

USING ELECTRONIC EVIDENCE

REGINALD A. HIRSCH
LAW OFFICE OF REGINALD A. HIRSCH
1980 Post Oak Boulevard
Suite 2210
Houston, Texas 77056
(713) 961-7800
(713) 961-3453 (Facsimile)
reghir@hirschfamilylaw.com

23RD ANNUAL FAMILY LAW CONFERENCE
SOUTH TEXAS COLLEGE OF LAW
HOUSTON, TEXAS
MARCH 5-6, 2009

TABLE OF CONTENTS

I.	Introduction	1
II.	What is it?	1
	A. Types of Electronic Data	1
	B. Deleted files aren't really deleted	2
	C. Metadata	2
	D. Where the Rubber meets the Road	7
III.	What To Do With It?	7
	A. Texas Rules of Procedure	7
	B. Case Law	10
	C. Spoilation Issues	12
	1. Spoilation Defined	12
	2. Spoilation Presumption	13
	3. Sanctions	14
	4. Duty to Preserve	14
	5. Tex.R.Civ.P. 193.3–Asserting a Privilege	16
	D. Communications	18
	E. Prohibited Conduct	19
	F. Interspousal Wiretap Exception	20
	G. Admissibility of Telephone Recordings	21
	H. Penalties for Violations	22
	I. Voice Mail	23
	J. Right of Privacy	23
IV.	How Do I Get Rid of It?	26
	A. What do you mean the computer Geek needs to be a Licensed Private Eye?	26
	B. Rules of Evidence and Procedure Apply to Electronic Evidence	31
	1. Authentication	31
	2. Self-Authentication	31
	3. Best Evidence Rule	33

4.	The Hearsay Rule	34
5.	Business Records Exception to Hearsay Rule	35
6.	Other issues - Privacy Concerns	35
7.	Last Thoughts	36
C.	Rule 107. Rule of Optional Completeness	36
V.	Conclusion	36
	Exhibit A	37

USING ELECTRONIC EVIDENCE

I. Introduction

The most complex issue in the 21st century from both a judicial and legal perspective, is electronic evidence. From the standpoint of the judiciary and family lawyers the questions are :

1. What the heck is it?
2. What do I do with it?
3. How do I get rid of it?

While these questions may be over-simplified, they are still essential for the administration of justice. There are over 250 Continuing Legal Education articles on the State Bar CLE website which address Electronic Evidence issues. So let's begin our examination. I have extracted material from a number of CLE articles and attempted to organize this paper in a manner so that you can quickly review information relevant to the point in time where a lawyer or judge can find resources helpful to resolving these complex issues.

II. What is it?

Electronic evidence is a term so broadly defined as to be almost infinite in scope.

A. Types of Electronic Data

The types of electronic data often seen in family law cases can be categorized into four basic groups: (1) voice transmissions which include audio tape, cell phone transmissions and voice mail; (2) computer generated data including databases, spreadsheets, e-mails, computer generated photographs and other information stored on computers; (3) information from PDA's (Personal Digital Assistant's) including calendars, notes and address books; and (4) video

transmissions including videotape and picture phones.

In family law litigation, information obtained from cell phone and land line telephone communication, pictures or videos stored within a cell phone, calendars and appointments listed in a management program or on a hand-held computer or PDA device, can contain a wealth of information regarding a person's activities and habits. A person's computer can include a wide variety of information including financial documents, spreadsheets, tax documents, e-mails, electronic messaging and data hidden within the computer such as common web sites visited and information downloaded to the hard drive from the internet. Data found on a computer may appear in one or more of the following forms:

1. Live Data would consist of the currently-in-use data files and include word processing, spreadsheets, electronic calendars, address books, case or contract management documents and other works in progress.
2. Replicant Data includes self generated storage of documents such as information on the computer's hard drive and is part of a redundant system designed to eliminate system failures.
3. Archival or backup data is a form of inactive data and includes information copied to removable media such as tapes, zip drives and CD-ROM. This inactive data can also include "file clones" which is designed to assist in the recovery of data that appears lost when a computer malfunctions or is misused. Additionally, Microsoft's newest operating system makes

USING ELECTRONIC EVIDENCE

“shadow copies” of files, which has and will become a fertile field for discovery in the coming years.

4. Hidden data or metadata consists of information contained with in an electronic version of a document and includes logs with information about when, where and who accessed the system. This data is not consciously or unconsciously recorded by the user, and would not be apparent in a printout, but is embedded in the document. It can include the date the document was created, the identity of the author, the identity of subsequent editors, and a history of edits to the documents among other things.

5. Residual data is the entirety or remnants of deleted files of which the file reference has been removed from the directory listings making the information invisible to most programs. Residual data remains undetected on disks and drives and can be the most costly form of data to recover from a computer.

6. Legacy data is older information stored in an electronic format that can no longer be read using current software. Most often legacy data takes the form of records in an existing database or a system in current use.

Computers can also contain information about internet use including the following.

7. Cache Files record internet addresses visited by the user and graphic elements of the web pages

8. Cookies are bits of information about the use and or the user of the

computer that are placed on the hard drive by web site operators.

9. Bookmarks are created by the user for one-click shortcuts which are stored on the computer.

See Rhonda Hunter, DISCOVERABILITY AND ADMISSIBILITY OF ELECTRONIC EVIDENCE, 31st Annual Advanced Family Law Course, August 2005

The issue as you can see is cost, volume of data, and the means to get the data in an understandable format.

B. Deleted files aren't really deleted.

First, an explanation of computer data and what makes it's recovery challenging and somewhat scary to the average person. A deleted file really isn't deleted. In the days of DOS (Disk Operating System) it was recognized that deleted data might need to be recovered so the first letter of the file was given a machine code character that made it unreadable except with a recovery utility. That is why the recycle bin of the computer under windows will allow you to “restore” a file. The machine code is then converted to a readable format, and the deleted file has been recovered. But in the event that the space occupied by the file is needed and overwritten, then the file is lost. There is other data that is not readily understood and that is called metadata.

C. Metadata

What is metadata? In an article entitled *Beyond Data about Data: The Litigator's Guide to Metadata*, Craig Ball states:

USING ELECTRONIC EVIDENCE

Ask an electronic evidence expert, 'What's metadata?' and there's a good chance you'll hear, 'Metadata is data about data'--another answer that's 100% accurate, and totally useless!

Perhaps it's more helpful to say that, "metadata is evidence, typically stored electronically, that describes the characteristics, origins, usage and validity of other electronic evidence." There are all kinds of metadata found in various places in different forms. Some is supplied by the user and some is created by the system. Some is crucial evidence and some just digital clutter. Understanding the difference--knowing what metadata exists and what evidentiary significance it holds--is an essential skill for attorneys dealing with electronic discovery."

As to why we care about the definition of metadata, see the following case where a federal judge was confronted with the issue:

In *Williams v. Sprint/United Mgmt Co.*, the Federal court ruled that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their METADATA INTACT, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order." 230 F.R.D. 640, 651 (D. Kan. 2005).

Having both embedded application metadata and external system metadata is advantageous because, when metadata is stored both within and without a file, *discrepancies* between the metadata can expose data tampering.

Like all data, embedded application metadata is just a sequence of ones and zeroes and, in that respect, no less "accessible" than any other data. Accessibility is a measure of an application's ability to convert those ones and zeroes into intelligible information. A programmer configures applications to display selected information—but not necessarily *all* information—by default. Information not displayed by default may be accessible by reconfiguring the program's default settings (such as when a user sets a spreadsheet program to display formulae instead of calculated values). Viewing other embedded data may require drilling down through application menus, such as when a user explores file properties for a Microsoft Office document. These properties are at hand and comprehensible, but tend not to lend themselves to easy printing. None of this is surreptitious data—it's there if the user elects to review it. In fact, despite the common practice to call metadata "hidden," the only application of metadata to warrant that description is the information the program employs internally to track, replicate or manage its actions. This data is, indeed, not readily accessible to the user via the program's menus and user-configurable settings, instead requiring specialized computer forensic tools and expertise to extract and interpret.

Every active file stored on a computer has at least one

USING ELECTRONIC EVIDENCE

corresponding external block of system metadata—every one, no exceptions. Files may also have multiple associated metadata blocks as well as embedded metadata fields. You will never face the question of *whether* a file has metadata—all active files do—instead, the issues are *what kinds* of metadata exist, *where* the metadata resides and whether it's potentially *relevant* such that it must be preserved and produced. Modern operating systems record a ream of data detailing the creation, use and status of files as well as the use and configuration of associated applications. Windows users see a few of these characteristics tracked in the “details” view of a folder. By default, only a file's name, size, type and date modified are displayed; however, right click on the column titles in Windows XP and another thirty-four-odd metadata fields can be displayed, including creation date, author and comments. But even this broad swath of metadata is just *part* of the information about the file recorded by the operating system.

Within the Master File Table are index records used by Windows XP to track all files, still more attributes are encoded in hexadecimal notation. In fact, an ironic aspect of Windows is that the record used to track information about a file may be larger than the file itself! Stored within the hives of the System Registry—the “Big Brother” database that tracks attributes covering almost any aspect of the system—are thousands upon thousands of attribute values called “registry keys.” Other records and logs track network activity and journal virtually every action. Within this maelstrom of metadata, some information is readily accessible and

comprehensible while other data is so byzantine and cryptic as to cause even highly skilled computer forensic examiners to scratch their heads. To preserve metadata and assess its relevance, you have to know it exists. So, for each category of data subject to discovery, assemble a list of associated metadata. You'll likely need to work with an expert the first time or two, but once you have a current and complete list, it will serve you in future matters.

