HIGH TECH EVIDENCE:
HOW TO FIND IT, RETRIEVE IT, AND GET IT IN

EDWIN J. (TED) TERRY
JAMES A. VAUGHT
KARL E. HAYS
Law Offices of
Edwin J. (Ted) Terry, Jr.
805 W. 10th Street, Suite 300
Austin, Texas 78701
Telephone: (512) 476-9597
Fax: (512) 476-6106

JAMES LARUE
103 Mesa View, #2
Grand Junction, CO 81503
(970) 245-6158
email: 102236.502@compuserve.com

STATE BAR OF TEXAS
28TH ANNUAL ADVANCED FAMILY LAW COURSE
August 5-8, 2002
Dallas, Texas
Chapter 41

Edwin J.(Ted)Terry, Jr.

Law Office of Edwin J.(Ted)Terry, Jr. Established 1975
805 West 10th Street Austin, Texas 78701 (512) 476-9597 Fax (512) 476-6106

EDUCATION University of Texas, B.A. in History, 1972
St. Mary's University, J.D., 1975

LICENSED Admitted to the United States Supreme Court
Admitted to the United States Federal District Court for the Western District of Texas
Board Certified by the Texas Board of Legal Specialization-Family Law 1981
Recertified in Family Law 1986,1991,1996 and 2001

PROFESSIONAL ASSOCIATIONS

American Board of Trial Advocates-Associate
American Bar Association- Family Law Section
Chapter member, Texas Family Law Foundation
Fellow-American Academy of Matrimonial Lawyers
Fellow-International Academy of Matrimonial Lawyers
Member, Family Law Council - term expires 2005
Member, Capital Area Trial Lawyers Association
Member, Williamson County Bar Association
President, American Academy of Matrimonial Lawyers-Texas Chapter
President of Travis County Family Law Advocates 1999-2000
State Bar of Texas -Family Law Section -Appellate Section
Member, Texas Academy of Family Law Specialists
Travis County Bar Association-Family Law Section-Appellate Section
Treasurer, Travis County Family Law Advocates-Political Action Committee 1999-2002
Member, Texas Trial Lawyers Association
Screening Committee Travis County Family Law Advocates-Political Action Committee -1999-2002

HONORS

Americas Top Lawyers 2001-2002- Family Law Section
The Best Lawyers in America- Family Law 1999-2002
Martindale-Hubbell-"AV" rating
Martindale-Hubbell Bar Register of Preeminent Lawyers

COMMITTEES & RESPONSIBILITIES

Planning Committee for 1994, 2000, 2001 and 2002 Advanced Family Law Seminar
Planning Committee for 1998, 2001 and 2002 New Frontiers in Marital Property Law Seminar
Planning Committee Marriage Dissolution Institute - 1998,1999,2000 and 2002
Co-Course Director, Family Law on the Front Lines Conference 2001 and 2002
Course Director- Ultimate Trial Notebook Family Law - 2000

Chair, Interdisciplinary Relations on Mental Health Committee-
1997, 1998, 1999, 2000 and 2001 - American Academy of Matrimonial Lawyers
Member of Newsletter Committee - American Academy of Matrimonial Lawyers
Member of the Foundation of the American Academy of Matrimonial Lawyers
Course Director-American Academy of Matrimonial Lawyers, Texas Chapter, Survival Retreat-2001
Chapter Leader, November 2001 Conference, American Academy of Matrimonial Lawyers
American Academy of Matrimonial Lawyers Social Function Committee 2002.
Nominating Committee - Family Law Council-2001
Membership Committee - Family Law Council 2001-2002
Co-Chair of Amicus Curiae Committee - Family Law Council 2001-2002
Chair, Texas Association of Family Law Specialists Legislative Oversight Committee -1999

ARTICLES CITED BY STATE SUPREME COURTS

Lenz v. Lenz, 45 Tex. Sup. Ct. J. 781, 783-84 (June 6, 2002), citing
"Relocation: Moving Forward or Moving Backward?",
31 Tex. Tech. L. Rev. 983 (2000).

Torrington Co. v. Stutzman, 46 S.W.3d 829, 839 (Tex. 2000), citing
"Trends in Preservation of Error (At Trial, Charge, and Post Verdict),"
13th Annual Advanced Civil Appellate Practice Course, State Bar of Texas,
Austin, Texas, October 1999.

Brown v. Brown, 621 N.W.2d 70, 79 (Neb. 2000), citing
"Relocation: Moving Forward or Moving Backward?",
15 Journal of American Academy of Matrimonial Lawyers 701 (Spring 1999).

Baures v. Lewis, 770 A.2d 214, 222 (N.J. 2001), citing
"Relocation: Moving Forward or Moving Backward?",
31 Tex. Tech. L. Rev. 983 (2000).

CLE ACTIVITY- SPEECHES, PANELS, & ARTICLES

INTERNATIONAL ACADEMY OF MATRIMONIAL LAWYERS

"Fiduciary Duties of Spouses and Non-Physical Torts", International Academy of Matrimonial Lawyers, Palm Beach, Florida, March 2000.

AMERICAN ACADEMY OF MATRIMONIAL LAWYERS

"Early-Stage Company Valuation,"American Institute of Certified Public Accountants/American Academy of Matrimonial Lawyers National Conference, Las Vegas, Nevada, May 2002.

"Issues Unique to Early-Stage Companies: Property and Support Conundrum,"American Institute of Certified Public Accountants/American Academy of Matrimonial Lawyers National Conference, Las Vegas, Nevada, May 2002.

"Valuation of Law Practice in Divorce", American Academy of Matrimonial Lawyers, Sanibel, Florida, 2002.

"Mental Health Professionals and the Legal System Including Ethical Issues," American Academy of Matrimonial Lawyers, Chicago, Illinois, November 1998.

"Relocation: Moving Forward, or Moving Backward?," American Academy of Matrimonial Lawyers Annual Conference, Chicago, Illinois, November 1996.

NEW FRONTIER'S MARITAL PROPERTY

LAW

"Valuation, Characterization and Division of Unusual Assets", New Frontiers in Marital Property Law, Santa Fe, New Mexico, October 2001.

