R. Orsinger
Board Certified in Family Law
& Civil Appellate Law by the
Texas Board of Legal Specialization

I. INTRODUCTION. The prevalence of computers and the growth of the Internet have greatly increased the amount of information that is captured and available to seek, review, use, and protect, in litigation. This Article raises issues that should be considered about the vast body of information known as "Electronically Stored Information" ("ESI").

II. FIVE ASPECTS OF DEALING WITH ESI. Because of the convenience and nominal cost of digital storage, and redundancy built into data processing, and the tracking features that are inherent in Internet protocols, the world is saving more data than ever before. In fact, we have reached the stage where the problem is too much information, rather than too little. When it comes to handling ESI in compliance with statutes and regulations, and to meet the demands of litigation, writers in the field divide the problems of electronic data into five categories: retaining/destroying, identifying, collecting, processing, and reviewing ESI. See generally The Electronic Discovery Reference Model <http://edrm.net>, and particularly <http://www.edrm.net/wiki/index.php/Main_Page>.

A. RETAINING/DESTROYING ESI. While some companies are required by various federal and state statutes and regulations to maintain certain information for certain periods of time, just because those time periods have been met does not necessarily mean that information can be safely destroyed. Plus, companies and individuals, whether or not they are subject to any statutory or regulatory retention requirement, must consider potential litigation when destroying data or allowing data to be destroyed.

Any time a company or person destroys recorded information, there is a risk that in subsequent litigation the opposing party will claim spoliation, and ask for discovery sanctions, fees, and costs. Nonetheless, people in the document management business say that it is permissible to destroy records pursuant to a commercially reasonable timetable that is applied as a consistent policy, with sensitivity toward information whose importance requires special treatment, and with an appreciation that the destruction of relevant information must cease when litigation can be reasonably anticipated.

1. Zubulake v. UBS Warburg, LLC. In *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D. N.Y. 2003), the U.S. District Judge Shira A. Scheindlin wrote that "anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary." The court relied upon *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72-73 (S.D. N.Y. 1991), where the court said:

> [N]o duty to preserve arises unless the party possessing the evidence has notice of its relevance. *See Danna v. New York*

> *Telephone Co.*, 752 F.Supp. 594, 616 n. 9 (S.D.N.Y.1990). Of course, a party is on notice once it has received a discovery request. Beyond that, the complaint itself may alert a party that certain information is relevant and likely to be sought in discovery. *See Computer Associates International, Inc. v. American Fundware, Inc.*, 133 F.R.D. 166, 169 (D. Colo. 1990); *Telectron, Inc. v. Overhead Door Corp.*, 116 F.R.D. 107, 127 (S.D. Fla. 1987). Finally, the obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced. *See Capellupo v. FMC Corp.*, 126 F.R.D. at 550-51 & n. 14; *Alliance to End Repression v. Rochford*, 75 F.R.D. 438, 440 (N. D. Ill.1976).

The *Turner* case in turn relied upon *Wm. T. Thompson Co. v. General Nutrition Corp*., 593 F.Supp. 1443, 1455 (C.D. Cal. 1984), where the court said:

> Sanctions may be imposed on a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information. While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

2. FRCP 37(e). In 2006, the U.S. Congress adopted what is now FRCP 37(e). Rule 37(e) provides:

> **(e) Failure to Provide Electronically Stored Information.** Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

Viewed literally, these words appear to contemplate destruction of data as necessary functions of the computer's operating system, such as the overwriting of digital information that results from random access storage of data on disk drives, and perhaps even the recycling of back-up tapes (which effectively wipes out earlier back-ups and replaces them with new ones).

Here is what the Advisory Committee note said about Rule 37(e). The Comments refer to subdivision 37(f), which now is subdivision 37(e):

> Subdivision (f) is new. It focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that attends ordinary use. Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part. Under Rule 37(f), absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.
>
> Rule 37(f) applies only to information lost due to the "routine operation of an electronic information system" -- the

ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs. The "routine operation" of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.

Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

> Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.
>
> The protection provided by Rule 37(f) applies only to sanctions "under these rules." It does not affect other sources of authority to impose sanctions or rules of professional responsibility.
>
> This rule restricts the imposition of "sanctions." It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes or alternatives for some or all of the lost information.

Some people consider Rule 37(e) to be a "safe harbor" provision that protects businesses or persons who destroy ESI pursuant to a routine record retention/destruction policy if they later find themselves in litigation. Timothy J. Carroll and Bruce A. Radke, *Federal Rules of Civil Procedure Concerning E-Discovery Impact* (2010).[1] Safety is a relative concept. The language of the Rule and the comments by the Advisory Committee do not reflect that FRCP 37(e) is a completely safe "safe harbor" when it comes to intentionally destroying data or allowing data to be lost.

[1] <http://www.busmanagement.com/article/Federal-Rules-of-Civil-Procedure-Concerning-E-Discovery-Impact>.

3. Post-FRCP 37(e) Case Law. *Zubulake* continues to be cited in cases decided after FRCP 37(e) was adopted. In W*ilson v. Thorn Energy, LLC*, 2010 WL 1712236, *2-4 (S.D. N.Y. 2010), the U.S. Magistrate Judge cited *Zubulake* when imposing sanctions for the failure of a litigant to preserve a copy of the contents of a flash drive. The Magistrate Judge rejected a Rule 37(e) safe harbor, saying: "the data on the flash drive was not overridden or erased as part of a standard protocol; rather, it was lost because the Defendants failed to make a copy." *Id.* at *3. In *Consolidated Edison Co. of New York, Inc. v. U.S.*, 90 Fed.Cl. 228, 256 (Fed. Cl. 2009), *Zubulake* was cited in connection with a spoliation claim. In *John B. v. Goetz*, 531 F.3d 448, 459 (6th Cir. 2008), *Zubulake* was cited for the proposition that "a party to civil litigation has a duty to preserve relevant information, including ESI, when that party 'has notice that the evidence is relevant to litigation or ... should have known that the evidence may be relevant to future litigation.'" There appears to be no doubt that there is a duty to preserve relevant data *at some point in time*. The point goes from the obvious (once a discovery request has been received for the information in question) to the not-so-obvious (when a person "should have known that the evidence may be relevant to future litigation"). Caution is advised.

Judge Shira A. Scheindlin, the judge who wrote the *Zubulake* opinion in 2003, revisited sanctions for mishandling ESI in 2010, in *Pension Committee of the Univ. of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F.Supp.2d 456 (S.D. N.Y. 2010). Judge Scheindlin commented: "This is a case where plaintiffs failed to timely institute written litigation holds and engaged in careless and indifferent collection efforts after the duty to preserve arose. As a result, there can be little doubt that some documents were lost or destroyed." In a 48-page opinion Judge Scheindlin methodically evaluates the behaviors of various plaintiffs who failed to retain emails prior to litigation or failed to make a thorough search for them once litigation was underway.

Judge Scheindlin wrote:

> It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation."'[O]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents.'" A plaintiff's duty is more often triggered before litigation commences, in large part because plaintiffs control the timing of litigation"

Id. at 466. The lawsuit was initiated in February of 2004. *Id.* at 473. But the judge ruled that the plaintiffs should have saved all relevant data starting by April of 2003, when the defendant's financial condition was deteriorating and several of the plaintiffs had consulted attorneys. *Id.* at 475.

The Federal Magistrate Judge's decision in *Phillip M. Adams & Assoc. v. Dell, Inc.*, 621 F. Supp. 1173 (N.D. Utah 2009), imposed spoliation sanctions based on the data retention practices of a defendant company in a patent infringement case. The defendant company had no centralized storage of computer, files or email. Individual employees were instructed to preserve emails they thought had long term value on their individual computers. *Id.* at 1181 and 1188. The Court noted that people in the computer industry were well aware of a flaw in floppy disk controllers for which, in late 1999, Toshiba paid billions of dollars in a class action suit. *Id.* at 1191. A class action suit was filed against Hewlett Packard in 1999 for the same problem, and against Sony in 2000. The claimed reverse-engineering of the plaintiff's

patented technique for correcting such floppy disk errors allegedly occurred during 2000, and no emails or source code of this engineering project was preserved. *Id.* The magistrate judge ruled that the defendant corporation should have been preserving evidence related to floppy disk controller errors in year 2000, *Id.* at 1190-91, although the patent infringement suit was not filed until 2007. *Id.* at 1190. The defendant company invoked the FRCP 37(e) "safe harbor for the routine good faith of an electronic operation system." The Court noted that the defendant company had no data back up policy. The email server overwrote old emails regardless of their importance. *Id.* at 1192. When computers were replaced, individual employees were charged with moving data from the old computer to the new one. And yet the company did store certain financial-related data in centrally accessible back-up servers, showing that the defendant company "does know how to protect data it regards as important." *Id.* at 1192. The Court said:

> The culpability in this case appears at this time to be founded in ASUS' questionable information management practices. A court-and more importantly, a litigant-is not required to simply accept whatever information management practices a party may have. A practice may be unreasonable, given responsibilities to third parties. While a party may design its information management practices to suit its business purposes, one of those business purposes must be accountability to third parties.

Id. at 1193.

3. The "Litigation Hold." A "litigation hold" is a request that the destruction of records and information be suspended because of anticipated litigation, or the onset of litigation, or especially when the client has received a letter requesting retention of ESI (typically emails) or a discovery request for production of ESI. The "litigation hold" may be issued by the opposing party's lawyer, or by the lawyer for the party whose data might be targeted.

In the *Pension Committee* case, counsel for some of the plaintiffs were taken to task for failing to issue a "litigation hold" to the clients. *Pension Committee,* 685 F. Supp.2d at 473. The court found the following failures to constitute gross negligence with regard to spoliation of evidence:

> After a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence. Thus, after the final relevant *Zubulake* opinion in July, 2004, the following failures support a finding of gross negligence, when the duty to preserve has attached: to issue a written litigation hold; to identify all of the key players and to ensure that their electronic and paper records are preserved; to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control; and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.