You'll want to know not only what the metadata field contains, but also its location and its significance. The numbers may surprise you. There are at least **eighty** easily accessible application and system metadata fields tracked for each Microsoft Word, PowerPoint and Excel document, *excluding* tracked changes, comments and Registry data (though a few are redundant and the majority of them rarely used).

In fact Microsoft in an article about Microsoft Word states the following:

The word document may contain content that you may not want to share with others when you distribute the document electronically. This information is known as “metadata”. Metadata is used for a variety of purposes to enhance the editing, viewing, filing, and retrieval of Microsoft Office documents.

Some metadata is readily accessible through the Microsoft Word user

USING ELECTRONIC EVIDENCE

interface; other metadata is only accessible through extraordinary means, such as opening a document in a low-level binary file editor. Here are some examples of metadata that may be stored in your documents:

- Your name
- Your initials
- Your company or organization name
- The name of your computer
- The name of the network server or hard disk where you saved the document
- Other file properties and summary information
- Non-visible portions of embedded OLE objects
- The names of previous document authors
- Document revisions
- Document versions
- Template information
- Hidden text
- Comments

Further Microsoft talks about the fast save feature and states the following:

The FastSave feature speeds up the process of saving a document by saving only the changes that are made to a document.

Because of the design of the FastSave feature, text that you delete from a document may remain in the document, even after you save the

document. If you are concerned about deleted text remaining in your documents, follow these steps:

1. On the **Tools** menu, click **Options**.
2. Select the **Save** tab.
3. Clear the **"Allow fast saves"** check box. Click **OK**.

As Kim Komando pointed out in a USATODAY article entitled "Remove Hidden Data in Microsoft Word Documents", dated January 19, 2006:

There are a number of ways to ensure that your personal or company data stays with you:

- Turn off Fast Save. This feature speeds up saving a document by saving only changes made to a document. However, text that you delete from a document may still remain. Microsoft recommends turning off this feature to eliminate any chance of deleted text remaining in the document. Click Tools, then Options. Click the Save tab. Clear the "Allow fast saves" check box and click OK.

- You can remove personal information from a document when you save it. In Word 2002 and 2003, click Tools, then Options. Click the

USING ELECTRONIC EVIDENCE

Security tab. Under Privacy options, select "Remove personal information from file properties on save" and click OK. In Word 2000, click Tools, the Options. Select the User Information tab. Clear the information in Name, Initials and Mailing Address and click OK.

- Turn off the Track Changes tool. In Word 2002 and 2003, click Tools, then Track Changes. In Word 2000 and earlier versions, click Tools, Track Changes, Highlight Changes. Click to clear the check mark in the "Track Changes while editing" box.

You can tell if the Track Changes feature is on by looking at the status bar (located at the bottom of every document). When Track Changes is enabled, TRK appears in the status bar. When Track Changes is disabled, TRK is dimmed.

Track Changes must be disabled before writing the document. Otherwise, any changes made will not be removed.

- Finally, a free Microsoft tool removes hidden data from Word, Excel and PowerPoint. The Remove

Hidden Data add-in tool (snipurl.com/3osw) will delete hidden text and comments from individual files or a batch of files at once.

Wow is that a potential area for discovery.

That is a partial answer as to why the recovery of metadata can be so important.

But the issue has gotten to be a huge problem with metadata and the information it can provide.

In Florida, a bar director was apparently tricked into providing a file that contained editing data to an opposing lawyer. Gary Blakenship, The Florida Bar News, What's in Your Document? Jan. 1, 2006. As a result, the Florida bar has an ethics opinion concluding that "a lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer." Any such metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit. Professional Ethics of the Florida Bar, Opinion 06-02 (September 16, 2006). The Florida opinion also notes an obligation on sending attorneys to protect confidential information, including information that might be revealed in hidden data. It also notes that this "may necessitate a lawyer's continuing training and education in the use of technology in transmitting and receiving electronic documents in order to protect client information." The Florida opinion specifically does not address what a

USING ELECTRONIC EVIDENCE

lawyer's obligations about hidden data are with regard to discovery of electronic documents in litigation, however, New York had come to a similar conclusion in 2001, holding that "(a) lawyer may not make use of computer software applications to surreptitiously "get behind" visible documents or to trace e-mail." New York State Bar Association Op. 749 (December 11, 2001). A second New York ethics opinion holds that lawyers have an obligation under disciplinary rules to avoid transmitting hidden data that is confidential. New York State Bar Association Op. 782 (December 8, 2004), online at <http://www.nysba.org/Content/NavigationMenu/AttorneyResources/Ethics Opinions/Opinion 782.htm>.

And if you think only lawyers and citizens are ones to be concerned about this issue consider this factoid: Editing information can show the revision history of a document. One of the most useful features of modern word processors is redline functionality which shows what portions of a document were changed between drafts. Comments can be made to documents that will not show up with the document is printed. Unfortunately, unless affirmative steps are taken to eliminate the redlines and comments, these can be passed along to adverse parties along with the electronic file. What you see is not necessarily what you get: the last thing you see on the screen or printed document may not be all of what a user on the other end can see. It has been told that the Lubbock Court of Appeals recently released opinions on their website that showed red line editing. The opinions were taken down after the problem was reported. See SELECTED LEGAL MALPRACTICE

AND ETHICAL ISSUES IN THE USE OF CURRENT TECHNOLOGY by Jett Hanna, State Bar of Texas, November 8 – 9, 2006 Dallas.

D. Where the Rubber meets the Road.

Now we have the tsunami of data, both original and metadata, and what the Court does with this? The second question is "What do we do with it?"

III. What To Do With It?

Let's examine some legal principles and case law to see how effectively a trial court deals with electronic evidence. Some guidance is provided by Texas and Federal Rules of Civil Procedure and Texas and Federal Case law.

A. Texas Rules of Procedure

Beginning with what the Texas Rules of Procedure reference about electronic evidence, the discovery rules set forth address electronic evidence. Rule 192.3(b) of the Texas Rules of Civil Procedure provides:

(b) Documents and tangible things. A party may obtain discovery of the existence, description, nature, custody, condition, location, and contents of documents and tangible things (including papers, books, accounts, drawings, graphs, charts, photographs, electronic or videotape recordings, data, and data compilations) that constitute or

USING ELECTRONIC EVIDENCE

contain matters relevant to the subject matter of the action. A person is required to produce a document or tangible thing that is within the person's possession, custody, or control. TEX. R. CIV. P. 192.3(b).

Rule 196.4 of the Texas Rules of Civil Procedure provides.

Electronic or Magnetic Data. To obtain discovery of data or 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. TEX. R. CIV. P. 196.4.

Let's examine the Rules as they apply to electronic evidence:

To summarize:

TRCP 192.3 requires:

1. Production of electronic evidence which contains or constitutes matters that are relevant to the subject matter of the action. (Courts should think filtering concepts. Remember reproduction of a whole hard drive is not relevant to every case)
2. A person is required to produce that which is in their possession, control or custody.

TRCP 196.4 requires:

1. The requesting party must specifically request the electronic or magnetic data and the form in which they want it produced. Caveat: Can you ask for a print out of all information on a hard drive?

Consider the following. The number of pages within a gigabyte varies greatly depending on the type of file in question. When determining the number of pages within a gigabyte it is important to consider a number of factors, such as different types of documents produce extremely different amounts of pages. For example, a Microsoft Excel file may use a small amount of disk space, yet

USING ELECTRONIC EVIDENCE

would likely result in a large number of pages if printed, while a Microsoft Outlook email file may take up a large amount of disk space, but would only result in a small number of pages if printed, likely one per email message. The ensuing common types of files often result in an average number of pages per gigabyte and megabyte as can be seen on Exhibit A.

There are not enough trees in the rain forest to print out the average 250 gigabyte hard drive filled with documents. You might want to impress a lawyer with this chart. See, http://www.setecinvestigations.com/resources/techhints/Pages_per_Gigabyte.pdf.

Or as another example consider this extract. The Manual for Complex Litigation illustrates how information stored electronically quickly becomes voluminous:

The sheer volume of [electronic] data when compared with conventional paper documentation, can be staggering. A floppy disk, with 1.44 megabytes, is the equivalent of 720 typewritten pages of plain text. A CD-ROM, with 650 megabytes, can hold up to 325,000 typewritten pages. One gigabyte is the equivalent of 500,000 typewritten pages. Large corporate computer networks create backup data measured in terabytes, or 1,000,000 megabytes: each

terabyte represents the equivalent of 500 billion typewritten pages of plain text. THE MANUAL FOR COMPLEX LITIGATION (4th) § 11.446.

So normally unless limited data is requested, a backup on some form of media is most cost effective.

2. The responding party must produce it if it is responsive to the request and available in the normal course of business and "reasonably accessible"(meaning basically no use of forensic tools). As one spouse said when asked how her husband's computer was relevant she said, "because that's where he lives and keeps his secrets."

3. If you can't produce it by reasonable means you must object and state so. Most lawyers miss this one.

4. This is one the judiciary sometimes misses: If the court orders the responding party to produce then the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

But what are "reasonable expenses of extraordinary steps?" In a review of case law there is only one conclusion that is fact driven by each case. Some authority for cost can be considered in the following cases:

Factors include (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from

USING ELECTRONIC EVIDENCE

other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information. *Zubulake v. Warburg LLC*, 2003 U. S. Dist. LEXIS 7939 (S.D.N.Y. May 13, 2003); also see *Zubulake v. Warburg LLC*, 2003 U.S. Dist. LEXIS 12654 (S.D.N.Y. July 24, 2003).