"Pretrial and Trial Strategies for the Complex Property Case", New Frontiers in Marital Property Law, Santa Fe, New Mexico, October 2000.

"Strategic Use of Law Beyond the Family Code", New Frontiers in Marital Property Law, San Diego, California, October 1999.

"Fiduciary Duties of Spouses, Effective Use of the Remedy of the Constructive Trust, Recoveries for Violations of these Duties, and Issues Presented When Spouses are Under Multiple and/or Conflicting Duties," New Frontiers in Marital Property Law, Santa Fe, New Mexico, October 1998.

"Dealing With Special Problems Relevant to Evaluation & Division of Professional Practices," Second Annual New Frontiers in Marital Property Law, San Diego, California, October 1997.

ADVANCED FAMILY LAW:

"Contesting and Defending Pre-marital Agreements" 28th Annual Advanced Family Law Course, Dallas, Texas August 2002.

"High Tech Evidence: How to Find It, Retrieve It and Get It In" 28th Annual Advanced Family Law Course, Dallas, Texas August 2002.

"Termination and Adoption: It Ain't Over Till It's Over" 28th Annual Advanced Family Law Course, Dallas, Texas August 2002.

"Professional Partings: Valuing Medical/Legal Professional Practices", 27th Annual Advanced Family Law Course, San Antonio, Texas, August 2001.

"Dealing with Mobile Parents: Domicile Restrictions and Relocations", Advanced Family Law Course, San Antonio, Texas, August 2001.

"Representing the High Tech Entrepreneur: IPO's, Venture Capitalists and Beyond", 26th Annual Advanced Family Law Course, San Antonio, Texas, August 2000.

"Family Law Court v. Probate Court: What Every Family Lawyer Should Know," 26th Annual Advanced Family Law Course, San Antonio, Texas, August 2000.

"The Appellate Process-the Good, the Bad, and the Ugly", 25th Annual Advanced Family Law Course, Dallas, Texas, August 1999.

"Breach of Fiduciary Duty and Nonphysical Tort Claims," Annual Advanced Family Law Course, San Antonio, Texas, August 1998.

"The Ab(use) of the Rules of Evidence and Privileges," Advanced Family Law Course, San Antonio, Texas, August 1997.

"Whose Kids are They Anyway? Reporting Child Abuse: Counterpoint - A Lawyer has a Duty to Report Child Abuse," State Bar of Texas Annual Meeting, Houston, Texas, June, 1997 and Advanced Family Law Course, San Antonio, Texas, August 1997.

"Recent Development in Custody Law", State Bar of Texas, Advanced Family Law Seminar, March 1997.

"Piercing Claims of Immunity in Family Law Litigation," Advanced Family Law Course, San Antonio, Texas, 1994.

"Getting and Characterizing Punitive Damages in Family Law Litigation," Advanced Family Law Course, San Antonio, Texas, August 1994.

ADVANCED CIVIL APPELLATE

"Trends in Preservation of Error (At Trial, Charge, and Post Verdict)," 13th Annual Advanced Civil Appellate Practice Course, State Bar of Texas, Austin, Texas, October 1999.

MARRIAGE DISSOLUTION

"Summary Judgments and Declaratory Judgments in Divorce", Marriage Dissolution Seminar, Austin, Texas, May 2002.

"Termination and Adoption: It Ain't Over Till It's Over", Marriage Dissolution Seminar, Austin, Texas, May 2002.

"Valuing and Dividing the Community Business, Marriage Dissolution Seminar, Corpus Christi,

Texas, May 2001.

"Bill of Review," 23rd Annual Marriage Dissolution Seminar, Fort Worth, Texas, May 2000.

"Sex and Lies: A Daubert Challenge, Techniques for Presenting the Child's Testimony to the Trial Court in a Child Abuse Case," 23rd Annual Marriage Dissolution Seminar, Fort Worth, Texas, May 2000.

"Appellate Tips: Judges Panel," 23rd Annual Marriage Dissolution Seminar, Fort Worth, Texas, May 2000.

"Litigating Marital Agreements: "You can't always get what you want....",22nd Annual Marriage Dissolution Institute, San Antonio, Texas, May 1999.

"Handling the Divorce Involving a Medical Practice," Marriage Dissolution Conference, Austin, Texas, May, 1998.

"Scratches on the Heart: Non-Physical Tort Claims," Marriage Dissolution Conference, Dallas, Texas, May, 1997.

"The Effective Use of the New Conservator Rights Responsibilities and Duties in a Custody Case," Marriage Dissolution Conference, South Padre Island, Texas, 1994.

TEXAS ACADEMY OF FAMILY LAW SPECIALISTS

"Presenting the Child's Perspective: Techniques for Presenting the Child's Preference of Conservator to the Trial Court," Texas Academy of Family Law Specialists, Las Vegas, Nevada, February 2000.

TEXAS TRIAL LAWYERS ASSOCIATION

"Conflicts Between Personal Injury and Family Law," Texas Trial Lawyers Association, Austin, Texas, February 1999.

"How Much Is Your Law Practice Worth? Valuing Personal Injury Law Practices for Purposes of Divorce," Texas Trial Lawyers Association, Dynamic Advocacy Seminar, Whitefish Montana, July, 1998.

"Discussion of Texas Supreme Court Cases Involving Tort Claims of Emotional Distress," joint meeting of Travis County Trial Lawyers and Travis County Women's Bar, Austin, Texas, 1994.

"Divorce & Emotional Distress: Custer's Last Stand,"1992.

UNIVERSITY OF TEXAS COURSES

"Child Support Collection: A Practical Guide to the Opportunities and Pitfalls in Enforcing and Defending Child Support Obligations," Family Law on the Front Lines, Galveston, Texas, April 2002.

"District Judges Panel: 10 Bad Things that Good Lawyers Do," Family Law on the Front Lines, Galveston, Texas, April 2002.

"Interaction of Probate Court and Family Law," Family Law on the Front Lines, Galveston, Texas, April 2001.