Id. at 471. The attorney for the plaintiffs was criticized for (i) failing to create a mechanism for collecting the preserved records so that they could be searched by someone other than the employees; (ii) failure of the attorney to provide supervision of the record review process; and (iii) failure of the attorney to supervise the collection process by reviewing, sampling, or spot-checking the collection process. *Id.* at 473.

B. IDENTIFICATION. In the context of the present discussion, "identification" is the process of differentiating information that is wanted from information that is not wanted.

1. Seeking Information. In litigation, if you are seeking information from others, there are forms and checklists you can use to help formulate your information request. Viewing these forms and these checklists critically, it becomes clear that many are derived from a paper-world perspective and merely ask for traditional information that is stored electronically rather than asking for information that is uniquely electronic. If you have hired a forensic expert, the expert can provide you with a list of items or categories of information s/he will need to review in doing her/his job. Even experts, however, may focus on the information that is traditionally required for the task, and not information that is unique to computer-based data. The key concern with seeking information in the 21st Century is 20th-century thinking: a lack of awareness of the digital information that is available, and a lack of creativity in imagining how available digital information might impact a case.

2. Providing Information. If you receive a discovery request from the opposing party, it may contain broad categories of information that are described in general terms. There may be judgment calls to be made about whether certain information falls under one category, or another, or is not included at all in the information request. It is often necessary to decide whether to produce the information in paper form, or pdf-format, or as original software files (i.e., Word, Wordperfect, Excel, etc.), and with or without metatdata. It is also necessary to identify confidential information that should be withheld from production. The confidential privilege may belong to your client, or it may belong to non-litigant third parties. In a lawsuit, the danger of evidence destruction arises, which can occur when even innocent policies regarding information retention and destruction are followed and you later learn that relevant evidence was destroyed, leading to claims of spoliation and requests for discovery sanctions.

C. COLLECTION. Data collection is an issue regardless of whether you are collecting data to assist your own client or in response to a discovery request from the opposing party. There can be client-related problems with the collection of information. This occurs, for example, where the client is unsophisticated in information management, or proves to be unreliable in locating and producing information, or where the process of gathering information requires the assistance of outsiders (like IT professionals), or where the collection of information interferes with the normal operation of a business.

If a business organization is required to locate and produce documents, it can be difficult and expensive just to find out where the information is stored. In addition to the main computer network servers, data may be stored on backup disks or tapes, individual work stations, laptops, hand-held devices, thumb drives, CDs, floppy drives, and personal computers of current and former employees. Data storage may have been outsourced to third parties.

The process of collecting ESI in response to a discovery request may become an issue in a motion for sanctions. A litigant can be sanctioned for a failure to "execute a comprehensive search for documents" or a "failure to sufficiently supervise or monitor their employees' document collection." *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F. Supp.2d 456, 477 (S.D. N.Y. 2010) (Judge Shira A. Scheindlin). In evaluating the earnestness of the search for documents, the court may consider "[w]hich files were searched, how the search was

conducted, who was asked to search, what they were told, and the extent of any supervision are all topics reasonably within the scope of the inquiry." *Id.*

D. PROCESSING. Once the needed information is identified, and has been gathered or is being gathered, it is necessary to process the information so that it can be reviewed and appropriate portions delivered to the requesting party. In a process of "culling," irrelevant documents are identified and segregated so they do not have to be reviewed by professionals who bill by the hour. De-duplication is advisable to remove repeated copies of the same document. A series of questions then arises. Will paper documents be scanned? Will scanned documents be text-searchable? Will electronic files be printed? Will documents be Bates-stamped? How will indexes be created, and who will do the indexing? Is there "legacy data" that is in old computer formats that are no longer kept current by the client?

E. REVIEW. In the old days, document review meant sitting in a room for days on end, looking at paper after paper out of box after box. Nowadays, outside vendors have developed software systems that can search ESI in a myriad of ways to pinpoint useful information. Many law offices, however, consign the review work to paralegals or associate attorneys, to visually inspect documents one-by-one. Or law firms delegate the review process to forensic experts to do page-by-page review.

The ruling in the *Pension Committee* case states that the litigant's attorney must ensure that the review process to identify relevant records should be robust, and should be subject to meaningful supervision and checked to be sure that the review process is executed according to plan. Texas courts have not endorsed these exacting standards, and it should not be forgotten that standards that are achievable by large, monied institutions who are litigating in federal district courts in Manhattan may not be fully transportable to small companies or individuals in the hinterland.

Extensive discussion of approaches to the review process are set out at The Electronic Discovery Reference Model <http://edrm.net>.

III. INTERNET PRIVACY. The computers that make up the Internet are accumulating uncountable quantities of information about everyone and everything. While much of this information has technical utility only, companies who want to sell advertising are doing nearly everything within their power to connect Internet information to particular Internet users, so that the information they have can be used in selling advertising. In the literature, the focus of the debate is on "personally identifiable information." Google, for example, takes the position that it can only associate its information with a particular IP address. Detractors argue that it is often possible to correlate the IP address with a specific individual, based on data from the content of searches, or by correlating the IP address to a subscriber to Gmail, or when the ISP connects the IP address to a specific street address that in turn can be associated with a particular person.

A. SEARCH ENGINES. The biggest collector of data is the Internet search engine Google.[2] According to a January 2010 estimate,[3] Google conducts 3 billion searches per day. The estimate credited Yahoo with 280 million searches per day, and Bing with

---

[2] Alma Whitten, *Are IP addresses personal?* <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html>.

[3] <http://searchengineland.com/by-the-numbers-twitter-vs-facebook-vs-google-buzz-36709>.

80 million searches per day. Princeton computer scientist Edward Felton called Google's storage of vast amounts of personal information "perhaps the most difficult privacy [problem] in all of human history."[4]

These Internet search services keep all the information they can about these searches.[5] To quote an October 2006 article from *Mother Jones Magazine*: "Over the years, Google has collected a staggering amount of data, and the company cheerfully admits that in nine years of operation, it has never knowingly erased a single search query."[6] The searches can be tied back to a particular Internet Protocol Address ("IP address"), which identifies the computer connected to the Internet that initiated the search.[7] While the IP address itself does not identify the person using that computer, the pattern of searches and the content of search queries can sometimes make it easy to identify the computer user.

B. BROWSER HISTORIES. A survey of members of the American Academy of Matrimonial Lawyers ("AAML") indicated that a high percentage of those lawyers used browser histories as evidence in divorce cases.[8] In most instances, an internet browser (like Internet Explorer or Mozilla Firefox) will record a history of search strings and web cites visited. The browsing history can be curtailed and erased with a little effort, but in most instances nothing is ever really erased from a hard drive by a user "delete." Plus, as noted above, the search engine providers save search data in their own archives.

C. SOCIAL NETWORKING WEBSITES. "A social networking site is an online place where a user can create a profile and build a personal network that connects him or her to other users."[9] "The share of adult internet users who have a profile on an online social network site has more than quadrupled in the past four years -- from 8% in 2005 to 35% now," according to the Pew Internet & American Life Project's December 2008 tracking survey.[10] A survey of members of the AAML reflected that "81% of AAML members cited an increase in the use of evidence from social networking websites during the past five years, while just 19% said there was no change. Facebook is the primary source of this type of evidence according to 66% of the AAML respondents, while MySpace follows with 15%, Twitter at 5%,

---

[4]Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH LAW REV. 1433, 1434 (2008).

[5] Google says: "Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser." <http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=162743> (last visited 9-27-2010).

[6] Adam L. Penenberg, *Is Google Evil?* October 10, 2006 <http://motherjones.com/politics/2006/10/google-evil>.

[7]An insightful discussion about whether an IP address is "personally identifiable information" is at <http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html>.

[8] *Married Browsers Beware: Top Divorce Lawyers Note Soaring Use of Internet and Spyware Evidence* (April 21, 2008) <http://www.aaml.org/go/about-the-academy/press/press-releases/married-browsers-beware-top-divorce-lawyers-note-soaring-use-of-internet-and-spyware-evidence>.

[9] *Social Networking Websites and Teens* (Jan. 7, 2007) <http://www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens/Data-Memo.aspx>.

[10] *Pew Internet Project Data Memo* (Jan. 14, 2009) <http://www.scribd.com/doc/10530929/PIP-Adult-Social-Networking-Data-Memo-FINAL>.

and other choices listed by 14%."[11]

IV. ELECTRONIC DISCOVERY. Pre-trial discovery of ESI is a growing issue in 21st Century litigation. For a general listing of ESI-related discovery cases, see *Federal Court Decisions Involving Electronic Discovery December 1, 2006 – July 31, 2009* (Kenneth J. Withers, Ed.),[12] and *Federal Court Decisions Involving Electronic Discovery* January 1, 2009 - May 31, 2010 (Kenneth J. Withers, Ed.).[13] Since it is much easier to request information in litigation than it is to gather and produce it, the challenge of responding to discovery requests is often greater than the challenge of making the requests. A comprehensive treatment on handling pretrial discovery of ESI is at Jerry Custis, LITIGATION MANAGEMENT HANDBOOK § 7:28, *Managing electronic discovery--Electronic discovery issues* (2009) [available on Westlaw at LTGMANHB § 7:28).[14]

A. FEDERAL DISCOVERY PROCEDURES. Federal Rule of Civil Procedure 34 deals with pre-trial discovery of documents and "electronically stored information." FRCP 45 deals with subpoenaing information, including ESI. FRCP 45(d)(1) governs "producing documents or electronically stored information" in response to a subpoena. An important concept introduced in Rule 45(d)(1)(D) is the idea that "[t]he person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost." Under FRCP 26(a)(i), a litigant who intends to use evidence, including ESI, must inform the requesting party of where the potentially relevant evidence exists, including where ESI is stored. FRCP 26(b)(2)(B) contains a "claw back" provision for confidential information accidentally produced. FRCP 26(b)(2)(C)(iii) requires the Court to limit the frequency or extent of discovery if the burden or expense outweighs its likely benefit.[15] FRCP 37 provides that "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

B. TEXAS DISCOVERY PROCEDURES. Texas Rule of Civil Procedure 196.4 deals with ESI:

> To obtain discovery of data or

---

[11] *Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers* (Feb. 10, 2010) <http://www.aaml.org/go/about-the-academy/press/press-releases/big-surge-in-social-networking-evidence-says-survey-of-nations-top-divorce-lawyers>.