For Texas federal case consideration see *Multitechnology Services v. Verizon Southwest*, 2004 U.S. Dist. LEXIS 12957 (N.D. Tex. July 12, 2004), in which the United States Magistrate in Fort Worth entered a protective order ordering Verizon, the producing party, to bear the initial \$60,000 cost to retrieve the requested electronic information, as the information was relevant and discoverable but only available from Verizon, but classified the cost as court costs to be recovered by the prevailing party at the end of the case.

However; remember this can be self policing to a request as one author pointed out, "Anecdotal information from the Texas experience indicates that predictable allocation of costs has dramatically reduced the overbroad nature of many requests." TEX. R. EVID. 902.

Additionally, the discovery rules may assist in the authentication of electronic data that has been produced by the other side in discovery. Texas Rule of Civil Procedure Rule 193.7 creates a presumption of authenticity for

documents produced in response to a request for written discovery, if not objected to within ten days after the producing party has actual notice that the document will be used. TEX. R. CIV. P. 193.7. Therefore, if a party produces a printed e-mail message through written discovery, the party to whom the email was given may not be required to authenticate the message.

B. Case Law

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). While at one time 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.), any general requirement for proving up the validity of the computing process for business records has been abandoned. Courts now agree that computerized business records can be proved up in the same manner as handwritten 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 admissible if requirements for business records are met); *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

USING ELECTRONIC EVIDENCE

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); *Hutchison 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); *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 human being).

The following are additional Texas Cases addressing authentication:

Davidson v. Great National Life Ins. Co., 737 S.W.2d 312, 314-15 (Tex. 1987) Photograph admissible upon sponsoring witness' testimony that photograph is "an accurate portrayal of the facts, and on verification by that witness or a person with knowledge that the photograph is a correct representation of such facts."

Seymour v. Gillespie, 608 S.W.2d 897, 898 (Tex. 1980) Tape recordings that fairly represent conversations admissible as fair representation. Elements of fair representation: (1) recording device capable of recording; (2) operator competent; (3) recording authentic and correct; (4) no changes, deletions, or additions; (5) properly preserved; (6) speaker identified; and (7) statement made voluntarily without inducement.

Mega Child Care, Inc. v. DPRS, 29 S.W.3d 303, 308, 312 (Tex. App.—Houston [14th Dist.] 2000 no pet.) "The Texas rules of Evidence require, as a predicate to admissibility, that evidence be properly authenticated or identified. . . . In other words, the proponent must show the trial court that the document or evidence in question is what he purports it to be. . . . Authentication may be accomplished by various means; one example offered by Rule 901 is where the evidence is authenticated by the testimony of a witness with knowledge. . . . [A] nonexistent document or document entry, by definition, cannot be authenticated; it does not exist, and no authentication is required."

S.D.G. v. State, 936 S.W.2d 371, 381 (Tex. App.—Houston [1st Dist.] 1996, writ denied) predicate for introduction of videotape without sound recording same as for photograph: (1) accurate and correct presentation; and (2) relevant. Predicate does not need to be provided by photographer, person photographed, or person present when photograph was made. "Any witness who observed the object or scene depicted in the photograph may lay the predicate." Trial judge has "considerable discretion in ruling on the admissibility of photography evidence."

Grossnickle v. Grossnickle, 935 S.W.2d 830, 848 (Tex. App.—Texarkana 1996, writ denied) American Express receipts admitted into evidence in case involving contested property division in attempt to prove amounts husband spent on girlfriend.

Reichold Chemicals v. Puremco Mfg., 854 S.W.2d 240, 248 (Tex. App.—Waco

USING ELECTRONIC EVIDENCE

1993, writ denied) photographs admissible upon proof that sponsoring witness has personal knowledge of accuracy of objects and events, see *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.App.—Corpus Christi 1986, writ ref'd n.r.e.) husband's tape recording of wife admitting to having used cocaine and having grown marijuana held admissible in divorce case in which husband received sole managing conservatorship of child.

Mata v. Mata, 710 S.W.2d 756, 759 (Tex.App.—Corpus Christi 1986, no writ) wife introduced photographs of "interior of the house with its furnishings" in support of her testimony regarding value of furnishings, shown in photograph.

See, Robert S. Hoffman, EVIDENCE AND DISCOVERY IN FAMILY LAW, State Bar of Texas, 17th Annual Advanced Evidence & Discovery Course, April 1-2, 2004 – Dallas.

C. Spoliation issues

1. Spoliation Defined

Spoliation is defined as "the improper destruction of evidence" relevant to a case. *Whiteside v. Watson*, 12 S.W.3d 614 (Tex.App.—Eastland, 2000); *Clements v. Conrad* 21 S.W.3d 514 (Tex. App. Amarillo, 2000). The intent of the spoliation doctrine is to prevent the subversion of the discovery process and the fair administration of justice by destroying evidence. *Trevino v. Ortega*, 96 S.W.2d 950, 955 (Tex.1998). The inquiry whether spoliation occurred begins with determining whether a duty existed to preserve the destroyed evidence. If a party violates a statutory,

regulatory or ethical duty to preserve evidence, within the broad discretion of the court, it may take measures ranging from an application of the spoliation presumption to in the most extreme cases, death penalty sanctions. *Trevino v. Ortega*, 96 S.W.2d 950, 955 and 959 (Tex.1998).

It is common in a normal business environment for periodic deletion of electronic data. When a duty arises to preserve such evidence, particularly electronic evidence, the discontinuation of an automatic deletion system may save the imposition of sanctions at a later date.

Deletion programs are normal requirements of business information systems. More and more, however retention policies are being designed to preserve relevant information. Retention policies must provide for the preservation of data which is discoverable in litigation. Once litigation is expected or ongoing, data retention policies should provide for the immediate cessation of auto-matic deletion of some information and recycling of backup tapes unless the information can be obtained from another source. In *Positive Software Solutions, Inc. v. New Century Mortgage Corporation*, 2003 U.S. Dist. LEXIS 7659 (N.D.Tex. 2003), the court ordered defendants to "preserve all existing backups or images of all servers or personal computers that now or previously contained any portion or part of the software in question, and any associated software, whether used for development, debugging, deployment, production or otherwise, including source code, object code, history or log files, or revision tracking files, and to

USING ELECTRONIC EVIDENCE

refrain from deleting any such files still resident on any servers or personal computers, and to preserve all existing backups or images of all email servers, pending further order of the court or directive of the arbitrator.” Also, see *Applied Telematics, Inc. V. Sprint Communications Co., L.P.*, 1996 WL 539595 (E.D.Pa. 1996) in which a party was sanctioned for continuing to recycle backup tapes after litigation started. There are cases which indicate that sanctions may not be imposed if the destruction of evidence was not intentional. In *Crescendo Investments v. Brice*, 61 S.W.3d 465 (Tex.App.-San Antonio, 2001, pet. denied), Mr. Brice stated that he normally erased e-mails after reading them and that he deleted files concerning personal business separate and apart from that the subject of the suit. The Court found that the e-mails were not destroyed with fraudulent intent or purpose and sanctions were not required.

2. The Spoliation Presumption

The issues related to the deletion of electronic data have led to the use of the spoliation presumption in dealing with intentionally lost or destroyed evidence. The intentional destruction or spoliation of evidence relevant to a case may give rise to a presumption that the destroyed evidence would have been favorable to its destroyer. See *Aguirre v. South Texas Blood & Tissue Center*, 2 S.W.3d 454, 457 (Tex.App.-San Antonio, 1999, pet. denied). This presumption arises only after the party not in control of the evidence has introduced evidence that is harmful to the party who had control of the evidence. *Watson v. Brazos Electric Power Cooperative, Inc.*, 918 S.W.2d

639, 643 (Tex.App.-Waco 1996, writ den'd).

A jury may be instructed that a party is entitled to show that the opposing party has destroyed evidence that would bear on a crucial issue in a case and that showing raises a presumption that the destroyed evidence would have been unfavorable to the spoliator or the one destroying the evidence. See *Whiteside v. Watson*, 12 S.W.3d 614 (Tex.App.-Eastland, 2000).

This presumption serves to insure that a litigant's rights are not impaired by another party's improper destruction of relevant evidence. *Trevino v. Ortega*, 969 S.W.3d 950, 953 (Tex.1998).

This is a rebuttable presumption. For discussion regarding overcoming the spoliation presumption see *Crescendo Investments v. Brice*, 61 S.W.3d 465 (Tex.App.-San Antonio, 2001, pet. denied). In *Crescendo*, Mr. Brice stated that he normally erased e-mails after reading them and that he deleted files concerning personal business separate and apart from that the subject of the suit, thereby overcoming the presumption. In Texas, there is no independent cause of action for spoliation of evidence. The inference arises in the context of the lawsuit in which the spoliation occurs. *Trevino v. Ortega*, 96 S.W.2d 950 (Tex. 1998).

However the most famous instruction for spoliation comes from the federal *Zubulake* case. *Zubulake v. UBS Warburg*, 2004 VVL 1620866 (S.D. N.Y., July 20, 2004) in which the instructions were:

USING ELECTRONIC EVIDENCE

I have already instructed you that the Court has found that several UBS employees failed to preserve some of their e-mails after they had been repeatedly instructed by UBS counsel . . . to preserve their e-mails. Some of those e-mails were eventually recovered from back-up tapes and produced to plaintiff. Others could not be recovered because back-up tapes no longer existed for certain months or portions of certain months. No one can ever know what would have been on those back-up tapes and whether relevant e-mails would have been recovered or produced. The fact that some UBS employees failed to preserve their e-mails after being instructed to do so, and that such e-mails cannot now be produced, is sufficient circumstantial evidence from which you are permitted, but not required, to conclude that the missing evidence was unfavorable to UBS.