"Daubert: Experts & Admissibility" Family Law on the Front Lines, The University of Texas School of Law, April 2001.

"Domestic Tort Liability and Characterization of Damages," Texas Marital Property Institute, Austin, Texas, October, 1997.

STATE BAR OF TEXAS COURSES

"Playing By the Rules," Winning Techniques in Family Law Litigation: Mastering the Challenge, Houston, Texas, December 1998.

"Emerging Issues in Custody Litigation," 1997 State Bar of Texas Legal Assistant Division Advanced Family Law Seminar, Austin, Texas, March, 1997.

"Changes in Texas Family Law," The College of the State Bar of Texas, Austin, Texas, 1994.

"Sharpening Negotiating Skills - Your Key to Success," State Bar of Texas, Women's Law Section, Austin, Texas, 1990.

"Mothers Without Custody," San Francisco, California, 1987.

"Child Abuse - The Quiet Crime," State Bar of Texas, San Antonio, Texas, 1985.

"Post Divorce, Modification of Conservatorship and Support Orders in Divorce," 1984: Division of Property and Decisions on Children, El Paso, Texas 1984.

"Bottom Line Appellate Issues," Ultimate Trial Notebook: Family Law, New Orleans, Louisiana, December 2000.

"The Social Worker: Learning from Your Expert What to Ask," Ultimate Trial Notebook: Family Law, Austin, Texas, 1994.

ASSOCIATION OF FAMILY AND CONCILIATION COURTS

"Parental Relocation Disputes: An Interdisciplinary Approach to Resolution," Second World Congress on Family Law and the Rights of Children and Youth with the 1997 Annual Conference of the Association of Family and Conciliation Courts, San Francisco, California, June, 1997.

"Gender Issues in Domestic Torts," Association of Family and Conciliation Courts, Montreal, Canada, May 1995.

SPEAKER/AUTHOR VARIOUS COURSES

"Grandparents Rights after *Troxel*" Capital Area Paralegal Association, Austin, Texas, January 2002.

Summary of the 1999 amendments to the Texas Family Code," Legal Assistant U, San Antonio, Texas, September 1999.

"Trying Jury Cases Under the Amendments to the Texas Family Code and the New Texas Pattern Jury Charge," Travis County Family Law Section Meeting, April 1996.

"What Attorneys Expect from an Appraiser in a Divorce Situation," American Society of Appraisers, Austin, Texas, November 1995.

"Complex Family Law Litigation, Interspousal Tort Claims," Texas College of Advanced Judicial Studies, 1993.

"Changes in the Family Code," Travis County Family Law Section Meeting, Austin, Texas, 1993.

Travis County Bar Association Third Annual Jury Selection Seminar, Family Law Voir Dire Demonstration, 1993.

"Issues Particular to the Appeal of Family Law Cases in Texas," Civil Appellate Seminar, Austin, Texas, April, 1994.

Travis County Bar Association Second Annual Jury Selection Seminar, Family Law Voir Dire Demonstration, 1992.

Travis County Domestic Relations Division - Child Custody Litigation, 1990.

"Child Custody Litigation," Tarrant County Bar Association, Fort Worth, Texas, 1990.

VARIOUS PUBLICATIONS

"Overview of the New Uniform Child Custody Jurisdiction Enforcement Act," The Newsletter of the American Academy of Matrimonial Lawyers, Winter 2000.

"Targeted by the Opposing Party; The Tort of Negligent Misrepresentation Applied to Divorce Lawyers," Texas Lawyer, December 1999.

"Relocation: Moving Forward or Moving Backward?", 15 Journal of American Academy of Matrimonial Lawyers 701 (Spring 1999).

"The Fiduciary Duty Between Spouses, A Look at "Fraud on the Community," Texas Lawyer, October, 1998.

"Torts in Texas the New Frontier," Texas Trial Lawyers Forum, 1992.

"Infliction of Emotional Distress: No Justice in the Middle Ground," Texas Trial Lawyers Forum, 1992.

"Evaluation and Division of Professional Goodwill and Professional Degrees During Marriage," Texas Trial Lawyers Forum, 1985.

Co-Author with Dan Price, "Post Divorce, Modification of Conservatorship and Support Orders in Divorce," Division of Property and Decisions on Children, 1984.

JAMES A. VAUGHT

Law Offices of Edwin J. (Ted) Terry, Jr.
805 West 10th Street
2nd Floor, Suite 300
Austin, Texas 78701
(512) 476-9597
(512) 476-6106 facsimile
e-mail: jvaught@tedterry.com

PROFESSIONAL ACTIVITIES

Law Offices of Edwin J. (Ted) Terry, Jr.

Board Certified, Civil Appellate Law (1988-present)
Board Certified, Family Law (2000-present)
Texas Board of Legal Specialization

LICENSED TO PRACTICE

The Supreme Court of Texas
The Supreme Court of the United States
The United States Courts of Appeals for the Fifth and Eighth Circuits
United States Federal District Court for the Western District of Texas

PROFESSIONAL MEMBERSHIPS & HONORS

Martindale-Hubbell - "AV" rating
Martingale-Hubbell Bar Register of Preeminent Lawyers

Member, Association of Attorney-Mediators

Member, Planning Committee, Family Law on the Front Lines (2001, 2002)

Member, Planning Committee, The Ultimate Trial Notebook - Family Law (2000)

Associate Chair, Family Law on the Front Lines (2002)

Member, Planning Committee, Fifth, Sixth, Ninth, Tenth, Eleventh and Thirteenth Annual Advanced Civil Appellate Practice Courses (1991-92, 1995-97, 1999)

Member, Planning Committee, University of Texas School of Law, First, Second and Third Annual Insurance Law Institutes (1996-98)

Member, Editorial Board, APPELLATE ADVOCATE, State Bar Appellate Practice & Advocacy Section 1994-97

Member, Council, State Bar Appellate Practice & Advocacy Section 1995-1998

Member, Task Force on Staff Diversity, Texas Commission on Judicial Efficiency 1995-96

Chair, Civil Appellate Law Section, Travis County Bar Association November 1991-1993, 1995-1997

Texas Academy of Family Law Specialists

Secretary/Treasurer, Travis County Family Law Advocates 2001-

Member, Travis County Bar Association Board of Directors
November 1991-1993, 1995-1997

Member, Planning Committee, Primer for Handling Civil Appeals,
Travis County Bar Association, Austin 1995, 1996

Staff Attorney, Hon. Jack Hightower, Justice
The Supreme Court of Texas 1989-1995

EDUCATION

Baylor University School of Law J.D., *cum laude* 1980

University of Texas B.A. 1974

SELECTED LAW RELATED PUBLICATIONS & PRESENTATIONS

"Contesting and Defending Premarital Agreements", 28th Annual Advanced Family Law Course, Dallas, Texas, August 2002.