[12] <http://www.fjc.gov/public/pdf.nsf/lookup/EDis0919.pdf/$file/EDis0919.pdf>.

[13] On Westlaw at CR045 ALI-ABA 1 <https://web2.westlaw.com/result/default.wl?ss=CNT&db=100059&mt=210&scxt=WL&caseserial=2019824761&tc=1&cxt=DC&sv=Full&rp=%2fFind%2fdefault.wl&ppt=SDU_119&findtype=1&rlti=1&cnt=DOC&ordoc=2019824761&serialnum=0354771406&vr=2.0&ifm=NotSet&fn=_top&service=Find&rlt=CLID_FQRLT8885172717189&tf=12&n=1&pbc=BC6E23F9&casecite=2009+WL+2957317&rs=WLW10.08>.

[14] <https://web2.westlaw.com/find/default.wl?serialnum=0304634779&ifm=NotSet&rp=%2ffind%2fdefault.wl&sv=Split&caseserial=2018546046&rs=WLW10.08&db=166688&casecite=621+F.Supp.2d+1173&findtype=1&fn=_top&mt=210&vr=2.0&pbc=BC6E23F9&ordoc=2018546046&RLT=CLID_FQRLT98663565418189&TF=756&TC=1&n=1>.

[15] In *In re eBay Seller Antitrust Litigation*, 2009 WL 361351 (N.D. Cal. 2009), a federal district judge ordered eBay to spend an estimated $300,000 to create a new data set of eBay data for the plaintiff to use in suing eBay.

information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot--through reasonable efforts--retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

The Texas Supreme Court case of *In re Weekley Homes, L.P.,* 295 S.W.3d 309 (Tex. 2009), contains several statements of note regarding ESI:

- Deleted and un-deleted e-mail messages, stored on a computer hard drive, constitute "electronic or magnetic data," within meaning of rule of procedure governing discovery requests for production of electronic or magnetic data.

- While a discovery request for production of e-mail messages may *imply* deleted e-mail messages, a party seeking production of deleted e-mail messages should expressly request them.

- The purpose of the Texas Rules of Civil Procedure specificity requirement for discovery requests seeking production of ESI is to ensure that such requests are clearly understood and disputes are avoided.

- Prior to sending requests for production of ESI, parties should share relevant information concerning electronic systems and storage methods so that agreements regarding protocols may be reached, or failing that, so that trial courts have the information needed to craft discovery orders that are not unduly intrusive or overly burdensome.

- The trial court could treat a "motion for limited access to [homebuilder's] computers" as a motion to compel production of electronic or magnetic data.

- If the trial court determines that requested ESI is not reasonably available, the court may nevertheless order production upon a showing by the requesting party that the benefits of production outweigh the burdens.

- In determining how ESI should be searched and then produced, courts are discouraged from giving litigants direct access to another party's electronic storage devices; courts should be extremely cautious to guard against undue intrusion.

A court-order allowing discovery of a non-resident defendant's computer hard drive was struck down in *In re Stern*, 2010 WL 3365856 (Tex. App.–Houston [1st Dist.] 2010) (orig. pet.). The trial court ordered this electronic discovery while the defendant's special

appearance was still pending. Because the discovery allowed exceeded jurisdictional issues, it was overbroad. It was stricken as a prohibited "fishing expedition." *Id.* at *13. The trial court appointed Houston attorney Craig Ball as a special master to review the defendant's entire hard drive. The court of appeals criticized the order appointing Ball: "Because the order does not supply search terms, Ball was given virtually free reign to plumb Stern's hard drive." *Id.* at *16. The appellate court went on to say:

> Granting a special master carte blanche authorization to sort through Stern's computer hard drive clearly violated the longstanding prohibition against impermissible "fishing expeditions."

Id. at *16.

C. COMMON ESI DISCOVERY-RELATED ISSUES. Texas attorney Craig Ball, who has often served as a court-appointed discovery master, has explained the principal issues he sees in electronic discovery disputes: (i) what e-mail system does the party use; (ii) what is the party's e-mail retention policy and practice; (iii) what are the party's backup practices; (iv) what devices and applications do the key players use that might implicate relevant ESI; (v) what forms of ESI does each party seek, and what forms will each party furnish; (vi) what data are at greatest risk of alteration or destruction; (vii) how does each party plan to filter, search and redact ESI; (viii) is ESI that is "gone" really gone?[16]

D. SUBPOENAING ESI FROM NON-LITIGANTS. As noted above, divorce lawyers are aware that non-litigants may have ESI that would be helpful in litigation. Lawyers are therefore subpoening ESI from non-parties, under the discovery-related Federal Rules of Civil Procedure and under the discovery rules of various states. Texas Rule of Civil Procedure 205.1 permits a party to issue a subpoena to a non-party to produce documents and information. The party seeking the discovery must give ten days' notice to other parties of the intent to issue the discovery subpoena.

Three federal courts have ruled that a person has standing under the Federal Rules of Civil Procedure to seek to quash a subpoena that would require a business to produce ESI that is protected by the Stored Communications Act, 18 U.S.C. § 2701(a)(1). *See Crispin v. Christian Audigier, Inc.*, 2010 WL 2293238, *4 (C.D. Cal. 2010) (quashing subpoenas for private information stored at Facebook, My Space, and other social networking sites); *J.T. Shannon Lumber Co., Inc. v. Gilco Limber, Inc.*, 2008 WL 3833216 (N.D. Miss. 2008) (quashing subpoena on Microsoft, Google, and Yahoo); *Hone v. Presidente U.S.A. Inc.*, 2008 U.S. Dist. LEXIS 55722, *4 (N.D. Cal. 2008) (quashing subpoena on Yahoo). TRCP 205.2. TRCP 192.6 permits the non-party, and "any other person affected by the discovery request," to move for a protective order. Rule 192.6 is essentially a "standing" rule, indicating that motions for protective orders can be filed any anyone "affected" by the discovery request.

The Federal Stored Communication Act provides privacy for communications stored with many third parties. Several courts have recognized a right to privacy for anonymous postings on web sites. *See* Clay Calvert, Kayla Gutierrez, Karla D. Kennedy, Kara Carnley Murrhee, *David Doe v. Goliath, Inc.: Judicial Ferment in 2009 for Business Plaintiffs Seeking the Identities of Anonymous Online Speakers*, 43 J. MARSHALL L. REV. 1 (2009).

---

[16] Craig Ball, *E-Discovery: A Special Master's Perspective* <http://www.craigball.com/EDD_SM_PERSP.pdf>.

In *Solarbridge Technologies, Inc. v. Doe*, 2010 WL 3419189 (N.D. Cal. 2010), the United States Magistrate Judge permitted a plaintiff to subpoena Yahoo! and Google to get information permitting the plaintiff to identify the source of an anonymous email that contained the plaintiff's trade secrets, etc.

It should be noted that in *In re Napster Copyright Litigation*, 462 F.Supp.2d 1060, 1068 (N.D. Cal. 2006), the federal district judge mentions in passing a non-party's duty to preserve information that has been subpoenaed.

Courts have litigated the question of when the court should shift the cost to a non-party of complying with subpoenas related to litigation in which the third party is not involved. The federal district judge in *Tessera, Inc. v. Micron Technology, Inc.*, 2006 WL 733498 (N.D. Cal. 2006), enumerated eight factors to consider: "(1) the scope of the request; (2) the invasiveness of the request; (3) the need to separate privileged material; (4) the non-party's financial interest in the litigation; (5) whether the party seeking production of documents ultimately prevails; (6) the relative resources of the party and the non-party; (7) the reasonableness of the costs sought; and, (8) the public importance of the litigation."[17]

E. SOURCES OF PRIVILEGE OR PRIVACY FOR ESI.

1. Federal Statutes. In *U.S. v. Olmstead*, 277 U.S. 438 (1928), the Supreme Court held that the Fourth Amendment protection against search and seizure did not apply to a wiretap installed without physical intrusion into a home or office. Congress thereafter adopted the Communications Act of 1934, which prohibited intercepting communications without the consent of the sender. 47 U.S.C. § 605. In *Katz v. U.S.*, 389 U.S. 347 (1967) ("bug" on exterior of telephone booth), the Supreme Court revised its analysis, and held that the Fourth Amendment applied to areas in which the person had a reasonable expectation of privacy. In 1968, Congress enacted the Federal Wiretap Act (FWA), which prohibited the interception of wire communications (i.e., telephone) and oral communications. In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), which extended the wiretap prohibition to mobile and cellular telephones and to electronic communications (i.e., email). However, capturing the broadcast portion of portable house telephones was not prohibited. In 1994, the ECPA was amended to protect the broadcast portion of portable telephones. After the disaster on September 11, 2001, Congress enacted the USA Patriot Act, which revised the Federal Wiretap Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act. See Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 LAW LIBR. J. 601 (2001).

The Fifth Circuit Court of Appeals once described the Federal Wiretap Act as being "famous (if not infamous) for its lack of clarity." *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994).

The Federal Stored Communication Act ("SCA") was adopted in 1986. The SCA distinguishes between an "electronic communication service" (ECS), which is a service that enables one to send or receive wire or electronic communications," and a "remote computing service" (RCS), which is a computer storage or processing service that uses an electronic communications system.

[17] *The Sedona Conference Commentary on Non-Party Production and Rule 45 Subpoenas* (Blakely, et al., editors 2008) <http://www.thesedonaconference.org/dltForm?did=Rule_45_Subpoenas>.