3. Sanctions

Civil sanctions for spoliation of evidence are governed by Rule 215, TEX. R. CIV. P. The severity of the sanction depends on the nature of the offense, however, the consequences of the failure to

produce electronic discovery can be immediately severe. Sanctions can include a jury instruction regarding the spoliation of evidence, monetary sanctions, exclusion of evidence, dismissal of a claim or the rendering of a default judgment commonly known as death penalty sanctions. Death penalty sanctions are the most severe sanction for discovery abuse. Courts have held that the dismissal of an action or the rendering of a default judgment is allowed when the spoliator's conduct is egregious, the prejudice to the nonspoliating party was great, and imposing a lesser sanction would be ineffective to cure the prejudice. See *Trevino v. Ortega*, 969 S.W.3d 950 (Tex.1998) (Justice Baker's concurring opinion). Also see, See Rhonda Hunter, DISCOVERABILITY AND ADMISSIBILITY OF ELECTRONIC EVIDENCE, 31st Annual Advanced Family Law Course, August 2005

4. Duty to Preserve

The Texas Supreme Court holds that the duty to preserve arises only when the party knows or should know that there is a substantial chance that a claim will be filed and that evidence in its possession or control will be material and relevant to that claim. *Wal-Mart Stores v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003); see also Weinstein & Berger, WEINSTEIN'S FEDERAL EVIDENCE § 301.06[4] at 301-28.3 (2d ed. 2003) ("There must be a sufficient foundational showing that the party who destroyed the evidence had notice both of the potential claim and of the evidence's potential relevance."). Although Johnson was not an electronic evidence case the principals apply. See, Judge Xavier Rodriguez, THE MANY

USING ELECTRONIC EVIDENCE

CHALLENGES PRESENTED BY ELECTRONIC DISCOVERY, State Bar of Texas, 19TH Annual Advanced Evidence and Discovery Course, April 26-27, 2006 - Houston.

The trial court is often confronted with what is commonly referred to as an anti-spoilation TRO where a spouse asks the court to preserve the data on let's say a computer and to stop any deletions from occurring until a hearing. Some programs parties install are setup to automatically delete data and injunctions should also seek to prevent these "scheduled" cleaning programs from removing data. Backups should also be preserved. but what about the spouse who works from a large corporation and the laptop is used in his or her daily work? Can the court enjoin the spouse from removing data or deleting data on a company computer? In one case the court granted the anti-spoilation injunction and the court ordered notice to the company. The company after review of the data sought the computer back which was returned to them. "When determining whether electronic information has been destroyed intentionally, courts often look to whether it was a regular practice of the party to discard the evidence. In *Doe v. Mobile Video Tapes, Inc.*, 43 S.W.3d 40, 56 (Tex.App.-Corpus Christi 2001, *no pet. history*), an invasion of privacy case, the only way, essentially, to affirm or negate the alleged cause of action was to view videotapes of certain television broadcasts. However, viewing the tapes proved impossible because no such videotapes existed; it was established at trial that it was the regular business practice of television station involved to tape an entire broadcast, keep the recording for seven

days, and then reuse the tape for subsequent broadcasts. *Id.* Consequently, the television station could not submit into evidence the recordings of the entire broadcasts in question. *Id.* According to the Corpus Christi Court of Appeals, while it was true that the television station destroyed the videotapes, there was no evidence that they intentionally disposed of the tapes so as to make them unavailable for use at trial; rather, the evidence showed that the television station destroyed the videotapes in the ordinary course of business. *Id.* Since the evidence was destroyed in the regular course of business, the Corpus Christi appellate court held that the television station adequately defended against an assertion of negligent or intentional destruction. *Id.*" See, ELECTRONIC INVESTIGATION AND DIGITAL EVIDENCE, Kathryn J. Murphy and Rick Robertson, State Bar of Texas, 30th Annual Marriage Dissolution Institute, May 10-11, 2007, El Paso.

Recently the family law courts in Harris County, Texas have been appointing a special master for electronic issues. The parties request that the special master cause a image hard drive to be made to ascertain what information is privileged, attorney client, work product, etc. The difficulty is there is tons of data to search. Filtering privileged material is expensive. Hiring a company to replicate the hard drive and filter privileged documents, can exceed over \$,3000.00 per hard drive. Then the data needs to be reviewed and hard drives reproduced in a privileged and non privileged format. In one of my cases, we had over 5 hard drive copies made before I could certify that the privileged data had been removed.

USING ELECTRONIC EVIDENCE

Under the Texas Rules of Civil Procedure, an objection based on a privilege requires a privilege log. Let's review the case law on privilege logs:

5. TEX. R. CIV. P. 193.3 --
Asserting a Privilege

a. *In re Living Ctrs. of Tex., Inc.*, 175 S.W.3d 253 (Tex. 2005). A nursing home that asserted medical committee and peer review privileges to the disclosure of records and documents satisfied its burden of showing prima facie entitlement to privilege by providing a representative sample of the documents at issue for in camera inspection, together with a privilege log and supporting affidavit. See TEX. R. CIV. P. 193.3(a). Texas law recognizes that a party asserting a privilege may initiate its claim and establish a prima facie case of privilege by submitting evidence short of tendering each and every document. If documents are not tendered, the privilege log should be thorough. A party should also consider affidavits to support the privilege log in the absence of documents produced for in camera review.

b. *In re Christus Health Southeast Tex.*, 167 S.W.3d 596 (Tex. App.—Beaumont 2005, orig. proceeding). This case contains an excellent discussion of the procedures for asserting a privilege. Instead of objecting to discovery based on privilege, a party may withhold the privileged material and assert privileges. The party must state in the response (or any amended or supplement response) or in a separate document that: (1) information or material responsive to the request has been withheld, (2) the request to which the information or

material relates, and (3) the privilege or privileges asserted. Then, the party seeking discovery may serve a written request that the withholding party identify the information and material withheld. Within fifteen days of service of the request, the withholding party must serve a response that: (1) describes the information or materials withheld that, without revealing the privileged information itself or otherwise waiving the privilege, enables other parties to assess the applicability of the privilege, and (2) asserts a specific privilege for each item or group of items withheld. Thus, the description of the information or material withheld must be specific enough that the requesting party can identify each document withheld and assess the applicability of that privilege. Any party may then request a hearing on a claim of privilege asserted. Because there is no presumption that documents are privileged, a party who seeks to limit discovery by asserting a privilege has the burden of proof.

c. *In re TIG Ins. Co.*, 172 S.W.3d 160 (Tex. App.—Beaumont 2005, orig. proceeding) under Rule 193.3, "after receiving a response indicating that material or information has been withheld from production, the party seeking discovery may serve a written request that the withholding party identify the information and material withheld." The rules of procedure contemplate that the parties will itemize the documents claimed to be privileged, and then produce evidence regarding the documents claimed privileged if, based on the documents withheld, the proponent of the discovery desires to pursue an attempt to obtain the documents. In this case, the parties did

USING ELECTRONIC EVIDENCE

not follow this procedure in asserting attorney work product privilege and work product issue was not properly before the trial court.

d. *In re Anderson*, 163 S.W.3d 136 (Tex. App.—San Antonio 2005, orig. proceeding). The party asserting a privilege has the burden of proof and must present necessary evidence at the hearing by testimony or affidavit, served at least seven days before the hearing, to support the privilege. Only after the party asserting a privilege has made a prima facie case—provided the proper privilege log and presented evidence supporting the privilege at the hearing—does the requesting party have the burden to show the court which specific documents or groups of documents it believes require an in camera inspection.

e. *In re Graco Children's Prod., Inc.*, 173 S.W.3d 600 (Tex. App. – Corpus Christi 2005, orig. proceeding). Defendant's response to plaintiff's request for production included a general objection based on privileges. Although defendant's objection was improper, as the rules specifically instruct counsel not to object to written discovery on the basis of privilege, such an objection will not waive a privilege. A party's failure to include specific assertions of privilege in its initial responses to each production request did not waive all privileges in this case. Rule 193.2(f) provides that a party does not waive the privilege if he objects and corrects the objection after it is pointed out. While *Graco* gives some solace to those who fail to follow Rule 193, many courts require strict compliance with the rules and failure to do so will result in a waiver. As an example, *in In re TIG Ins.*

Co., 172 S.W.3d 160 (Tex.App. – Beaumont 2005, orig. proceeding), the court found that the parties had waived the right to raise by mandamus the issue of whether the trial court had improperly ordered the production of work product documents. The court noted that the party “objected to producing documents that were attorney work product” but went on to state that they would produce them at a reasonable time and place. Also, the objecting party filed to follow the requirements of Rule 193.3(b) TEX. R. CIV. P. and did not raise the issue of whether the documents were work product at the hearing. *Id.* at 169.

In the special master case in which I previously referred to we had a whoops I can't believe I just released privilege data. The attorney recognizing that an error had been made (attorney client emails where on the hard drive) invoked what has been referred to as the claw or pullback rule. It is as follows:

The Texas rules provide a procedure for handling inadvertent disclosures under TEX. R. CIV. P. 193.3(d). A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

USING ELECTRONIC EVIDENCE

See *Warrantech Corp. v. Computer Adapters Servs., Inc.*, 134 S.W.3d 516, 524 (Tex. App.—Fort Worth 2005, no pet.) (applying TEX. R. CIV. P.193.3(d), the court found that there was not intentional waiver of the attorney client privilege and that the waiver had been inadvertent. See, Kim J. Askew, PRIVILEGES, State Bar of Texas, 19th Annual Advanced Evidence and Discovery Course, April 26-27, 2006 - Houston.