"High Tech Evidence: How to Find It, Retrieve It and Get It In", 28th Annual Advanced Family Law Course, Dallas, Texas, August 2002.

"Termination and Adoption: It Ain't Over Till It's Over", 28th Annual Advanced Family Law Course, Dallas, Texas, August 2002.

"Early-Stage Company Valuation"American Institute of Certified Public Accountants/American Academy of Matrimonial Lawyers National Conference, Las Vegas, Nevada, May 2002.

"Summary Judgments and Declaratory Judgments in Divorce", Marriage Dissolution Seminar, Austin, Texas, May 2002.

"Termination and Adoption: It Ain't Over Till It's Over", Marriage Dissolution Seminar, Austin, Texas, May 2002.

"Child Support Collection: A Practical Guide to the Opportunities and Pitfalls in Enforcing and Defending Child Support Obligations," Family Law on the Front Lines, Galveston, Texas, April 2002.

"Valuation of Law Practice in Divorce," American Academy of Matrimonial Lawyers, Sanibel, Florida March 2002.

"Valuation, Characterization and Division of Unusual Assets", New Frontiers in Marital Property Law, Santa Fe, New Mexico, October 2001.

"Professional Partings: Valuing Medical/Legal Professional Practices", 27th Annual Advanced Family Law Course, San Antonio, Texas, August 2001.

"Valuing and Dividing the Community Business, Marriage Dissolution Seminar, Corpus Christi, Texas, May 2001.
"Interaction of Probate Court and Family Law," Family Law on the Front Lines, Galveston, Texas, April 2001.

"Bottom Line Appellate Issues," Ultimate Trial Notebook: Family Law, New Orleans, Louisiana, December 2000.

"Pretrial and Trial Strategies for the Complex Property Case", Santa Fe, New Mexico, October 2000.

"Representing the High Tech Entrepreneur: IPO's, Venture Capitalists and Beyond", 26th Annual Advanced Family Law Course, San Antonio, Texas, August 2000.

"Family Law Court v. Probate Court: What Every Family Lawyer Should Know", 26th Annual Advanced Family Law Course, San Antonio, Texas, August 2000.

"Bill of Review", 23rd Annual Marriage Dissolution Institute, Fort Worth, Texas, May 2000

"Appellate Tips: Judges Panel", 23rd Annual Marriage Dissolution Institute, Fort Worth, Texas, May 2000

"Fiduciary Duties of Spouses and Non-Physical Torts", International Academy of Matrimonial Lawyers, Palm Beach, Florida, March 2000.

Internal Procedures in the Texas Supreme Court Revisited: The Impact of the Petition for Review and Other Changes, 31 TEX. TECH L. REV. 63 (2000)

"Strategic Use of Law Beyond the Family Code", New Frontiers in Marital Property Law, San Diego, California, October 1999.

"Trends in Preservation of Error (At Trial, Charge, and Post Verdict)", 13th Annual Advanced Civil Appellate Practice Course, State Bar of Texas, Austin, Texas, October 1999.

"The Appellate Process-the Good, the Bad, and the Ugly", 25th Annual Advanced Family Law Course, Dallas, Texas, August 1999.

"Litigating Marital Agreements: "You can't

always get what you want....",22nd Annual Marriage Dissolution Institute, San Antonio, Texas, May 1999.

"Fiduciary Duties of Spouses, Effective Use of the Remedy of the Constructive Trust, Recoveries for Violations of These Duties, and Issues Presented When Spouses are under Conflicting Fiduciary Duties," New Frontiers in Marital Property Law, Sante Fe, New Mexico October 1998

"Appeal of the Coverage Suit," Third Annual Insurance Law Institute (University of Texas School of Law, October 1998) (panelist/speaker and co-author);

"The New Appellate Rules -- At Last!" Eleventh Annual Advanced Civil Appellate Practice Course, Dallas September 1997 (speaker and author);

GUIDE TO THE NEW RULES OF APPELLATE PROCEDURE (State Bar of Texas 1997) (contributing author);

Motion Practice in the Texas Supreme Court, 59 TEX. B. J. 846 (October 1996)

"Factual and Legal Sufficiency in the Texas Supreme Court," Tenth Annual Advanced Civil Appellate Practice Course, Austin 1996 (co-author)

"Inside the Texas Supreme Court," Ninth Annual Advanced Civil Appellate Practice Course, San Antonio 1995 (moderator and author)

Internal Procedures in the Texas Supreme Court, 26 TEX. TECH L. REV. 935 (1995)

Jurisdiction in the Supreme Court of Texas: "Amount in Controversy", 7 APPELLATE ADVOC. 3 (May 1994) (co-author)

"Internal Procedures and Motion Practice in the Supreme Court," Seventh Annual Advanced Civil Appellate Practice Course, Austin 1993 (speaker and author)

KARL E. HAYS
Law Offices of Edwin J. (Ted) Terry, Jr.
805 W. 10TH STREET, SUITE 300
AUSTIN, TEXAS 78701
(512) 476-9597
Fax (512) 476-6106

EDUCATION

St. Mary's School of Law, Juris Doctor, 1985
University of Texas at San Antonio, B.A., 1982

PROFESSIONAL ACTIVITIES

Board Certified, Family Law, 1996
Certified Mediator, 1994
Board Certified, Civil Appellate Law, 1993
Board Certified, Civil Trial Law, 1991

PROFESSIONAL AFFILIATIONS

Texas Academy of Family Law Specialists, Travis County Bar Association, Texas Bar Association, College of the State Bar, San Antonio Bar Association, San Antonio Family Law Association, Texas Bar Foundation

SELECTED LAW RELATED PUBLICATIONS & PRESENTATIONS

"Contesting and Defending Premarital Agreements", 28th Annual Advanced Family Law Course, Dallas, Texas, August 2002.