The prohibition against disclosure contained in the SCA is:

> § 2702. Voluntary disclosure of customer communications or records
>
> (a) Prohibitions.--Except as provided in subsection (b) or (c)--
>
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
>
> (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

In the case of *J.T. Shannon Lumber Co., Inc. v. Gilco Limber, Inc.*, 2008 WL 3833216, *1 (N.D. Miss. 2008), the court ruled that stored emails could not be subpoenaed from the email service provider:

> The Stored Communications Act of 1986 prohibits the unauthorized disclosure of stored electronic communication and customer account information unless an exception applies. 18 U.S.C. § § 2701-03 (2006). The statute prohibits a person or entity that provides an electronic communication service to the public from knowingly divulging the contents of any communication that is carried or maintained on the system. 18 U.S.C. § 2702(a). The exceptions listed in the statute do not include a civil subpoena issued under Rule 45. 18 U.S.C. § 2702(b); *In re Subpoena Duces Tecum to AOL*, 550 F.Supp.2d 606, 611 (E.D. Va. 2008); *See also*[18] *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004); *F.T.C. v. Netscape Communications Corp.*, 196 F.R.D 559 (N.D. Cal. 2000). Further, an electronic communication service provider is also prohibited from divulging customer records unless an exception applies. 18 U.S.C. § 2702(c). Again, there is no exception to this statutory prohibition against disclosure pursuant to a civil discovery subpoena.

[18] Timothy G. Ackermann, *Consent and Discovery under the Stored Communications Act*, 56-DEC FED. LAW. 42 (2009).

See Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008) (declining to permit a litigant to subpoena stored text messages but allowing the messages to be pursued through a request for production of documents directed to a party); *In re Subpoena Duces tecum to AOL, LLC*, 550 F.Supp.2d 606, 611 (E.D. Va. 2008) (quashing subpoena of email records from AOL); *O'Grady v. Superior Court*, 39 Cal.App.4th 1423, 44 Cal.Rptr.3d 72 (Cal. App. 2006) (SCA renders unenforceable subpoenas seeking to compel email service provider to disclose the contents of emails stored on their facilities).

In *Crispin v. Christian Audigier, Inc.*, 2010 WL 2293238, *11 (C.D. Cal. 2010), the court held that the social networking sites Facebook and My Space were electronic communication services and that *private* messaging information was protected by the SCA and could not be produced in response to a civil subpoena.

Viacom International Inc. v. Youtube Inc., 253 F.R.D. 256, 264 (S.D. N.Y. 2008), held that the ECPA prohibited discovery in a civil case of "private videos" stored on You Tube, in the area where videos are not made available to the public.

While the communication content stored by ECS and RCS is protected from disclosure, it is possible that non-communication data may be discoverable, such as the number and times of communications, total hours logged on to the system, etc.

2. Privileges Under Texas Law. Article 5 of the Texas Rules of Evidence set out evidentiary privileges that cut off discovery in certain areas (lawyer-client, doctor-patient, psychotherapist-patient, etc.). There are other privileges in state and federal law. TRCP 192.5 makes attorney work product non-discoverable.

V. METADATA. "Metadata" is data about data, or more specifically, "information describing the history, tracking, or management of an electronic document." *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 646 (Dist. Ct. Kan. 2005) (discussing the law concerning discovery of electronic documents and associated metadata in litigation). Metadata was described this way eDISCOVERY & DIGITAL EVIDENCE:[19]

> It refers to hidden data that usually can only be seen when a digital document is viewed in its native format using the program that originally produced the document. Often even the user of a program may not know it is there unless he or she knows how to find it. When a document is created by a particular program (such as MS Word) there is hidden information (metadata) about that document that can only be viewed if the document is opened by that program. Examples include the modification history or the date and time when the document was first created or edited and by whom.

An authoritative definition of "metadata" is contained in the Sedona Conference's Glossary p. 34 (2010):[20]

---

[19] Jay E. Grenig and William C. Gleisner, III with general consultants Troy Larson and John L. Carroll, eDISCOVERY & DIGITAL EVIDENCE § 1:5 [available on Westlaw as EDISCOVERY § 1:5] <https://web2.westlaw.com/result/previewcontroller.aspx?TF=756&TC=4&serialnum=0307455661&rs=WLW10.08&ifm=NotSet&casecite=187+P.3d+822&fn=_top&sv=Split&pbc=3F1E7F52&ordoc=2016562293&findtype=1&caseserial=2016562293&db=190121&vr=2.0&rp=%2ffind%2fdefault.wl&mt=210&RP=/find/default.wl&bLinkViewer=true>.

[20] <http://www.thesedonaconference.org/dltForm?did=glossary2010.pdf>.

> Metadata: Data typically stored electronically that describes characteristics of ESI, found in different places in different forms. Can be supplied by applications, users or the file system. Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted. Can be altered intentionally or inadvertently. Certain metadata can be extracted when native files are processed for litigation. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed to paper or electronic image. See also Application Metadata, Document Metadata, Email Metadata, Embedded Metadata, File System Metadata, User-Added Metadata and Vendor-Added Metadata. For a more thorough discussion, see The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (Second Edition).

Wikipedia has a detailed entry on metadata. The Wikipedia entry describes metadata as "a concept that applies mainly that applies mainly to electronically archived or presented data and is used to describe the a) definition, b) structure and c) administration of data files with all contents in context to ease the use of the captured and archived data for further use." *Id.* at 1. The entry says: "Metadata is defined as data providing information about one or more other pieces of data, such as:

> - means of creation of the data
> - purpose of the data,
> - time and date of creation,
> - creator or author of data,
> - placement on a network (electronic form) where the data was created,
> - what standards used, etc."

Id. at 2.

Here is what the *Sedona Conference Commentary on ESI Evidence & Admissibility*[21] says about metadata:

> Metadata can be another useful checkpoint for determining authenticity. For example, email messages generally contain a substantial amount of metadata information, including a unique message ID as well as information on the unique Internet locations (IP addresses) where the message originated and was handled along the way to its destination.
>
> Similarly, operating system metadata can be a useful tool. Most operating systems maintain information about individual files – the dates that a file was created, last modified and last accessed. For example, in a case where an individual claims that it did not create a document until July 1, but the system metadata shows that the document was created on May 1, this data may be helpful.
>
> However, metadata can be unreliable and is usually subject to manipulation and non-obvious deletion. A moderately sophisticated user may be able to manipulate system dates, and although traces of this manipulation may be left behind, detecting such traces can be extremely difficult and expensive, or simply impossible. Worse, use of files after the fact, such as an investigator opening a file for review, can modify metadata and make it useless or misleading for authenticity purposes. Accordingly, careful attention should be

[21] <http://www.thesedonaconference.org/dltForm?did=ESI_Commentary_0308.pdf>.

> paid to the methods used to authenticate metadata.

Id. at 13.

The court in *O'Neill v. City of Shoreline*, 187 P.3d 822 (Wash. App. 2008), held that, where an email was read out loud by the deputy-mayor of a city during a public meeting, both the email and the metadata associated with the email constituted a public record under Washington State's Public Records Act.

As noted above, metadata can play an important role in authenticating ESI.

VI. AUTHENTICATION OF DIGITAL INFORMATION. Litigation in the 21st Century will require lawyers and courts to determine acceptable ways to authenticate digital information, and to puzzle through the application of the hearsay rule to ESI.

A. AUTHENTICATION OF EVIDENCE (GENERALLY). No evidence is admissible unless it has been authenticated. This authentication requirement is met by evidence sufficient to support a finding that the matter in question is what its proponent claims. TRE 901. Typical forms of authentication are by testimony of a witness with knowledge, lay opinion on genuiness of handwriting, identification of a voice by someone who has heard the speaker speak, etc. TRE 901(b). Digital information is notably absent from the list of examples.

Some documents are self-authenticating: domestic government documents under seal, or if not under seal then attested to under seal by a public officer that the signer had the capacity and the signature is genuine; foreign public documents which are attested and certified as genuine; certified copies of public records; official publications; newspapers and periodicals; trade inscriptions showing ownership, control or origin; acknowledged documents; commercial paper; and business records accompanied by "business records affidavit." TRE 902 ("Self-Authentication").

TRCP 193.7 provides that documents produced by a party in response to written discovery are automatically authenticated against the producing party for pretrial purposes, unless the producing party makes an objection with 10 days of notice that the document will be used.

Authentication requires only a prima facie showing that the evidence is what it is claimed to be. As stated in *United States v. Gotchman*, 547 F.2d 778, 784 (3rd Cir. 1976):

> What appellant overlooks is that the showing of authenticity is not on a par with more technical evidentiary rules, such as hearsay exceptions, governing admissibility. Rather, there need be only a prima facie showing, to the court, of authenticity, not a full argument on admissibility. Once a prima facie case is made, the evidence goes to the jury and it is the jury who will ultimately determine the authenticity of the evidence, not the court. The only requirement is that there has been substantial evidence from which they could infer that the document was authentic . . . .

Accord, U.S. v. Pantic, 308 Fed. Appx. 731, 733 (4th Cir. 2009) ("The district court plays a gate-keeping role in assessing whether the proponent has established a suitable foundation from which the jury could reasonably find that the evidence is authentic. . . . The proponent's burden of authentication is slight–only a prima facie showing is required."); *U.S. v. Jardina*, 747 F.2d 945, 951 (5th Cir. 1984) ("When confronted with evidence of questionable origin, the court should admit the evidence if a prima facie showing of authenticity is made"); *Alexander Dawson, Inc. v. NLRB*, 586 F.2d 1300, 1302

(9th Cir. 1978) (per curiam) ("The issue for the trial judge under Rule 901 is whether there is prima facie evidence, circumstantial or direct, that the document is what it is purported to be. If so, the document is admissible in evidence."); *State v. Bell*, 2009 WL 1395857, *3 (Ohio App. 2009) ("the 'sufficient to support a finding' standard is not rigorous, and the threshold of admissibility articulated in it is low"). Some courts have said that the threshold for authenticating evidence is low. *United States v. Reilly*, 33 F.3d 1396, 1404 (3rd Cir. 1994). Stated differently: evidence is admissible if there is a sufficient showing that the proposed evidence *could be* what it is claimed to be; the jury decides whether or not, in actuality, the evidence *is* what it is claimed to be. For the court, the burden of persuasion is prima facie proof. For the jury, the burden of persuasion is a preponderance, clear and convincing, or beyond a reasonable doubt, as the case may be. In support of a motion for summary judgment, the authentication must be conclusive. In opposition to a motion for summary judgment, the doubt about authenticity must be sufficient that reasonable minds might differ on the question of whether the evidence is what it is claimed to be.