For the bench trial a readily accessible Miranda Warning Card is recommended . More has been written on this area and I must get weekly calls about the recording of conversation, from true phone intercepts, to recorders in the bedroom, to secret video tape recordings. So let's review the statutes and case law on wiretap and intercepts of all types

D. Communications

Federal Law created national standards for private and governmental surveillance of wire and oral conversations. The Federal Wiretap Act, initially created in 1968 was known as Title II of the Omnibus Crime Control Act. This act governed private and governmental surveillance until it was amended in 1986. Oral and wire communications are now governed by the Electronic Communications Privacy Act of 1986 ("ECPA"). 18 U.S.C.A. Sec. 2510-3127. (1986). Title I of the ECPA regulates electronic surveillance of conversations and is known as the "Wiretap Act."

Title II regulates access to e-mail, fax and voicemail communication and is

known as the "Stored Communications Act."

Title I of the ECPA regulates the intentional interception of wire, oral and electronic communications. 18 U.S.C. Sec. 2511. Title 1 regulates only intentional actions. Title 1 is limited to the acquisition of the contents of communications contemporaneous with their transmission.

This Federal wiretap statute prohibits the interception of certain telephonic communications. Section 18 U.S.C. Sec. 2510(1) (1994) defines wire communication, while 18 U.S.C. Sec 2510(2) (1994) defines oral communication.

"Oral communication" is defined as: "Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." Title 18 U.S.C.A. Sec. 2510 (2) (1994).

"Electronic communication" is defined as: "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectric or photo optical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication [as defined and regulated in other sections; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device; or (D) electronic fund transfer information stored by a financial

USING ELECTRONIC EVIDENCE

institution in a communications system used for the electronic storage and transfer of funds.” Title 18 U.S.C.A. Sec. 2510 (12)(1994).

E. Prohibited Conduct

The interception of certain oral and wire communications is prohibited under federal law. The Federal Wiretap Act subjects a person to criminal and civil penalties for engaging in prohibited conduct specifically if one (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication; (b) intentionally uses, endeavors to use or procures any other person to use , or endeavor to use any electronic, mechanical, or other device to intercept any oral communication.; c) intentionally discloses or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; and (d) intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection. Title 18 U.S.C.A. Sec. 2511(1). It is not unlawful under the Federal Wiretap Act for a person to intercept such a communication if one of the parties to the conversation has consented to the interception as outlined under the provisions for exceptions in the statute. Specifically, in governmental surveillance, It shall not be unlawful...for

a person acting under color of law to intercept a wire, oral or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. Title 18, U.S.C.A. 2511(2)c). And for non government persons: It shall not be unlawful... for a person not acting under color of law to intercept a wire, oral or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious action in violation of the Constitution or laws of the United States or of any State. Title 18, U.S.C.A. 2511 (2)(d).

Texas law also allows for recording of conversations under certain circumstances. Recorded telephone conversations between parties are admissible if one party is aware of the taping. *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.App.-Corpus Christi 1986, writ ref'd n.r.e.). Individual states are allowed to offer more protection than the Federal Wiretap Act provides. The practitioner should be aware, consequently, that other states may require both parties to a conversation to consent to its recording. (See the state wiretap statues of states i.e. Florida, California and Maryland .) The Texas state wiretap statute is found in the Texas Civil Practice and Remedies Code Sec. 123.001-04. It states:

Sec. 123.002 Cause of Action

(A) A party to a communication may sue a person who:

USING ELECTRONIC EVIDENCE

(1) intercepts, attempts to intercept, or employs or obtains another to intercept or attempt to intercept the communication;

(2) uses or divulges information that he knows or reasonably should know was obtained by interception of the communication; or

(3) as a landlord, building operator, or communication common carrier, either personally or through an agent or employee, aids or knowingly permits interception or attempted interception of the communication.

(b) This section does not apply to a party to a communication if an interception or attempted interception of the communication is authorized by Title 18, United States Code, Section 2516.

“Communication is defined as: ...speech uttered by a person or information including speech that is transmitted in whole or in part with the aid of a wire or cable.

(2) Interception means the aural acquisition of the contents of a communication through the use of an electronic, mechanical, or other device that is made

without the consent of a party to the communication, but does not include the ordinary use of:

(A) a telephone or telegraph instrument or facility or telephone and telegraph equipment;

(B) a hearing aid designed to correct subnormal hearing to not better than normal;

(C) a radio, television, or other wireless receiver; or

(D) a cable system that relays a public wireless broadcast from a common antenna to a receiver.

Tx.Prac.&Rem.Code Sec. 123.001

F. Interspousal Wiretap Exception

Many jurisdictions hold that a recording of a conversation by one spouse of a communication by another spouse with a third party is permissible. Texas is not one of those jurisdictions. While recorded telephone conversations between parties are admissible if one party is aware of the taping, *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.App.-Corpus Christi 1986, writ ref'd n.r.e.), there is no exception to the federal wiretap law that allows for one spouse to tape record a conversation of the other spouse with a third party. See *Kent v. State*, 809 S. W. 2d 664, 668 (Tex.App.-Amarillo 1991, *pet ref'd*); *Turner v. P.V. International Corporation*, 765 S.W.2d 455, 469-470 (Tex.App.-

USING ELECTRONIC EVIDENCE

Dallas, 1988), *writ denied per curiam* 778 S.W.2d 865 (Tex. 1989).

Recording a telephone conversation without a court order or consent of one of the parties in most instances is illegal and of the federal courts that have ruled on the issue, few recognize an exception for the recording of one's spouse. In these cases the statute prohibits the interception of wire communications by any person except as specifically provided by the statute. In *Collins v. Collins*, 904 S.W.2d 792 (Tex.App.-Houston [1st Dist.] 1005, *writ denied*, 923 S.W.2d 569 (Tex. 1996) *per curiam*, husband argued that spouses should be exempt from the federal wiretap law and state provisions and that spouses should have the right to tape conversations and use the tapes in divorce proceedings.

The Court held that illegally obtained telephone recordings could not be used in a civil proceeding reasoning that spouses, as well as other persons, have rights of privacy that should be upheld. *Collins v. Collins*, 904 S.W.2d 792, 797 (Tex.App.-Houston [1st Dist.] 1005, *writ denied*).

The placement of a recording device in a room to intercept oral communication is also subject to regulation under Title I of the Wiretap Act. Where a recording device is used to capture a live or face to face encounter between a spouse and another adult, neither of whom have consented to the conversation, the audio recording is an illegal wiretap barring an exception and is not permitted.

However in a widely criticized 5th Circuit Case, the 5th Circuit said a spouse using

the community phone could record his or her spouse and 3rd parties in phone conversations. However the court in it's conclusion stated the following: As should be obvious from the foregoing, we are not without doubts about our decision. However, we have concluded that the statute is not sufficiently definite and specific to create a federal cause of action for the redress of appellant's grievances against her former husband. Our decision is, of course, limited to the specific facts of this case. No public official is involved, nor is any private person other than appellee, and the locus in quo does not extend beyond the marital home of the parties. See *Simpson v. Simpson*, 490 F.2d 803 (5th Cir.1974).

G. Admissibility of Telephone Recordings

The Federal Wiretap Statute requires the exclusion of evidence obtained in an illegal wiretap for use in trial. Section 2515 states:

Section 2515 Prohibition of use as evidence of intercepted wire or oral communication

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body,

USING ELECTRONIC EVIDENCE

legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter. Title 18 U.S.C.A. 2515.

The Texas Penal Code Sec. 16.02(b)(1) provides that a person commits an offense if he “intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral or electronic communication.” Tex.Pen.Code Ann Sec. 16.02 (b) (1) 2000. The Dallas Court of Appeals in *Turner v. P.V. International Corporation*, 765 S.W.2d 455, 469-470 (Tex.App.-Dallas, 1988), *writ denied per curiam* 778 S.W.2d 865 (Tex. 1989), has held that the Federal Wiretap Statute precludes the admission of recorded telephone conversations that were acquired in violation of the federal statute. The Supreme Court reserved any ruling on the illegality or admissibility of wiretapped tapes.

A Texas court has stated, however, that tape recordings, even if obtained without the consent of a party to it, are admissible if the proper predicate is laid. *Kotrla v. Kotrla*, 718 S.W.2d 853, 855 (Tex.App.-Corpus Christi 1986, *writ ref'd n.r.e.*).

However, in *Collins v. Collins*, 904 S.W.2d 792 (Tex.App.-Houston [1st Dist.] 1005, *writ denied*, 923 S.W.2d 569 (Tex. 1996) *per curiam*, the Court held that illegally obtained telephone recordings could not be used in a civil proceeding involving spouses, since spouses as well as other persons, have

rights of privacy that should be upheld. 904 S.W.2d 792, 797 (Tex.App.-Houston [1st Dist.] 1005, *writ denied*). Telephone conversations are authenticated “by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if:

- (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called; or
- (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

Tex. R. Evid. Rule 901(6).

The Federal Rules of Evidence list the predicate for introducing an audiotape recording into evidence. Taped telephone conversations may be admitted by showing that:

- (1) the recorder was capable of recording;
- (2) the operator was competent;
- (3) the recording is authentic and correct;
- (4) no changes, deletions or additions have been made;
- (5) the recording has been appropriately preserved;
- (6) all speakers are identified; and
- (7) the testimony was voluntary rather than induced. Fed.R.Evid Sec. 901.