"High Tech Evidence: How to Find It, Retrieve It and Get It In", 28th Annual Advanced Family Law Course, Dallas, Texas, August 2002.

"Termination and Adoption: It Ain't Over Till It's Over", 28th Annual Advanced Family Law Course, Dallas, Texas, August 2002.

"Early-Stage Company Valuation"American Institute of Certified Public Accountants/American Academy of Matrimonial Lawyers National Conference, Las Vegas, Nevada, May 2002.

"Summary Judgments and Declaratory Judgments in Divorce", Marriage Dissolution Seminar, Austin, Texas, May 2002.

"Termination and Adoption: It Ain't Over Till It's Over", Marriage Dissolution Seminar, Austin, Texas, May 2002.

"Child Support Collection: A Practical Guide to the Opportunities and Pitfalls in Enforcing and Defending Child Support Obligations," Family Law on the Front Lines, Galveston, Texas, April 2002.

"Valuation of Law Practice in Divorce," American Academy of Matrimonial Lawyers, Sanibel, Florida March 2002.

"Valuation, Characterization and Division of Unusual Assets", New Frontiers in Marital Property Law, Santa Fe, New Mexico, October 2001.

"Professional Partings: Valuing Medical/Legal Professional Practices", 27th Annual Advanced Family Law Course, San Antonio, Texas, August 2001.

"Valuing and Dividing the Community Business, Marriage Dissolution Seminar, Corpus Christi, Texas, May 2001.

"Interaction of Probate Court and Family Law," Family Law on the Front Lines, Galveston, Texas, April 2001.

"Bottom Line Appellate Issues," Ultimate Trial

Notebook: Family Law, New Orleans, Louisiana, December 2000.

"Pretrial and Trial Strategies for the Complex Property Case", Santa Fe, New Mexico, October 2000.

"Representing the High Tech Entrepreneur: IPO's, Venture Capitalists and Beyond", 26th Annual Advanced Family Law Course, San Antonio, Texas, August 2000.

_____

Co-Author, Bill of Review", 23rd Annual Marriage Dissolution Seminar, Fort Worth, Texas, May 2000.

Co-Author, "Sex and Lies: A Daubert Challenge, Techniques for Presenting the Child's Testimony to the Trial Court in a Child Abuse Case, 23rd Annual Marriage Dissolution Seminar, Fort Worth, Texas, May 2000.

Co-Author, "Fiduciary Duties of Spouses and Non-Physical Torts", International Academy of Matrimonial Lawyers, Palm Beach, Florida, March 2000.

Co-Author, "Presenting the Child's Perspective: Techniques for Presenting the Child's Preference of Conservator to the Trial Court", Texas Academy of Family Law Specialists, Las Vegas, Nevada, February 2000.

Co-Author, "Strategic Use of Law Beyond the Family Code", New Frontiers in Marital Property Law, San Diego, California, October 1999.

Co-Author, "Trends in Preservation of Error (At Trial, Charge, and Post Verdict)", 13th Annual Advanced Civil Appellate Practice Course, State Bar of Texas, Austin, Texas, October 1999.

Co-Author, "Summary of the 1999 amendments to the Texas Family Code", Legal Assistant U, San Antonio, Texas, September 1999.

Co-Author, "The Appellate Process-the Good, the Bad, and the Ugly", 25th Annual Advanced Family Law Course, Dallas, Texas, August 1999

Co-Author, "Malpractice", Advanced Family Law Course, State Bar of Texas, San Antonio, Texas, 1992.

Co-Author, "Malpractice, Advanced Family Law Course, State Bar of Texas, San Antonio, Texas, 1991.

Co-Author, "Expert Witnesses", Advanced Family Law Course, State Bar of Texas, San Antonio, Texas, 1990.

Table of Contents

I. INTRODUCTION

According to a 2001 study by the University of California-Berkeley, 93% of all new information is created in digital format. Jason Krause, *Discovery Channels*, ABA Journal, p. 50 (July 2002) [hereinafter referred to as "Krause"]. In 1998, 3.4 trillion email messages were sent across the world, including 343 billion in the United States alone. Daniel Bishop and Amy Horowitz, *Electronic Discovery*, p. 1, ADVANCED BUSINESS & COMMERCIAL LITIGATION COURSE (2001) [hereinafter referred to as "Bishop and Horowitz"]. Experts estimate that 30% of the information stored in computers is never printed out, in other words, it exists only in electronic forms. *See*, *Id.*

One commentator, musing upon such statistics, has concluded that "...discovery today ought to be almost entirely an electronic affair," but adds, with so little case law upon which to draw, courts across the country still struggle with how to handle the discovery of high tech evidence. Krause, at p. 50. Moreover, warns such commentator, in the current unsettled legal environment, electronic discovery can become combative, so much so as to deserve the characterization of "electronic warfare." *Id.*

The present discussion, then, presents an overview of this increasingly critical topic of electronic–or "high tech"–discovery. Although the express context of this presentation is a divorce in Texas, it must be noted that there is little, if any, reported Texas authority on the issue of electronic discovery in the context of a Texas divorce. Indeed, there is little authority anywhere on the issue in the context of matrimonial law. The vast majority of existing reported authority arises in the context of commercial litigation, and much of that involves federal law. Accordingly, the principals articulated in the commercial cases and treated herein, whether state of federal, will have to be translated and applied by the Texas practitioner to Texas divorces. In the present article, federal law–primarily reported federal cases–will be discussed when necessary, but not in great detail.