It should be noted that merely authenticating a document does not guarantee its admissibility. *See Wright v. Lewis*, 777 S.W.2d 520, 524 (Tex. App.--Corpus Christi 1989, writ denied) (despite the fact that a letter was authenticated, the letter was not admissible because of the hearsay rule).

B. AUTHENTICATING COMPUTER-RELATED EVIDENCE. In the early days of computers, one appellate court expressed the view that proof regarding the reliability of the computer equipment in question was a necessary prerequisite to the admission of business records generated by that computer. *See Railroad Comm'n v. So. Pacific Co.*, 468 S.W.2d 125, 129 (Tex. Civ. App.--Austin 1971, writ ref'd n.r.e.). Subsequent Texas decisions abandoned the requirement for proving up the validity of the computing process as a predicate for business records. Courts now agree that computerized business records can be authenticated in the same manner as hand-written business records. *See Voss v. Southwestern Bell Tel. Co.*, 610 S.W.2d 537, 538 (Tex. Civ. App.--Houston [1st Dist.] 1980, writ ref'd n.r.e.) (computer records are admissible if requirements for business records are met). *Accord, Longoria v. Greyhound Bus Lines, Inc.*, 699 S.W.2d 298, 302 (Tex. App.--San Antonio 1985, no writ) (computerized business records may be authenticated in the same manner as other business records, and it is not necessary to show that the machine operated properly or that the operator knew what he was doing; at its inception, however, the data itself must be based upon personal knowledge); *Hutchinson v. State*, 642 S.W.2d 537, 538 (Tex. App.--Waco 1982, no writ) (criminal case) (adopting same rule established in civil cases regarding admissibility of computer-generated records). *See Hill v. State*, 644 S.W.2d 849, 853 (Tex. App.--Amarillo 1982, no writ) (telephone company records admissible as business records, even though the information was initially recorded automatically on magnetic tape, rather than by a human being).

At the present time, the focus is less on the technicalities of the computer data and is more on disputes over whether ESI such as emails, chat room or blog postings, or World Wide Web pages, can properly be attributed to a particular person. In cases someone asserts "I didn't send that email message," even though the email was connected to that person's account or was sent using his or her computer. Any email user knows that it is possible to "spoof," meaning to alter an email header to make it look like it is from a particular sender when it is not. In *Govan Brown & Assoc., Ltd. v. Does 1 and 2*, 2010 WL 3076295 (N.D. Cal. 2010), the Court

explained how to identify the sources of a G-mail email: "once it obtains the IP addresses for the two electronic mail accounts from Google, that information, in turn, will allow it to determine the Internet Service Providers for the account holders. [Plaintiff] further explains that once the Internet Service Providers are identified, it will be able to initiate separate proceedings to compel disclosure of the identities of the two email account holders." *Id.* at * 1. Such discovery was allowed in *Solar Bridge Technologies, Inc. V. John Doe*, 2010 WL 3419189 (W.D. Cal. 2010).

See People v. Johnson, 875 N.E.2d 1256, 1259-60 (Ill. App. 2007) ("In the case of computer-generated records, a proper foundation additionally requires a showing that: standard equipment was used; the particular computer generates accurate records when used appropriately; the computer was used appropriately; and the sources of the information, the method of recording utilized, and the time of preparation indicate that the record is trustworthy and should be admitted into evidence").

In *U.S. v. Whitaker*, 127 F.3d 595, 601-02 (7th Cir. 1997), *cert. denied*, 522 U.S. 1137 (1998), the court rejected an attack on the authenticity of computer records obtained from a third party's computer that implicated the defendant in criminal activity, even though no government witness was able to vouch for anything beyond the fact that the obtained the information from the third party's computer.

Paul F. Rothstein, FED. RULES OF EVIDENCE (3d ed.), Rule 901 [on Westlaw at FEDRLSEV R 901], lists the following cases and authorities relating to "Computer-Generated Material, E-mails, Web-Postings, and Related Material":

• *U.S. v. Jackson*, 208 F.3d 633, 53 Fed. R. Evid. Serv. 1030 (7th Cir. 2000) (authentication required to be sure material in website was actually put there by group whose website it was, rather than someone else; web posting offered for its truth is hearsay; not business record of internet service provider; also doesn't meet trustworthiness requirement).

• *ACTONet, Ltd. v. Allou Health & Beauty Care*, 219 F.3d 836 (8th Cir. 2000) (HTML codes authenticated by similar foundation to authentication of photographs).

• *U.S. v. Tank*, 200 F.3d 627, 53 FED. R. EVID. SERV. 830 (9th Cir. 2000) (identification of who made chat room posting on Internet).

• *U.S. v. Simpson*, 152 F.3d 1241, 49 FED. R. EVID. SERV. 1631 (10th Cir. 1998) (authentication under Rule 901(a) of website data).

• *U.S. v. Siddiqui*, 235 F.3d 1318, 55 FED. R. EVID. SERV. 301 (11th Cir. 2000) (e-mail can be authenticated under 901(b)(4) by circumstantial features).

• *Superhighway Consulting, Inc. v. Techwave, Inc.*, 1999 WL 1044870 (N.D. Ill. 1999) (e-mail produced from a party's files that purports on its face to have been sent by the party can be authenticated by these circumstances).

• *Van Westrienen v. Americontinental Collection Corp.*, 94 F. Supp. 2d 1087, 54 Fed. R. Evid. Serv. 511 (D. Or. 2000) (the defendants' websites containing misleading information about debt collections were admissible to show punitive damages because the plaintiff had viewed its contents and submitted an affidavit detailing what he viewed, although authenticity appears not to have otherwise been questioned).

• *Richard Howard, Inc. v. Hogg*, 1996 WL 689231 (Ohio Ct. App. 3d Dist. Putnam County 1996) (under state equivalent of 901(b)(1), witness who was neither recipient nor sender of e-mail who offered no other details as to how he knew this e-mail was sent between these particular parties could not authenticate the e-mail nor did anyone offer

any other method of authentication).

• *U.S. v. De Georgia*, 420 F.2d 889 (9th Cir. 1969) (absence of record of particular transaction in company computer allowed to prove it did not occur; discusses foundation needed and the access that must be given to the other side).

• *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774, 53 Fed. R. Evid. Serv. 1 (S.D. Tex. 1999) (internet information is "one large catalyst for rumor, innuendo, and misinformation" and therefore inherently untrustworthy; furthermore, there is no way to overcome this presumption of untrustworthiness).

• Cobauth, *Bloom v. Commonwealth: Identifying the Face Behind the Instant Message*, 8 RICH. J.L. & TECH. 17 (2002).

• Joseph, *Internet and E-Mail Evidence*, 13 PRAC. LITIGATOR 45 (2002).

• Mason, *Electronic Signatures Evidence: The Evidential Issues Relating to Electronic Signatures, Part I*, 18 COMPUTER L. & SEC. REP. 175 (2002).

• Schultz & Keena, *Navigating the Perils of Discovery in the E-Information Age*, 56 WASH. ST. B. NEWS 20 (2002).

• Thompson, *The Paper Trail has Gone Digital: Discovery in the Age of Electronic Information*, 71 J. KAN. B.A. 16 (2002).

• Zimmerman, *Evidence in the Digital Age*, 76 Law Inst.J. 77 (2002); Raysman & Brown, Electronic Signatures, 214 N.Y. L.R. 3 (1995).

• Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records under the Federal Rules of Evidence*, 80 NW. U. L. REV. 956 (1986).

• Long, *Discovery and Use of Computerized Information: Examination of Current Approaches*, 13 PEPP. L. REV. 405 (1986).

• Younger, *Computers and the Law of Evidence*, 1 N.Y.L.J., (1975).

• Abelle, *Evidentiary Problems Relevant to Checks and Computers*, 5 RUTGERS J. OF COMPUTERS AND THE LAW 323 (1976).

• Lautsch, *Digest of State Law Relating to Computers*, 17 JURIMETRICS J. 39 (1976).

• See generally, the periodical, Law & Computer Technology.

Hon James Carr and Patricia L. Bellia, 2 LAW OF ELECTRONIC SURVEILLANCE § 7:59, *Basic Elements–Authenticity and Accuracy–Computer Data* [on Westlaw at ELECTSURV § 7:59] give the following cases regarding the admission of computer-based information [the following case-related information is quoted or taken from the text, footnotes 10-16]:

• admitting e-mails: *U.S. v. Gagliardi*, 506 F.3d 140, 151 (2nd Cir. 2007); *U.S. v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000); *U.S. v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006); *Bobo v. State*, 285 S.W.3d 270, 274 (Ark. App. 2008); *Simon v. State*, 632 S.E.2d 723 (Ga. App. 2006); *People v. Downin*, 828 N.E.2d 341, 350–51 (Ill. App. 2005); *Dickens v. State*, 927 A.2d 32, 36-38 (Md. App. 2007); *Kearley v. State*, 843 So. 2d 66 (Miss. App. 2002); *State v. Taylor*, 632 S.E.2d 218, 230-31 (N.C. App. 2006); *State v. Bell*, 882 N.E.2d 502 (Ohio App. 2008), *judgment aff'd*, 2009 WL 1395857 (Ohio App. 2009), appeal not allowed, 914 N.E.2d 1064 (2009); *Varkonyi v. State*, 276 S.W.3d 27, 35 (Tex. App.--El Paso 2008, pet. denied); *Shea v. State*, 167 S.W.3d 98, 104–05 (Tex. App. Waco 2005, pet. denied); *Massimo v. State*, 144 S.W.3d 210, 215-17 (Tex. App. --Fort Worth 2004, no pet.).

• admitting e-mails copied verbatim from a cell phone: *U.S. v. Culberson*, 2007 WL 1266131 (E.D. Mich. 2007) (admission allowed even though the original electronic version had been purged automatically by the service provider).