H. Penalties for Violations

There are civil and criminal penalties which may be imposed for violation of the Federal Wiretap Act. Minimal

USING ELECTRONIC EVIDENCE

liquidated damages of \$10,000 are recoverable. Actual and punitive damages are recoverable.

Remedies for violation of the Texas Wiretap Statute include:

- (1) an injunction prohibiting a further interception, attempted interception, or divulgence of use of information obtained by an interception;
- (2) statutory damage of \$1000;
- (3) all actual damages in excess of \$1000;
- (4) punitive damages in an amount determined by the court or jury; and
- (5) reasonable attorneys fees and costs. Tex.Civ.Practice&Rem. Code Sec. 123.004.

I. Voice Mail

Voicemail messaging has become transfigured over the years. In digital voicemail systems voicemails are saved as an electronic file on the hard drive. This led to question whether voicemail should be treated as an oral communication (such as with telephone conversations) or an electronic communication (such as with e-mail). The USA Patriot Act, enacted in the aftermath of the events surrounding September 11, 2001, made extensive revisions to laws dealing with governmental and private surveillance of wire and electronic communications. The USA Patriot Act now clearly identifies that voicemail is to be treated the same as e-mail under the Stored Communications Act. The Stored Communications Act is located in Title II of the Electronic Communications Privacy Act of 1986. Title II regulates access to e-mail, fax and voicemail communication.

Unlike the Federal Wiretap Act there is no rule for exclusion of evidence under the Stored Communications Act. (Title II). A voicemail that constitutes an illegal interception under the Stored Communications Act may nevertheless be otherwise admissible in court.

J. Right of Privacy

This may surprise some of you - the word "privacy" is actually never used in the text of the [US Constitution](#), or any of its amendments. The Texas Supreme Court in *Texas State Employees Union, et al., Petitioners, v. Texas Department of Mental Health and Mental Retardation, et al., Respondents* (Tex.) 746 S.W.2d 203; held the following:

While the Texas Constitution contains no express guarantee of a right of privacy, it contains several provisions similar to those in the United States Constitution that have been recognized as implicitly creating protected "zones of privacy." *Cf. Roe v. Wade*, 410 U.S. 113, 152, 93 S.Ct. 705, 726, 35 L.Ed.2d 147 (1972). Section 19 of the Texas Bill of Rights protects against arbitrary deprivation of life and liberty. TEX.CONST., art. 1, § 19. Section 8 provides the freedom to "speak, write or publish", and section 10 protects the right of an accused not to be compelled to

USING ELECTRONIC EVIDENCE

give evidence against himself. TEX.CONST., art. 1, §8, 10. Sections 9 and 25 guarantee the sanctity of the individual's home and person against unreasonable intrusion. TEX.CONST., art. 1, § 9, 25. Finally, the Texas Constitution protects the rights of conscience in matters of religion. TEX.CONST., art. 1, §6. Each of these provisions gives rise to a concomitant zone of privacy. *Cf. Griswold v. Connecticut*, 381 U.S. 479, 484, 85 S.Ct. 1678, 1681, 14 L.Ed.2d 510 (1965). We do not doubt, therefore, that a right of individual privacy is implicit among those "general, great, and essential principles of liberty and free government" established by the Texas Bill of Rights. TEX.CONST., art. I, Introduction to the Bill of Rights. We hold that the Texas Constitution protects personal privacy from unreasonable intrusion. This right to privacy should yield only when the government can demonstrate that an intrusion is reasonably warranted for the achievement of a compelling governmental objective that can be achieved by no less

intrusive, more reasonable means."

Therefore one may assert a cause of action for invasion of privacy under Texas law even if a federal or state criminal statute has not been violated.

Most states have recognized a tort right to privacy in common law. The common law privacy intrusion tort is violated if someone intentionally intrudes upon the private affairs, seclusion or solitude of another person by means that would be highly offensive to a person or ordinary sensibilities. In cases where wiretap acts are not violated, the common law invasion of privacy tort may apply to the forms of surveillance that have been discussed in this paper. A violation of the invasion of privacy tort might result in an award for compensatory damages, but it would not be a basis for excluding evidence in divorce or custody proceedings. Section 625B of the Restatement (Second) of Torts (1977) provides a cause of action in the following circumstances:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or in his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Under Section 625B, to recover on the tort of invasion of privacy, the complainant must show:

- I. Conduct in the nature of an intrusion;
- II. Private nature of the thing or place intruded upon; and
- III. The intrusion was substantial and the conduct highly offensive

USING ELECTRONIC EVIDENCE

or objectionable to the reasonable person.

Professor William L. Prosser catalogued four distinct injuries under the tort of invasion of privacy:

- (1) intrusion upon a person's right to be left alone in his or her own affairs;
- (2) publicity given to private information about a person;
- (3) appropriation of some element of the person's personality for commercial use; and
- (4) false light.

See, William L. Prosser, *HANDBOOK OF THE LAW OF TORTS* 638 (2D ED. 1955). These four variations of the tort were adopted by the Second Restatement of Torts. See Restatement (Second) of Torts § 652A (1977).

Texas recognizes a cause of action for willful invasion of privacy, which is a person's right to be left alone in his or her own affairs. *Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973). The Texas Constitution protects personal privacy from unreasonable intrusion and guarantees the sanctity of the home and person against unreasonable intrusion. *Texas State Employees Union v. Texas Dep't of Mental Health and Mental Retardation*, 746 S.W.2d 203 (Tex. 1987). To recover on the tort of invasion of privacy, the complainant must show:

1. Conduct in the nature of an intrusion;
2. Private nature of the thing or place intruded upon; and
3. The intrusion was substantial and the conduct highly offensive

or objectionable to the reasonable person.

The concept of invasion of privacy covers intrusion on a party's seclusion, solitude, or private affairs. See *Boyles v. Kerr*, 855 S.W.2d 593 (Tex. 1993); *Texas State Employees Union v. Texas Dep't of Mental Health and Mental Retardation*, 746 S.W.2d 203 (Tex. 1987).

Liability for invasion of privacy does not depend on any publicity given to the person whose interest is invaded or to his affairs. *Clayton v. Richards*, 47 S.W.3d 149 (Tex.App.–Texarkana 2001, no pet.); Restatement (Second) of Torts 752B, cmt. A. One case has approved a punitive damages award of \$1,000,000 (21% of defendant chiropractor husband's net worth) where the defendant had bugged telephones of wife's attorneys and engaged in other outrageous conduct. *Parker v. Parker*, 897 S.W.2d 918, 930 (Tex. App.–Fort Worth 1995, writ denied) overruled on other grounds by *Formosa Plastics Corp. USA v. Presidio Engineers & Contractors, Inc.*, 960 S.W.2d 41.

See ELECTRONIC INVESTIGATION AND DIGITAL EVIDENCE, Kathryn J. Murphy and Rick Robertson, State Bar of Texas, 30th Annual Marriage Dissolution Institute, May 10-11, 2007, El Paso

Here's a typical call I get at least once a month. My client has accessed the community computer and observed the spouse engaged in _____ activity. You fill in the blank. Is that legal and what kind of trouble am I in by just looking at the material. Let's just

USING ELECTRONIC EVIDENCE

examine the right of privacy aspect for now.

The real litmus test for claims of invasion of privacy depends on the answer to: "Was the material or data preserved in a manner to give rise to a reasonable expectation of privacy?" If the answer is "yes" you may have a claim for invasion of privacy. So we need to ascertain things like location of the computer, was it password protected and if so was the password kept secret and not disclosed, was the computer used by family members or 3rd parties, was the computer a personal or business computer, was the computer used by the other spouse regular or infrequent, what steps did the user take to secure his or data, etc. There are many weight factors to consider, but the test again was there a reasonable expectation of privacy. This is the key to understanding the right of privacy.

IV. How Do I Get Rid of It?

A. What do you mean the computer geek needs to be a licensed private eye?

Yes you read that right. Hyattye O. Simmons, General Counsel, Dallas Area Rapid Transit, Legal Department wrote an article entitled COMPUTER FORENSICS ON A BUDGET, for the State Bar of Texas 19th Annual Suing and Defending Governmental Entities Course, July, 2007 and stated the following:

Computer forensics involves the scientific study (preservation, collection, analysis, etc) of computers and

electronic data in a manner that is consistent with the principles of the rules of evidence and rules of procedure.

See Michael Scheetz, *COMPUTER FORENSICS: AN ESSENTIAL GUIDE FOR ACCOUNTANTS, LAWYERS, AND MANAGERS*, p. 2, 25 (Wiley & Sons, Inc., 2007).

Therefore, the person who performs computer forensics is often highly trained in both law and computer science. See Robert C. Newman, *COMPUTER FORENSICS: EVIDENCE COLLECTION AND MANAGEMENT*, pp. 130 - 135; pp. 325 - 338 (Taylor & Francis Group, 2007). In Texas, this person may also be required to have a private investigator's license. See TEX. OCC. CODE ANN. §§ 1702.002 (18), 1702.104(2), together with TEX. GOV'T. CODE ANN. § 311.005(2); TEX. OCC. CODE ANN. §§ 1702.002 (16), 1702.321, 1702.322. The Texas Department of Public Safety, Regulatory Licensing issued two opinions that many courts, lawyers, lay persons and even computer forensic experts are unaware of and they are as follows:

Computer Forensics August 21, 2007

The computer forensics industry has requested clarification of the Private Security Bureau's position regarding whether the services commonly associated with computer forensics constitute those of an "investigations company"

USING ELECTRONIC EVIDENCE

and are therefore services regulated under the Private Security Act (Chapter 1702 of the Occupations Code). It is hoped that the following will be of assistance.