The Authors have received permission to draw from two excellent articles on electronic discovery, the first by Peter Vogel, Kim Robinson, Josh Roseman and Eric Levy, *Electronic Evidence*: *Discovery and Admission*, INTELLECTUAL PROPERTY LAW (2001), and the second by Terry O. Tottenham, Lana K. Varney, and Larry Johnson, *Discovery and Admissibility of Electronic Evidence*, p. 5, HIGH TECH LITIGATION MEGACOURSE (2001) [hereinafter referred to as "Tottenham, *et. al*."]. The Authors gratefully acknowledge the fine work of these several commentators.

II. THE NATURE OF HIGH TECH EVIDENCE

Electronic evidence is not limited to the files that a person consciously saves on a computer. Instead, in most lawsuits, there are hundreds of different types of electronic evidence to be discovered. Much of this evidence exists *only* in electronic form, such as: email text, headers, and file attachments, voice mail, electronic calendars, materials on corporate intranets, website log files regarding visitors, browser information including caches of visited sites and cookies, and countless other information. Such evidence can be a smoking gun in a lawsuit, since most people do not fully appreciate the extent to which information on a computer system can be accumulated, retained, and later recovered. Accordingly, lawsuits and litigants would be remiss if they were not aware of where to find such evidence.

Generally, all data on a computer system can be found in one of four places: (1) in *active data* that is readily available to users, such as word processing documents and email messages; (2) in *archival data* that is no longer in use, but stored separately to free-up space on a drive; (3) in *backup data* that is copied to some portable media to protect users from a system failure; or (4) *residual data* that appears to be gone or deleted, but may still be recoverable from the computer system.

In addition to data files, the computer system may contain a cornucopia of background information about any particular person's activity on the computer system, such as what files the user may have modified or how long the user was on the system. *Id*. The importance of such background use information cannot be overestimated, particularly in litigation contexts such as a divorce.

The continuing existence of the computer user's "track record" can create problems for the user. For example, in *Denton County v. Howard*, 22 S.W.3d 113, 116 (Tex.App.–Fort Worth 2000, no pet.), a whistleblower suit, the plaintiff alleged that while updating records on a computer operated by a Denton County employee, he discovered that the computer had been used to access 250 to 300 homosexual websites on the internet. Because the plaintiff believed that such activity constituted an illegal use of government property, he reported the information to a superior, who promptly fired him. *Id*. *Denton County* thus establishes two pertinent propositions: (1) a computer is like an elephant, rarely forgetting, often leaving behind a big pile of refuse into which someone may later unwittingly step; and (2) even in cyberspace, no good deed goes unpunished.

Thus, it is not difficult to imagine how many people, when served with divorce papers, begin to wonder what exactly is on their hard drive, or on that of his or her spouse.

III. TYPICAL TYPES OF HIGH TECH EVIDENCE

Typically, lawyers seek electronic discovery in four types of requests, generally not individually and often overlapping. Requests generally seek:

1. Generating and producing paper copies of electronically stored data (printing it out);

2. Production of electronic copies of electronically stored data (getting it on disks or tape);

3. Inspecting a party's electronic storage device (looking at the computer "originals"); or

4. Compelling manipulation of a party's own electronically-stored data (forcing the producing party to crunch the data).

The scope of the electronic discovery request is often restricted by ignorance of electronic storage, ignorance of what type of data is stored electronically, and the court. Teaching yourself about the basics of electronic storage of information and enlightening your clients about the "hidden files" often associated with electronic storage of data is the first step in responding to and limiting electronic discovery. Teaching the court of the potential scope of the electronic discovery request and how much of the data is irrelevant and insignificant to the lawsuit is a second critical step.

A. Documents.

Today, it is as rare as a bearded-man in a tiara and miniskirt running for mayor of Austin that a document is not created on a computer. Few documents are created without initial drafts, and it is not uncommon for multiple drafts of documents to be maintained on computers. Certainly the trend toward a "paperless world" has lead many clients to maintain computer originals as archives. Most computer programs automatically create backup files for works in progress in the event of a system failure. Some backups are deleted when the system is shut-off, but others remain in a particular directory on the hard drive.

Generally, each electronic file has a unique file name, file size, distribution route of the document and modification date and time. Most large law corporations now use Document Management Systems (DMS) to handle document management. These systems track all file access including creation, modification, printing, reading, copying and deletion. Lawyers may try to argue this information may be useful because it provides the exact minute the last time a document was altered. Computer clocks can be manipulated, however, and an argument can be made that the information is not reliable and only reflects the date the file was transferred, rather than originally created.

1. Metadata

Most importantly, electronic versions of documents contain more information than their paper counter parts. Metadata is information contained within the electronic version of a document that may not be apparent in a printout of the same document. Not too ago, for example, it was revealed that Microsoft Office inserts special identification numbers in documents (created in Word, Power Point, or Excel) which can sometimes be used to trace the source of a document to a particular computer. Microsoft provides a patch to kill this undocumented feature. Similarly, Word's revision tracking feature will often be used to show the changes between two drafts. However, if the document is sent to someone else with the tracking feature simply toggled off, the recipient may be able to re-toggle the display feature and identify all the recent changes (including deletions). Finally, some word processing programs may save a certain number of "undo" operations along with the electronic version of a document. A recipient of the electronic document can simply click on "edit" and "undo" to see recent changes that were made to the document.

If your clients are using WordPerfect, ensure that they turn off the "save undo/redo items with document" feature on their systems. In those instances where a receiving party does not need to edit the file, it should be sent in Adobe Acrobat (PDF) format. This non-editable document will appear exactly as it would in print, but will contain no additional data. Similarly, in Word 2000, you can produce a document in Rich Text Format (RTF) and in HTML format, both of which would not contain replicant or "additional data" other than the text. [NOTE: HTML will contain Author information]. This will allow the receiving party to search, edit and otherwise manipulate the text while the sender need not fear producing metadata.