• admitting instant messages: *U.S. v. Gagliardi*, 506 F.3d 140, 151 (2nd Cir. 2007); *Hammontree v. State*, 642 S.E.2d 412, 415 (Ga. App. 2007); *People v. Clevenstine*, 68

A.D.3d 1448, 891 N.Y.S.2d 511, 515 (3d Dep't 2009), *leave to appeal denied*, 14 N.Y.3d 799, 899 N.Y.S.2d 133, 925 N.E.2d 937 (2010); *People v. Pierre*, 41 A.D.3d 289, 838 N.Y.S.2d 546, 548–49 (1st Dep't 2007); *In re F.P.*, 878 A.2d 91, 93-95 (Pa. App. 2005).

• admitting chat room communications: *U.S. v. Tank*, 200 F.3d 627, 631–32 (9th Cir. 2000); *U.S. v. Simpson*, 152 F.3d 1241, 1249 (10th Cir. 1998); *Ford v. State*, 617 S.E.2d 262, 265–266 (Ga. App. 2005); *State v. Webster*, 955 A.2d 240, 244 (Me. 2008); *State v. Bell*, 882 N.E.2d 502 (Ohio App. 2008); *U.S. v. Barlow*, 568 F.3d 215, 220 (5th Cir. 2009) (logs).

• admitting text messages: *State v. Damper*, 225 P.3d 1148, 1152-53 (Ariz. App. 2010); *Dickens v. State*, 927 A.2d 32, 36–37 (Md. App. 2007); *State v. Thompson*, 777 N.W.2d 617, 624-25 (N.D. 2010) (dictum).

• admitting copies of digital images: *Midkiff v. Com.*, 54 Va. App. 323, 678 S.E.2d 287, 294 (2009), *judgment aff'd*, 2010 WL 2305819 (Va. 2010).

• admitting records relating to use of the computer: *People v. Hawkins*, 98 Cal. App. 4th 1428, 99 Cal. App. 4th 1333a, 121 Cal. Rptr. 2d 627, 643 (Cal. App. 2002), *as modified on denial of reh'g*, (July 2, 2002), *review denied*, (Aug. 28, 2002), *cert. denied*, 123 S. Ct. 1256, 154 L. Ed. 2d 1021 (U.S. 2003) (record of when computer was accessed).

• admitting data obtained by mirror imaging a hard drive: *Bone v. State*, 771 N.E.2d 710, 716 (Ind. App. 2002); State v. Cook, 777 N.E.2d 882 (Ohio App. 2002).

See also 71 AM. JUR. TRIALS §111, *Computer Technology in Civil Litigation* [on Westlaw at 71 AMJUR TRIALS § 111].

See also Monique C.M. Leahy, *Civil Pretrial Involving Text Messaging Evidence*, 115 Am. Jur. Proof of Facts 3d 1 (2010).[22]

A recent case is *State v. Craycraft*, 2010 WL 610601 (Ohio App. 2010), where a criminal defendant claimed that the state had not proven that he was the person who participated by computer in a series of instant message (IM) exchanges on AOL. The IMs were made using the defendant's girlfriend's AOL screen name. A third-party witness involved in the IM exchanges copied and pasted them into an email that he sent to himself, then printed it. The appellate court ruled that extrinsic evidence, coupled with the content of the IMs, sufficed to warrant admission of the IMs into evidence. The appellate court discussed what it called the "distinctive characteristics" method of authentication where "a speaker in a conversation may be identified because only he could utter the speech under the circumstance." *Id*. at *7. Stated differently, authentication can be achieved by showing from what is said or the way something is said that a fact finder could believe that the person claimed to have sent the message did in fact send the message.

C. BEST EVIDENCE RULE ISSUES. TRE 1001(3) provides that "[i]f data are stored in a computer or similar device, any print-out or other output readable by sight, shown to reflect the data accurately, is an 'original'." In *Robinson v. State*, No. B14-91-00458-CR (Tex. App.--Houston [14th Dist.] 1992, pet. ref'd) (not for publication) [1992 WL 133831], the Court held that it was

---

[22] <https://web2.westlaw.com/find/default.wl?serialnum=0354974574&ifm=NotSet&rp=%2ffind%2fdefault.wl&sv=Full&caseserial=0348595640&rs=WLW10.08&db=119405&casecite=56-DEC+FEDRLAW+42&findtype=1&fn=_top&mt=210&vr=2.0&pbc=BC6E23F9&ordoc=0348595640&RLT=CLID_FQRLT44663195316189&TF=756&TC=1&n=1>.

proper to permit a witness to testify to the results of a computer search without qualifying as an expert or presenting computer printouts. In this case, the witness said that a computer search on the bank's computer confirmed that an account number on a suspicious check was fictitious. According to the Court, the best evidence rule was not implicated because the witness was merely explaining the process he went through to determine whether an account number was a valid one with his bank. The Court also said that the best evidence rule did not apply because the evidence was offered to show the non-existence of a bank account. The case raises an interesting question. The best evidence rule objection would go to the computer data reflecting the results of the search. Can the witness properly testify to what the computer search indicated, without introducing into evidence a printout of the results, or is such testimony tantamount to oral testimony as to the contents of a writing? Arguably TRE 1001(3)'s provision, that the best evidence rule is met by a print-out or "other output readable by sight," applies to print-out brought to court or output readable by sight in the courtroom.

D. HEARSAY. Hearsay is defined as a statement of a person. TRE 801(a). A machine is not a person, and therefore computer output is not inherently hearsay. *Stevenson v. State*, 920 S.W.2d 342, 343 (Tex. App.--Dallas 1996, no pet.). However, a computer may issue information that contains hearsay. In dealing with computerized records, it is important to distinguish human communications stored on a computer, or human communications processed by a computer, from computer-generated information that reflects the internal operation of the computer. For example, in *Burleson v. State*, 802 S.W.2d 429 (Tex. App.--Fort Worth 1991, pet. ref'd), a prosecution for harmful access to computer, the court held that information displayed by computer, as to how many payroll records were missing, was not hearsay, because it was not an out-of-court statement made by a person. Even if it were, said the court, the computer operator, who testified based on what he saw on the computer display, qualified as expert who could rely on the computer's display, even if the display's results were not admissible. The court observed, however, that the information reflected on the computer display was "generated by the computer itself as part of the computer's internal system designed to monitor and describe the status of the system." *Id.* at 439. The court cited two out-of-state cases. In *People v. Holowko*, 109 Ill.2d 187, 93 Ill.Dec. 344, 486 N.E.2d 877, 878-79 (1985), the Illinois Supreme Court held that computerized printouts of phone traces were not hearsay because such printouts did not rely on the assistance, observations, or reports of a human declarant. The print-out was "merely the tangible result of the computer's internal operations." In *State v. Armstead*, 432 So.2d 837, 839-41 (La. 1983), the Louisiana Supreme Court held that computerized records of phone traces were not hearsay, in that they were computer-generated rather than computer-stored declarations. *Burleson v. State*, 802 S.W.2d at 439 n. 2.

In *May v. State*, 784 S.W.2d 494, 497 (Tex. App.--Dallas 1990, pet. ref'd), the appellate court surprisingly held that numbers viewed on an intoxilyzer's computer screen were hearsay. *May* in turn relied upon *Vanderbilt v. State*, 629 S.W.2d 709, 723-24 (Tex. Crim. App. 1981), which held that it was improper for the state's firearm witness, not testifying as an expert, to relate that a computer search of an FBI database rendered a print-out of a list of weapons that could generate the ballistic markings on the bullet in question, and that the gun in question was on that list. The Court of Criminal Appeals cited to an earlier case where it had held it to be error for a witness to repeat in front of the jury information obtained from a computer database. *See*

Vanderbilt, 629 S.W.2d at 723. The conclusion reached in *May* was criticized in Schlueter, *Hearsay--When Machines Talk*, 54 TEX. B.J. 1135 (Oct. 1990). It is apparent that in *May* the Dallas Court of Appeals did not distinguish testimonial information contained in a computer information file from computer-generated calculations based on a scientific and mathematical algorithm, with no component of human communication. This error was rectified in *Stevenson v. State*, 920 S.W.2d 342 (Tex. App.--Dallas 1996, no pet.), which said: "We overrule *May* only as to the language that refers to the intoxilyzer result, itself, as hearsay." *Id.* at 344. To recap: If the input is hearsay, then the output is hearsay. If the hearsay input meets an exception to the hearsay rule, then the output should meet the same exception.

In *State v. Bell*, 2009 WL 1395857, *5 (Ohio App. 2009), the court held that printouts of on-line conversations on MySpace are not business records as they are not "records of [the] regularly conducted activity" of the owner of MySpace.

E. PROCESS OR SYSTEM. If an attack is to be levied on computer-generated information, as opposed to computer-stored human communications, the attack could be an attack on authenticity under TRE 901(b)(9), relating to a process or system, for failure to show that a process or system that was used to produce the result produces an accurate result. In the *Holowko* case referred to above, the Illinois Supreme Court noted that judicial notice of the reliability of computer science might be appropriate in certain situations. The Louisiana Supreme Court, in *Armstead*, also referred to above, likened the computer-generated information to demonstrative evidence of a scientific test or experiment.

When a computer program takes data and processes it to reach a result, there can be questions about the validity of the computer process. In many instances, the calculations or processing performed by the computer program will require proof of reliability. The reliability of the output of standardized computing devices, such as a hand-held calculator, are not suspect and should be easy to authenticate. In proprietary software that makes calculations or generates charts or graphs based on non-standardized programming, the validity of the process could be in issue. For example, in an electronic spreadsheet an issue can arise about the formulas that were entered into the spreadsheet. In specially-designed software, the validity of assumptions or calculations embedded in the computer program can be a concern. In such situations, the court has the power to require that the underlying code be made available in discovery so that the coding of the program can be checked and the program can be tested. However, some courts will protect the proprietary interest of the litigant or the forensic expert by not requiring the production of computer coding or spreadsheet formulas, where (as is often the case) the calculations can be verified from the output or results without the necessity of inspecting the underlying coding or formulas. *See Viacom International Inc. v. Youtube Inc.*, 253 F.R.D. 256, 259-60 (S.D.N.Y.2008), where the court refused to require You Tube and Google to produce its search coding in a suit for copyright infringement.