First, the distinction between “computer forensics” and “data acquisition” is significant. We understand the term “computer forensics” to refer to the *analysis* of computer-based data, particularly hidden, temporary, deleted, protected or encrypted files, for the purpose of discovering information related (generally) to the causes of events or the conduct of persons. We would distinguish such a content-based analysis from the mere scanning, retrieval and reproduction of data associated with electronic discovery or litigation support services.

For example, when the service provider is charged with reviewing the client’s computer-based data for evidence of employee malfeasance, and a report is produced that describes the computer-related activities of an employee, it has conducted an investigation and has therefore provided a regulated service. On the other hand, if the company simply collects and processes electronic data (whether in the form of hidden, deleted, encrypted files, or otherwise), and provides it to the client in a form

that can then be reviewed and analysed for content by others (such as by an attorney or an investigator), then no regulated service has been provided.

The Private Security Act construes an investigator as one who obtains information related to the “identity, habits, business, occupation, knowledge, efficiency, loyalty, movement, location, affiliations, associations, transactions, acts, reputation, or character of a person; the location, disposition, or recovery of lost or stolen property; the cause or responsibility for a fire, libel, loss, accident, damage, or injury to a person or to property; or for the purpose of securing evidence for use in court.” Tex. Occ. Code §1702.104. Consequently, we would conclude that the provider of computer forensic services must be licensed as an investigator, insofar as the service involves the analysis of the data for the purposes described above.

With respect to the statutory reference to “securing evidence for use in court,” we would suggest that the mere accumulation of data, or even the organization and cataloguing of data for discovery purposes, is not a regulated service. Rather, in this context, the Bureau would interpret the reference to “evidence” as referring to the *report* of the computer forensic examiner, not the data itself. The acquisition of the data, for evidentiary purposes, precedes the analysis by the computer forensic examiner, insofar as it is raw and unanalyzed. The mere collection and organization of the evidence into a form that can be reviewed and analysed by others is not the “securing of evidence” contemplated by the statute.

USING ELECTRONIC EVIDENCE

This analysis is consistent with the language of HB 2833 (Tex. Leg. 80th Session), which amends Section 1702.104. The amendment confirms that the “information” referred to in the statute “includes information obtained or furnished through the review and analysis of, and the investigation into the content of, computer-based data not available to the public.”

It may well be that the hardware on which the data exists is itself the product of an investigation, but that is a separate question. Rev 01-15-08

Computer Repair & Technical Assistance Services, October 18, 2007

Computer repair or support services should be aware that if they offer to perform investigative services, such as assisting a customer with solving a computer-related crime, they must be licensed as investigators. The review of computer data for the purpose of investigating potential criminal or civil matters is a regulated activity under Chapter 1702 of the Texas Occupations Code, as is offering to perform such services. Section 1702.102 provides as follows:

§1702.104. Investigations Company

(a) A person acts as an investigations company for the purposes of this chapter if the person:

(1) engages in the business of obtaining or furnishing, or accepts employment to obtain or furnish, information related to:

(A) crime or wrongs done or threatened against a state or the United States;

(B) the identity, habits, business, occupation, knowledge, efficiency, loyalty, movement, location, affiliations, associations, transactions, acts, reputation, or character of a person;

(C) the location, disposition, or recovery of lost or stolen property; or

(D) the cause or responsibility for a fire, libel, loss, accident, damage, or injury to a person or to property;

(2) engages in the business of securing, or accepts employment to secure, evidence for use before a court, board, officer, or investigating committee;

(3) engages in the business of securing, or accepts employment to secure, the electronic tracking of the location of an individual or motor vehicle other than for criminal justice purposes by or on behalf of a governmental entity; or

(4) engages in the business of protecting, or accepts employment to protect, an individual from bodily harm through the use of a personal protection officer.

USING ELECTRONIC EVIDENCE

(b) For purposes of subsection (a)(1), obtaining or furnishing information includes information obtained or furnished through the review and analysis of, and the investigation into the content of, computer-based data not available to the public. Please be aware that providing or offering to provide a regulated service without a license is a criminal offense. TEX. OCC. CODE §§1702. 101, 1702.388. Employment of an unlicensed individual who is required to be licensed is also a criminal offense. TEX. OCC. CODE §1702.386.

As important as Chapter 1702 of the Texas Occupations Code is, such individuals who are not licensed are subject to:

§ 1702.388. VIOLATION OF CHAPTER ; OFFENSE. (a) A person commits an offense if the person violates a provision of this chapter for which a specific criminal penalty is not prescribed.

(b) An offense under this section is a Class A misdemeanor, except that the offense is a felony of the third degree if the person has previously been

convicted under this chapter of failing to hold a license, registration, certificate, or commission that the person is required to hold under this chapter. Acts 1999, 76th Leg., ch. 388, § 1, eff. Sept. 1, 1999.

§ 1702.386 . UNAUTHORIZED EMPLOYMENT ; OFFENSE. (a) A person commits an offense if the person contracts with or employs a person who is required to hold a license, registration, certificate, or commission under this chapter knowing that the person does not hold the required license, registration, certificate, or commission or who otherwise, at the time of contract or employment, is in violation of this chapter.

(b) An offense under Subsection (a) is a Class A misdemeanor.

Class A misdemeanors in Texas have the following penalties:

- Confinement for term not to exceed 1 year in county jail; and/or
- A fine not to exceed \$2,000
- Up to 2 years of Community Supervision or 3 years with extension

USING ELECTRONIC EVIDENCE

Consider the following from House Bill 2833 which just amended the statute:

§ 1702.381. CIVIL PENALTY. (a) A person who is not licensed under this chapter, who does not have a license application pending, and who violates this chapter may be assessed a civil penalty to be paid to the state not to exceed \$10,000 for each violation.

(b) A person who contracts with or employs a person who is required to hold a license, certificate of registration, or security officer commission under this chapter knowing that the person does not hold the required license, certificate, or commission or who otherwise, at the time of contract or employment, is in violation of this chapter may be assessed a civil penalty to be paid to the state in an amount not to exceed \$10,000 for each violation.

(c) A civil penalty under this section may be assessed against a person on proof that the person has received at least 30 days' notice of the requirements of this section.

Get out the Miranda Card!

As if things are not confusing enough, in July, 2007 the Board issued the following opinion:

Litigation Support & Document Retrieval Industry. July 26, 2007

This is in response to a request for an opinion letter regarding whether the changes to Section 1702.104 affected by House Bill 2833 apply to the above-referenced businesses.

The concern was with the following language, added as subsection (b) to 1702.104:

For purposes of subsection (a)(1), obtaining or furnishing information includes information obtained or furnished through the review and analysis of, and the investigation into the content of, computer-based data not available to the public.

Specifically, the question was asked whether this subsection would apply to the provision of "electronic data discovery" services to the legal and corporate community, such that a license would be required under the Private Security Act (Chapter 1702 of the Texas Occupations Code).

Of course, the phrase 'electronic data discovery' encompasses many activities, some of which may require licensure. However, if:

USING ELECTRONIC EVIDENCE

1. The company does not obtain or secure data by way of an investigative analysis;
2. Does not analyse or review the content of the data;
3. Processes the data (provided by others) in order to create a database that can be searched by the lawyer/clients; and/or
4. Reproduce or retrieve the documents or images upon request of the clients;

Then it would appear that the company is not engaging in activities for which a private investigations company license is required.

Meaning a basic backup or image copy does not require a license, but if as the person compares the original with an image to confirm he or she made a duplicate original backup that might/would require a license.

So be careful in the employment of computer forensic experts. Unanswered by the board is would a computer forensic company like Kroll located in Minnesota be required to have its technicians licensed, but the gotcha is the statute applies to those who employ said computer experts, which means possible prosecution for a Texas resident.

B. Rules of Evidence and Procedure Apply to Electronic Evidence.

1. Authentication

Electronic evidence is not inherently different than other evidence. Authentication and a finding of a

hearsay exception is necessary to get the evidence admitted. *Longoria v. Greyhound Bus Lines, Inc.*, 699 S.W.2d 298, 302 (Tex. App.—San Antonio 1985, no writ) (computerized 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). Evidence is not admissible unless it has been authenticated. The requirement of authentication as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. TEX. R. EVID. 901(a).

2. Self-Authentication

Some documents are self-authenticated and extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

- (1) Domestic Public Documents Under Seal.
- (2) Domestic Public documents Not Under Seal.
- (3) Foreign Public Documents. See *Wolfe v. Wolfe*, 918 S.W.2d 533, 542 (Tex. App.—El Paso 1996, writ denied) (opinion of New Zealand court containing statements chastising wife's behaviour admissible as authenticated foreign judgment under Rule 902(3) in divorce case.).
- (4) Certified Copies of Public Records.
- (5) Official Publications.
- (6) Newspapers and Periodicals.

USING ELECTRONIC EVIDENCE

- (7) Trade Inscriptions and the Like.
- (8) Acknowledged Documents.
- (9) Commercial Paper and Related Documents.
- (10) Business Records Accompanied by Affidavit.

TEX. R. EVID. 902.

Additionally, the discovery rules may assist in the authentication of electronic data that has been produced by the other side in discovery. Texas Rule of Civil Procedure 193.7 creates a presumption of authenticity for documents produced in response to a request for written discovery, if not objected to within ten days after the producing party has actual notice that the document will be used. TEX. R. CIV. P. 193.7. Therefore, if a party produces a printed e-mail message through written discovery, the party to whom the email was given may not be required to authenticate the message. 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).