2. Directory "Trees"

Well-crafted electronic discovery requests seek not only the information that is embedded within the computer file itself, but the information that is not embedded which often can be just as important. Each computer file is "located" within a directory structure on a storage device: 1) at the "root" directory; or 2) within a sub-directory. A knowledgeable request will seek a print-out or file containing a directory "tree," showing where all the files are located.

B. E-mails

We have all heard stories of how the proverbial "smoking gun" was retrieved from a party's electronic mail system. E-mail users, without being reminded, can be less conscientious and more informal in e-mail messages than in written letters or memos. E-mails may remain stored for long periods of time and may appear on back-up tapes. Perhaps the most highly publicized,

and ironic example of e-mail damaging a corporation is the Microsoft antitrust litigation. During the Microsoft litigation, Bill Gates, in a sworn deposition, flatly contradicted his statements in an e-mail from James Barksdale, chief executive of Netscape, to America Online's chairman, Steve Case, in which he referred to Case as "Franklin D." and himself as "Joseph Stalin" in an allusion to the leaders of the United States and the Soviet Union in World War II. *See* Amy Harmon, *"E-Mailers Tighten Up Loose Lips; Companies, Citing Legal Concerns, Curb Electronic Messages,"* Int'l Herald Trib., Nov. 12, 1998 and James V. Grimaldi, *"The Gates Deposition: 684 Pages of Conflict,"* Seattle Times, Mar. 16, 1999, at Al. These examples of cavalier e-mail should be reason for concern and the impetus for proactivity with respect to electronic document issues for all companies. *See GTFM, Inc. et al. v. Wal-Mart Stores, Inc.,* 2000 WL 335558 (S.D.N.Y.)(defendant sanctioned for counsel's initial representation that requested computer data did not exist, contradicted a year later by deposition testimony that the data existed when they were requested, but were subsequently destroyed).

E-mail may exist on local work stations, network file servers or on any of a number of commercial computer service providers. E-mail and programs generating faxes from computers keep logs of dates of transmission and receipt. It is therefore a simple, routine task to match computer activity chronologically to significant dates in a lawsuit: who knew what, where and when. Similarly, online identities and relationships can be proven by the contents of a user's e-mail address book. As with files, deleted entries in address books can often be recovered, proving not only the presence of the deleted entry, but also an implied attempt to hide that evidence. Users who delete address book entries are often unaware that deletion can be reversed, creating powerful opportunities to discover impeachment evidence.

Some software includes the ability to track the number of times a user sends e-mail to someone, both within and without the computer system. Look for a "Frequent Contacts" tab of the Address Book function of the software. This log can usually be deactivated so that the Frequent Contacts will not be logged information.

Reminding all e-mail users that their messages may ***not*** be private, confidential, or immune from being seen on the 10:00 o'clock news is a prudent step that should be taken frequently. It is an almost impossible task to control the flow and proliferation of e-mail. Still, a client can and should implement and post prominently a policy prohibiting private use of e-mail, reminding employees that all e-mails are like postcards, available for all to read, including the employer. From time to time, employee e-mail should be monitored for compliance. Old e-mail should be routinely deleted and expunged. Make your clients aware of the persistent nature of e-mails and suggest that they not back-up e-mails in a "normal" rotation, which has a long life span (months and even years in some cases), but to have a separate back-up scheme and rotate them on a few days or at most a week. This will make it difficult if not impossible to produce damaging e-mails. However, it will also make it impossible to restore e-mails from backup that were accidentally deleted longer than the rotation scheme. Thus any exculpatory e-mails, if not printed and saved as hard copies, will be beyond recovery.

Your clients should also consider using encryption technology that helps cautious e-mailers send messages so encrypted they become indecipherable to even the most powerful computer forensics technology. Some programs currently available are so powerful that nothing in the forensics world can recover an e-mail encrypted in this fashion. Bear in mind, of course, that the encryption service provider may be subject to the court's jurisdiction and required to hold on to the "key" that will allow recovery of the e-mail.

One final telling example of an expensive restoration process is in *Linnen v. A.H. Robins Co., Inc.,* 1999 WL 462015 (Mass. Super. 1999) a case that presents a situation lawyers and their clients will surely want to keep in mind. The *Linnen* case was a state court wrongful death action dealing with the infamous weight-loss drug fen/phen. *See Id.* at *1. The central issue in the case was the defendant's knowledge of the risks of the product. *See Id.* Plaintiffs sought discovery of any electronic mail messages retained by Wyeth-Ayerst Laboratories (Wyeth) that were responsive to the plaintiffs' discovery requests. *See Id.* at *2. Not surprisingly, Wyeth opposed such discovery, claiming it had already produced a large number of documents, including e-mail messages. *See Id.* at *1-2. Further, Wyeth objected on the grounds that it would be unduly burdensome and costly for it to restore the back-up tapes containing the e-mail and other documents. *See Id.* at *1. Moreover, if ordered to produce such information, Wyeth requested that the plaintiffs be compelled to absorb the cost. *See Id.*

The plaintiffs in *Linnen* became interested in the discovery of e-mail when they learned through discovery that many Wyeth employees had used e-mail to communicate regarding the issues that were the subject of the lawsuit. *See Id.* at *2. The plaintiffs then specifically requested e-mail sent or received by fifteen individuals on several topics for a certain time period. *See Id.* Wyeth responded that it had "'no mass storage devices' or other back-up tapes containing electronic mail messages" for that period. *Id.* However, Wyeth was able to produce e-mail messages saved on personal computers. *See Id.* Several months later, Wyeth became aware that it had back-up tapes in storage that could contain responsive information. *See Id.* at *3-4. As it turned out, Wyeth located over one thousand back-up tapes from a variety of software systems. *See Id.* at *4. Five categories of tapes existed, including over one thousand tapes from the relevant time period. *See Id.* The cost to restore

one category of the tapes ranged between $300,000 to $350,000 and $850,000 to $1.4 million for another. *See Id.*

Rather than order a wholesale restoration, the Court held that it would await the outcome of the protocol endorsed in the Federal Court Multi-District Litigation (MDL). The MDL is a consolidated suit brought by thousands of plaintiffs alleging injury as a result of diet-related pharmaceutical products, wherein Wyeth, also a defendant in the MDL, agreed in that case to restore a sampling of tapes from each of the categories which were identified as possibly containing relevant information. *See Id.* at *5. Under the MDL protocol, Wyeth would bear the initial costs but had the right to seek reimbursement of up to $25,000 from plaintiffs. *See Id.* Only upon a showing good cause would further production be required. *See Id.* Pending the findings in MDL, the Court in *Linnen* left open the issue for re-evaluation. *See Id.* at *6.