Several courts have held that merely printing out computer data does not implicate the Rule 901(b)(9) proof of process or system authentication requirement. *United States v. Meienberg*, 263 F.3d 1177, 1179-80 (10th Cir. 2001) ("The computer printouts were not the result of a 'process or system used to produce a result'; they were merely printouts of preexisting records that happened to be stored on a computer"); *People v. Huehn*, 53 P.3d 733, 737 (Colo. App. 2002) ("courts have generally declined to require testimony

regarding the functioning and accuracy of the computer process where, as here, the records at issue are bank records reflecting data entered automatically rather than manually").

F. EXPERT OPINIONS EMBEDDED IN COMPUTER OUTPUT. It is important to recognize the interplay between the admissibility of computer output and the admissibility of expert opinions that rely on the computer output or are woven into computer output. Many times experts rely on computer-generated information as the basis for their expert opinion. Issues of reliability of methodology and the reliability of underlying data can be latent aspects of the computer processing involved. In these situations, the data entered into the computer program and the way the computer program "massages" the data are precisely where the *Daubert/Robinson* focus should be brought to bear. These issues are discussed in Section VI.B below in connection with computer forensics, but the same standards of admissibility apply equally to an expert who has constructed a "model" based on the facts of a situation and renders opinions based on that model. As an example, testimony about lost profits in a business litigation context often turn on the reliability of the model used by the expert and the data the expert feeds into the model. Although these issues may arise in a fight over computer output, they are really governed by *Daubert/Robinson* standards. It must be remembered that computers do only what they are told to do. So, reliability issues involve who gave the computer the instructions, what those instructions were, and the quality of the data that were fed into the computer.

G. THE SEDONA CONFERENCE COMMENTARY ON ESI EVIDENCE. The Sedona Conference has published a *Commentary on ESI Evidence and Admissibility*.[23] The Commentary states:

> This commentary . . . is divided into three parts: Part I is a brief survey of the applicability and application of existing evidentiary rules and case law addressing the same. Part II addresses new issues and pitfalls that are looming on the horizon. Part III provides practical guidance on the use of ESI in depositions and in court.

Id. at 1. The Commentary argues that different types of ESI require different approaches. It discusses the admissibility of email, website posting, text messaging, chat room content, and computer-stored records and databases. *Id.* at 4-8.

VII. COMPUTER FORENSICS. Computer forensics involves techniques that permit a skilled person to obtain and analyze ESI that is not available to those who merely use application software, i.e., metadata. The International Association of Computer Investigative Specialists (IACIS) gives the following definition:

> Computer forensics may be defined as the retrieval and analysis of data
>
> From a seized computer hard drive or other electronic media…
>
> Performed in such a manner that the results are...
>
> Reproducible by another examiner who...
>
> Following the same steps, reaches the same conclusions.[24]

A. CERTIFYING ORGANIZATIONS.

---

[23] <http://www.thesedonaconference.org/dltForm?did=ESI_Commentary_0308.pdf>.

[24] <http://www.iacis.com/assets/docs/trainning/IACIS_Program_Description-20101.pdf>.

The forensic computer industry is in the early stages of becoming formalized. See Jason Krause, *Computer Forensics Experts, Who's Your Daddy?*, Law Technology News (8-31-2010).[25] Krause quotes Texas attorney Craig Ball as saying:

> "The fact is that most certifications in computer forensics mean little more than that the person has paid a fee and completed a form," says Craig Ball, a computer forensics examiner in Austin, Texas. "I hold multiple certifications, so it's not that I feel they have no value; but I think that you can pass the certification exams and still be a markedly inadequate examiner."

Krause mentions three certification organizations: International Information Systems Security Consortium, Inc. (open only to law enforcement and military); the EnCase Certified Examiner program from Guidance Software; and the International Society of Forensic Computer Examiners' Certified Computer Examiner program.

B. ADMISSIBILITY OF FORENSIC EXPERT TESTIMONY. In order to admit expert evidence, over objection, the proponent must show five things: (1) that the expert is qualified; (2) that the expert's methodology is reliable; (3) that the underlying data is reliable; (4) that the evidence is relevant; and (5) that the expert's opinion would assist the trier of fact.

1. Qualifications. Under TRE 702, a person may testify as an expert only if (s)he has knowledge, skill, experience, training or education that would assist the trier of fact in deciding an issue in the case. *See Broders v. Heise*, 924 S.W.2d 148, 149 (Tex. 1996). Whether an expert is qualified to testify under Rule 702 involves two factors: (1) whether the expert has knowledge, skill, etc.; and (2) whether that expertise will assist the trier of fact to decide an issue in the case. Courts sometimes evaluate the first prong, of adequate knowledge, skill, etc., by asking whether the expert possesses knowledge and skill not possessed by people generally. *Broders*, 924 S.W.2d at 153. *See Duckett v. State*, 797 S.W.2d 906, 914 (Tex. Crim. App. 1990) ("The use of expert testimony must be limited to situations in which the issues are beyond that of an average juror"); John F. Sutton, Jr., *Article VII: Opinions and Expert Testimony*, 30 HOUS. L.REV. 797, 818 (1993) [Westlaw cite 30 HOULR 797].

2. Reliability of Methodology. In the case of *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S. Ct. 2786, 125 L.Ed.2d 469 (1993), the U.S. Supreme Court held that FRE 702 overturned earlier case law requiring that expert scientific testimony must be based upon principles which have gained "general acceptance" in the field to which they belong. *Id*. at 594, 2797. Under Rule 702, the expert's opinion must be based on "scientific knowledge," which requires that it be derived by the scientific method, meaning the formulation of hypotheses which are verified by experimentation or observation. The Court used the word "reliability" to describe this necessary quality. *Id*. at 595, 2797. The U.S. Supreme Court's opinion in *Daubert* applies in all federal court proceedings.

In *Daubert*, the Supreme Court gave a non-exclusive list of factors to consider on the admissibility of expert testimony in the scientific realm: (1) whether the expert's technique or theory can be or has been tested; (2) whether the technique or theory has been subject to peer review and publication; (3) the known or potential rate of error of the technique or theory when applied; (4) the

---

[25] <http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202471294324>.

existence and maintenance of standards and controls; and (5) whether the technique or theory has been generally accepted in the scientific community. In *Kumho Tire Co. v. Carmichael,* 526 U.S.137, 11 S. Ct. 1167, 143 L.Ed.2d 238 (1999), the Supreme Court said that the reliability and relevancy principles of *Daubert* apply to all experts, not just scientists, and where objection is made the court must determine whether the evidence has "a reliable basis in the knowledge and experience of [the relevant] discipline." *Id*. at 148, 1174. The trial court has broad discretion in determining how to test the expert's reliability. *Id. Kuhmo Tire* acknowledged that the list of factors in *Daubert* did not apply well to certain types of expertise, and that other factors would have to be considered by the court in such instances.

The Texas Supreme Court adopted the U.S. Supreme Court's *Daubert* analysis for TRE 702, requiring that the expert's underlying scientific technique or principle be reliable, in *E.I. du Pont de Nemours v. Robinson*, 923 S.W.2d 549 (Tex. 1995). The Texas Supreme Court listed factors for the trial court to consider: (1) the extent to which the theory has been or can be tested; (2) the extent to which the technique relies upon the subjective interpretation of the expert; (3) whether the theory has been subjected to peer review and/or publication; (4) the technique's potential rate of error; (5) whether the underlying theory or technique has been generally accepted as valid by the relevant scientific community; and (6) the non-judicial uses which have been made of the theory or technique. *Id* at 557.

As with the U.S. Supreme Court, the Texas Supreme Court was required to adapt the *Robinson* "hard science" criteria to other fields of expertise. In *Gammill v. Jack Williams Chevrolet, Inc.*, 972 S.W.2d 713 (Tex. 1998), the Texas Supreme Court announced that the reliability and relevance requirements of *Robinson* apply to all types of expert testimony. In *Gammill* a unanimous Supreme Court said:

> We conclude that whether an expert's testimony is based on "scientific, technical or other specialized knowledge," *Daubert* and Rule 702 demand that the district court evaluate the methods, analysis, and principles relied upon in reaching the opinion. The court should ensure that the opinion comports with applicable professional standards outside the courtroom and that it "will have a reliable basis in the knowledge and experience of [the] discipline." [FN47]

Id. at 725-26. After *Gamill, Daubert/Robinson* challenges may involve two prongs: (1) establishing the "applicable professional standards outside the courtroom" and (2) establishing that these standards were met by the expert in this instance.

3. Reliability of Underlying Data. Expert testimony is inadmissible if the underlying data does not provide a sufficient basis for the expert's opinions and conclusions. The requirement that the expert's underlying data be sufficient is explicitly stated in TRE 705(c).

TRE 705. Disclosure of Facts or Data Underlying Expert Opinion

> **(a) Disclosure of Facts or Data.** The expert may testify in terms of opinion or inference and give the expert's reasons therefor without prior disclosure of the underlying facts or data, unless the court requires otherwise. The expert may in any event disclose on direct examination, or be required to disclose on cross-examination, the underlying facts or data.

> **(b) Voir dire.** Prior to the expert giving the expert's opinion or disclosing the underlying facts or data, a party against whom the opinion is offered upon request in a criminal case shall, or in a civil case may, be permitted to conduct a voir dire examination directed to the underlying facts or data upon which the opinion is based. This examination shall be conducted out of the hearing of the jury.
>
> **(c) Admissibility of opinion.** If the court determines that the underlying facts or data do not provide a sufficient basis for the expert's opinion under Rule 702 or 703, the opinion is inadmissible.
>
> **(d) Balancing test; limiting instructions.** When the underlying facts or data would be inadmissible in evidence, the court shall exclude the underlying facts or data if the danger that they will be used for a purpose other than as explanation or support for the expert's opinion outweighs their value as explanation or support or are unfairly prejudicial. If otherwise inadmissible facts or data are disclosed before the jury, a limiting instruction by the court shall be given upon request.