While at one time 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.), any general requirement for proving up the validity of the computing process for business records has been abandoned.

Courts now agree that computerized business records can be proved up in the same manner as handwritten 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 admissible if requirements for business records are met); *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); *Hutchison 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); *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 human being).

The following are additional Texas Cases addressing authentication:

Davidson v. Great National Life Ins. Co., 737 S.W.2d 312, 314-15 (Tex. 1987) (Photograph admissible upon sponsoring witness' testimony that photograph is "an accurate portrayal of the facts, and on verification by that witness or a person with knowledge that the photograph is a correct representation of such facts.").

USING ELECTRONIC EVIDENCE

Seymour v. Gillespie, 608 S.W.2d 897, 898 (Tex. 1980) (Tape recordings that fairly represent conversations admissible as fair representation. Elements of fair representation:

- (1) recording device capable of recording;
- (2) operator competent;
- (3) recording authentic and correct;
- (4) no changes, deletions, or additions;
- (5) properly preserved;
- (6) speaker identified; and
- (7) statement made voluntarily without inducement).

Mega Child Care, Inc. v. DPRS, 29 S.W.3d 303, 308, 312 (Tex. App.—Houston [14th Dist.] 2000 no pet.) (“The Texas rules of Evidence require, as a predicate to admissibility, that evidence be properly authenticated or identified. . . . In other words, the proponent must show the trial court that the document or evidence in question is what he purports it to be. . . . Authentication may be accomplished by various means; one example offered by Rule 901 is where the evidence is authenticated by the testimony of a witness with knowledge. . . . [A] nonexistent document or document entry, by definition, cannot be authenticated; it does not exist, and no authentication is required.”) *S.D.G. v. State*, 936 S.W.2d 371, 381 (Tex. App.—Houston [1st Dist.] 1996, writ denied) (predicate for introduction of videotape without sound recording same as for photograph: (1) accurate and correct presentation; and (2) relevant predicate does not need to be provided by photographer, person photographed, or person present when photograph was made.

“Any witness who observed the object or scene depicted in the photograph may lay the predicate.” Trial judge has “considerable discretion in ruling on the admissibility of photography evidence.”). *Grossnickle v. Grossnickle*, 935 S.W.2d 830, 848 (Tex. App.—Texarkana 1996, writ denied) (American Express receipts admitted into evidence in case involving contested property division in attempt to prove amounts husband spent on girlfriend.). *Reichold Chemicals v. Puremco Mfg.*, 854 S.W.2d 240, 248 (Tex. App.—Waco 1993, writ denied) (photographs admissible upon proof that sponsoring witness has personal knowledge of accuracy of objects and events shown in photograph.)

Kotrla v. Kotrla, 718 S.W.2d 853, 855 (Tex. App.—Corpus Christi 1986, writ ref’d n.r.e.) (husband’s tape recording of wife admitting to having used cocaine and having grown marijuana held admissible in divorce case in which husband received sole managing conservatorship of child.). *Mata v. Mata*, 710 S.W.2d 756, 759 (Tex.App.—Corpus Christi 1986, no writ) (wife introduced photographs of “interior of the house with its furnishings” in support of her testimony regarding value of furnishings.).

3. Best Evidence Rule.

The “best evidence rule” provides that to prove the content of a writing, recording, or photograph, the original writing, recording or photograph is required. TEX. R. EVID. 1002. A duplicate may be used unless (1) a question is raised as to the authenticity of the original, or (2) the use of the duplicate in lieu of the original under the circumstances would be unfair. *Tex.R. Evid. 1003*.

USING ELECTRONIC EVIDENCE

An original is not required if: (1) the original has been lost or destroyed (except by the offering party in bad faith); (2) no original can be obtained by any available judicial process or procedure; (3) no original is located Texas, or (4) the opponent, after having been put on notice of the need for the original, does not produce it. Tex. R. Evid. 1004.

Texas Rule of Evidence 1001(c) provides that “[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original’.”

Consider just a plain old photograph, a common piece of evidence offered thousands of times daily throughout this country in a multitude of legal settings. Would it be important to know if it was taken by a digital camera versus a traditional let’s say 35MM film camera. If so what questions arise when it’s taken by a digital camera and an objection is made as to “best evidence”.

4. The Hearsay Rule.

Hearsay is not admissible except as provided by statute or the rules of evidence or by other rules prescribed pursuant to statutory authority. TEX. R.EVID. 802. Inadmissible hearsay admitted without objection shall not be denied probative value merely because it is hearsay. *Id.*

(4) Hearsay is “a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.” TEX. R. EVID. 801(d).

By definition, a “prior statement by witness,” admission of a party opponent,” and “depositions” in the same case are not hearsay. TEX. R. EVID. 801(e). A “statement is (i) an oral or written verbal expression or (ii) nonverbal conduct of a person that is intended to substitute for a verbal expression. TEX. R. EVID. 801(a). A “declarant” is a person who makes a statement. TEX. R.EVID. 801(b).

Hearsay is defined as a statement of a person.

TEX. R. EVID. 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. Human communications stored on a computer, must be distinguished from human communications processed by a computer and 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), which involved a prosecution for harmful access to a computer, the court held that information displayed by computer was not hearsay, because it was not an out of-court statement made by a *person*. 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 *Burleson* court cited two out-of-state cases. In *People v. Holowko*, 109 Ill.2d 197, 93 Ill. Dec. 344, 486 N.E.2d 877, 878-79 (1985), the Illinois Supreme Court held that computerized

USING ELECTRONIC EVIDENCE

printouts of phone traces were not hearsay because such printouts did not rely on the assistance, observations, or reports of a human declarant. The printout 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. An e-mail is an out-of-court statement, and is potentially hearsay. An e-mail is not hearsay if it is not offered for the truth of the matter asserted under Rule of Evidence 801(c) and (d), or if it is an admission of a party opponent under Rule of Evidence 801(e)(2). If the e-mail is hearsay, then the proponent must find an exception to the hearsay rule that applies.

5. Business Records Exception to Hearsay Rule.

The business records exception to the hearsay rule includes computer records. Copies of business records can be authenticated by the testimony of the custodian of the records or other qualified witness. See TEX. R. EVID. 803(6). Authentication can also be done by affidavit, as provided in Rule 902(10) of the Texas Rules of Evidence.

Computerized business records can be proved up in the same manner as handwritten 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 admissible if requirements for business records are met); see also, *Longoria v.*

Greyhound Bus Lines, Inc., 699 S.W.2d 298, 302 (Tex. App.—San Antonio 1985, no writ) (computerized 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). See, Robert S. Hoffman, EVIDENCE AND DISCOVERY IN FAMILY LAW, State Bar of Texas, 17th Annual Advanced Evidence & Discovery Course, April 1-2, 2004 – Dallas.

6 Other issues- Privacy Concerns

Privacy concerns are also an issue with electronic discovery. What happens, for example, when the opposing party requests an entire database or seeks to image an entire hard drive, which would reveal what web sites have been visited and any other privately stored information? While there is no clear holding on this issue, the Texas Supreme Court has intimated that the broad scope of discovery must sometimes be narrowed to account for privacy concerns. In *In re Ci Host, Inc. v. Creative Innovations, Inc.*, 92 S.W.3d 514, (2002), the Texas Supreme Court considered a trial court order to produce all backup tapes, even though some tapes contained protected information and e-mails that may be considered confidential by some of the business’s customers. Although the business had waived its objections to the discovery request, the court maintained that it was “loath to allow [the business] to unilaterally waive its customers’ privacy rights by its failing to adhere to the discovery rules.” *Id.* at 517 (citing *Eli Lilly & Co. v. Marshall*, 850 S.W.2d 155,

USING ELECTRONIC EVIDENCE

160 (Tex. 1993). It therefore denied a writ of mandamus to order production in order to allow the trial court and parties to address the privacy considerations. See, Judge Xavier Rodriguez, THE MANY CHALLENGES PRESENTED BY ELECTRONIC DISCOVERY, State Bar of Texas, 19th Annual Advanced Evidence and Discovery Course, April 26-27, 2006 – Houston

challenge for judges, practitioners and litigants for many years to come.

Reggy Hirsch
Metadata partially removed©

7. Last Thoughts

The partial contents of a hard drive are admitted and opposing counsel says "Your honor, objection 'optional completeness.'" – scary right©

C. Rule 107. Rule of Optional Completeness

When part of an act, declaration, conversation, writing or recorded statement is given in evidence by one party, the whole on the same subject may be inquired into by the other, and any other act, declaration, writing or recorded statement which is necessary to make it fully understood or to explain the same may also be given in evidence, as when a letter is read, all letters on the same subject between the same parties may be given. "Writing or recorded statement" includes depositions.

V. Conclusion

Well hopefully the antacids have taken effect, the aspirin has kicked in and the nausea dissipated. The world of electronic evidence is as complex as a field of law as it is a complex field of science and the future will remain a

USING ELECTRONIC EVIDENCE

EXHIBIT A

AVERAGE NUMBER OF PAGES PER GIGABYTE AND MEGABYTE

Document Type	Average Pages/Doc	Average Pages/GB	Average Pages/MB
Microsoft Word	8	64,782	63
Email	1.5	100,000	97
Microsoft Excel	50	165,791	161
Lotus 1-2-3	55	287,317	280
Microsoft	14	17,552	17
Power Point Text	20	677,963	662
Image	14	15,477	15