4. Relevancy of the Expert Evidence. *Daubert* and *Robinson* contain a relevancy requirement for expert evidence. As explained in *Gammill v. Jack Williams Chevrolet, Inc.*, 972 S.W.2d 713, 720 (Tex. 1998):

> The requirement that the proposed testimony be relevant incorporates traditional relevancy analysis under Rules 401 and 402 of the Texas Rules of Civil Evidence. To be relevant, the proposed testimony must be "sufficiently tied to the facts of the case that it will aid the jury in resolving a factual dispute." Evidence that has no relationship to any of the issues in the case is irrelevant and does not satisfy Rule 702's requirement that the testimony be of assistance to the jury. It is thus inadmissible under Rule 702 as well as under Rules 401 and 402.

Some courts and commentators call this connection the "fit" between the evidence and the issues involved in the case.

5. Helpfulness of the Expert Evidence. Tex. R. Evid. 702 requires that the expert's testimony "assist the trier of fact." There are some issues where the jury is capable of making its own determination, without the assistance of expert testimony. In those instances, expert testimony is not admissible. *K-Mart Corp. v. Honeycutt*, 24 S.W.3d 357, 360 (Tex. 2000) ("When the jury is equally competent to form an opinion about the ultimate fact issues or the expert's testimony is within the common knowledge of the jury, the trial court should exclude the expert's testimony").

6. Applying These Standards to Computer Forensics. The field of computer forensics is relatively new compared to biochemistry, engineering, fingerprint comparison, arson investigation, etc. The principles of computer forensics are not taught in every university or police department, and there are no widely-accepted authoritative texts concerning these matters. Certifying organizations are in their infancy, and their certification process lacks the rigor characteristic of more mature fields. While some standardization has been achieved by ANSI and ISO, there is no central authority that issues standards for computer forensics. However, computer manufacturers, operating system designers, and software designers, have consistent protocols for the way their products process data. Internet email protocols are by their very nature standardized across the industry. So there are pockets of standardization in the computer industry.

Computer forensics has the advantage, assuming that the metadata is not altered or destroyed, that the expert's methodology, once explained, may be duplicated, the underlying data can be confirmed, and the degree to which the expert's conclusions are subjective will be evident. As noted above, however, there are concerns about the integrity of some metadata.

VIII. APPENDIX.

A. FAMILY LAW PRACTICE MANUAL. The Texas Family Law Practice Manual deals with ESI, but in a non-robust way. Here is the form book's request for ESI. References to electronic information are in italics. Note that the form request only asks for paper-like information that is stored electronically. No information that is uniquely electronic is specified, such as metadata, disk drives, etc. The form Response does have three provisions that deal with purely electronic data.

Form 5-23

[Petitioner/Respondent]'s Request for Production and Inspection

[to Party]

* * *

Definitions

* * *

"Item," "document," or "documents" includes, but is not limited to, each tangible thing, recording, or reproduction of any visual or auditory information, including but not limited to papers, books, accounts, drawings, graphs, charts, photographs, *electronic* or videotape recordings, data, and data compilations, however made, whether handwritten, typewritten, or printed material, drafts, duplicates, carbon copies, photocopies, *e-mail, scanned documents, digital documents,* and all other copies.

* * *

Instructions

* * *

If any of this information is solely in electronic or magnetic form, you must produce this information by providing [Petitioner/Respondent] with this information on CD-ROM computer disks formatted for IBM-compatible computers with a notation identifying the computer program (including version identification) necessary to access the information.

* * *

Exhibit A

General Documents

1. . . .

2. All diaries, notes, memoranda, journals, or calendars, including electronic diaries, memoranda, journals, or calendars, letters and correspondence, *including electronic writings (for example, e-mail and text messages),* or other written logs that relate to–

a. conservatorship;
b. possession and access;
c. child support and health insurance for the child[ren];
d. division of community property and liabilities, including claims for a disproportionate division of the community estate;
e. claims for reimbursement;
f. claims for spousal maintenance;
g. attorney's fees;
h. fault in the breakup of the marriage;
i. tort claims; and
j. requests for permanent injunctions.

* * *

36. All residence [include if applicable: business,] and wireless telephone records of the parties since [date].

* * *

Form 5-24

Response to Request for Production and Inspection

* * *

Objection is made to the request for production of data or information that exists in electronic or magnetic form because [Petitioner/Respondent] failed to specify the form in which [Petitioner/ Respondent] wants it produced. Tex. R. Civ. P. 196.4.

Objection is made to the request for production of data or information that exists in electronic or magnetic form because [Respondent/Petitioner] cannot—through reasonable efforts—retrieve the data or information requested. Tex. R. Civ. P. 196.4.

Objection is made to the request for production of data or information that exists in electronic or magnetic form because [Respondent/Petitioner] cannot—through reasonable efforts—produce the data requested in the form requested. Tex. R. Civ. P. 196.4.

B. LITIGATION HOLD LETTER. The following letter was offered by the Public Agencies Risk Management Association[26] as a sample of a letter placing a "litigation hold" on an opposing party's ESI.

Opposing party preservation letter-[sample]

Re: [CASE NAME] PRESERVATION OF ELECTRONIC DISCOVERY

Dear [OPPOSING COUNSEL/PARTY]

I. Demand for Preservation of Electronically Stored Information

[OUR CLIENT] hereby demands that [opposing party] preserve all documents, tangible things and electronically stored information ("ESI") potentially relevant to any issues in the above entitled matter.

As used in this document, "you" and "your" refers to [Opposing party] and its predecessors, successors in interest, assignees, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, employees, servants, agents, attorneys, and accountants.

You should anticipate that much of the information subject to disclosure or responsive to discovery in this matter is stored on your current and former computer systems and other media and devices (such as: personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter, "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

• Digital communications (e.g., e-mail, voice mail, instant messaging);
• Word processed documents (e.g., Word or WordPerfect documents and drafts);
• Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
• Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
• Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
• Sound Recordings (e.g., .WAV and .MP3 files);
• Video and Animation (e.g., .AVI and .MOV files);
• Databases (e.g., Access, Oracle, SQL Server data, SAP);
• Contact and Relationship Management Data (e.g., Outlook, ACT!);

---

[26] <http://www.parma.com/documents/10RMC/F6_Opposing%20party%20preservation%20letter-%5Bsample%5D.pdf>.

• Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
• Online Access Data (e.g., Temporary Internet Files, History, Cookies);
• Presentations (e.g., PowerPoint, Corel Presentations)
• Network Access and Server Activity Logs;
• Project Management Application Data;
• Computer Aided Design/Drawing Files; and,
• Back Up and Archival Files (e.g., Zip, .GHO)

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obliged to preserve potentially relevant evidence from both these sources of ESI, even if you do not anticipate producing such ESI.

The demand that you preserve both accessible and inaccessible ESI relevant to this matter is limited, reasonable, and necessary. As you are aware, the recent state and federal laws require that you preserve and at the appropriate time produce all sources of ESI. For good cause shown, the court may order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible must be preserved in the interim so as not to deprive [our client] of his right to secure the evidence or the Court of its right to adjudicate the issue.

II. Preservation Requires Your Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information with the earlier of a Created or Last Modified date on or after [insert date] through the date of this demand and concerning: [examples]

1. The events [related in any matter to {describe event}or [causes of action described in your complaint];
2. All e-mail communications and attachments…
3. All text message communications on any cell phone or other electronic device use by [name] between [dates]
4. All voice mail communications….
5. All electronic tracking data of vehicles involved in the incident…
6. All dashboard cameras or other electronic surveillance of …..
7. ESI you may use to support claims in this case;
8. Communications [by, to, with, involving]…
9. The [insert event] alleged in paragraph 15 of the Complaint;
10. All dispatch communications…

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. Be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve document, tangible things and other potentially relevant evidence.

III. Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act

diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

IV. Guard Against Deletion

You should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees and officers. It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

V. Preservation in Native Form

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible

VI. Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC

and BCC fields.

VII. Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7.

VIII. Home Systems, Laptops, Online Accounts and Other ESI Venues

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems may contain potentially relevant data. To the extent that officers, board members, employees, sale representatives, or other employees have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as Facebook, Twitter, AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

IX. Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like. You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI. You must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

X. Paper Preservation of ESI is Inadequate

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

XI. Agents, Attorneys and Third Parties

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

XI. System Sequestration or Forensically Sound Imaging

We suggest that with respect to [insert names], removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step. In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective.

As we anticipate the need for forensic examination of one or more of these systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss. By "forensically sound," we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

XII. Preservation Protocols

It is my intent to work with you to form an agreement regarding an acceptable protocol for forensically sound preservation. If you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them.

XIII. Do Not Delay Preservation

I'm happy to discuss reasonable preservation steps; however, you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay. Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which [client] is entitled, such failure would constitute spoliation of evidence, and could result in sanctions.

XIV. Confirmation of Compliance

Please confirm that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

I appreciate your continuing courtesy and professionalism.

Very Truly Yours

IX. BIBLIOGRAPHY.

- Clay Calvert, Kayla Gutierrez, Karla D. Kennedy, Kara Carnley Murrhee, *David Doe v. Goliath, Inc.: Judicial Ferment in 2009 for Business Plaintiffs Seeking the Identities of Anonymous Online Speakers,* 43 J. MARSHALL L. REV. 1 (2009).

- Timothy J. Carroll and Bruce A. Radke, *Federal Rules of Civil Procedure Concerning E-Discovery Impact* (2010) <http://www.busmanagement.com/article/Federal-Rules-of-Civil-Procedure-Concerning-E-Discovery-Impact>.

- The Electronic Discovery Reference Model <http://edrm.net>.

- Sheldon M. Finkelstein and Evelyn R. Storch, *Admissibility of Electronically Stored Information: It's Still the Same Old Story,* 23 J. AM. ACAD. MATRIM. L. 45 (2010).

- Jayni Foley, Note, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 457 (2007)

- Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH LAW REV. 1433 (2008).

- *The Sedona Conference Commentary on Non-Party Production and Rule 45 Subpoenas* (Blakely, et al., editors 2008)

<http://www.thesedonaconference.org/dltForm?did=Rule_45_Subpoenas>.