Of particular interest to clients and their lawyers was the Massachusetts court's comment in *Linnen*:

> [T]his is one of the risks taken on by companies that have made the decision to avail themselves of the computer technology now available to the business world. To permit a corporation such as Wyeth to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results. *Id.* (citations omitted).

C. Networks

On a grander scale, discovery requests will seek information regarding the entire system. Many computer network systems automatically create and maintain logs of certain activities on the computer system. These logs identify when the system was turned on, turned off, if there was access from remote terminals, and other potentially important data. Additionally, there are communication programs that create logs of communication activities, identifying such things as connections to other computers via modem and the transferring of files.

D. Storage Devices

Frequently, discovery requests seek storage devices or diskettes that are in use or have recently been in use in hopes of finding "deleted" files. In English, the word delete means "erase, remove, etc." In computer, however, "delete" means "available to write over." Computers maintain a FAT or "file allocation table" which is like a table of contents, where each "live" file is kept intact and kept from being overwritten by newly generated files. When a file is "deleted," only its name is removed from the FAT, but otherwise for a period of time–which can be a long time–part or all of the file's content remains reconstructable. And even if over time the bytes of information that once were a part of a "live" file are overwritten, other portions of it may be strewn about the hard disk at various locations, capable of total or partial reconstruction. Finding and "undeleting" deleted files can provide a rich source of information, particularly if the files were deleted at about the time a party was sued and it tried to hide or destroy sensitive information. Diskettes store information in the same way and deleted files do not automatically disappear unless the disk is reformatted.

After deletion, some files cannot be recovered whole. In such cases, fragments of those files will often linger on a computer's disk drive. Although the whole file may be beyond saving, fragments may be detectable and, by appropriate combinations of technology and experience, their original form may be inferred and partially reconstructed. There are a variety of simple utility programs available for retrieving deleted documents. There are also programs developed to ensure deleted means *deleted*. Take steps to ensure that your clients' systems are protected with such software. When a requesting party asks why they have such software, they can tell them their attorney advised it.

E. Internet Service Providers

If internet use is at issue, discovery requests often will seek access to a party's web browser, which automatically caches the information and images from web pages that are visited. This leaves behind a record of what sites were visited in the user's computer. These requests can also uncover information about the user placed in a file by a web site operation for quick recall when the user visits again ("cookies"), bookmarked files (one-click shortcuts to favorite web sites created by the user), and downloaded text and images for storage on local hard drives, floppy disks or servers.

Various special-purpose computers retain logs of internet access. These include firewalls, proxy servers, terminal servers, modem pool administrators, and potentially every type of system that helps move data from a corporate network to or from the internet. Web servers can also produce audit trails demonstrating where someone has gone within a web-site. The user's IP address (a unique address associated with a computer) is recorded and saved in a log on the web server. This may have special importance for a client's Extranet where client communications might be taking place. Knowing where these systems might be found, and how to keep the records intact, can be a valuable source of evidence. Additionally, such logs often track access to corporate systems from outside users.

Unless the software setting is changed, these caches remain stored on the hard drive, often without the user realizing it. Tell your clients to

periodically have their systems management reset the software, particularly if there is no reason to maintain such information. There are numerous software releases that will scrub browser history, URL lists and "cookie files" upon request or every time the machine is turned on. Encourage your clients to consider the use of these programs.

F. Proprietary Online Services

Chat rooms, list servers (e-mail based discussions using a push technology), Use net (could be considered a bulletin board) and bulletin boards are relatively new forms of computer-mediated communication also subject to discovery. Like web use, exchanges in these forums are subject to plaintiffs' claims that they may be substantive evidence of wrongdoing (e.g., copyright infringements), circumstantial evidence of wrongdoing (e.g., distribution of copyrighted materials), or simply embarrassing. Complete transcripts of conversations or postings are seldom kept for more than a few days, so discovery may be confined to records of participation. Again, remind clients of potential disclosure of these activities.

G. Voice Messaging Systems

Voice mail systems store electronic copies of voice messages until deleted or for a fixed period of time. In many cases, voice messages are preserved for long periods of time on the system's storage devices even though the intended recipient has "deleted" the message(s). Clients should consider establishing routine procedures for clearing voice messages after a short period of time.

H. Litigation Support Systems

Targets of opportunity are also seen in lawyers' litigation support systems. Most litigation support systems will contain electronically stored versions of relevant documents on a database. More complex systems can be designed to perform complex statistical analysis of electronically stored data. Discovery requests for these systems are most successfully defended by asserting the attorney work product privilege. Courts have consistently held, however, that the level of protection from discovery afforded litigation support systems will depend on the level of attorney input into the contents of the system. Those systems actually developed by lawyers, which contain summaries or notes regarding important documents and trial strategies in addition to databases, generally receive the most protection as opposed to strict databases of otherwise discoverable documents.

A party resisting the production of computer materials may assert that computer analyses and programs or information in a database to be reviewed by the experts have been generated by its attorneys, and therefore necessarily reveal the mental processes and strategies of the attorneys. *See, e.g., Santiago v. Miles,* 121 F.R.D. 636 (W.D.N.Y. 1988); *Williams v. E.I. du Pont de Nemours & Co.,* 119 F.R.D. 648 (W.D. Ky. 1987). In *Shipes v. BIC Corp.,* 154 F.R.D. 301, 309 (M.D. Ga. 1994), an in-house legal department's database was protected as work product where it would be impossible to separate the work product from the non-work product data and the entire system arguably constituted work product.

Litigation support databases which index the documents produced in the litigation are not discoverable. *In re IBM Peripheral EDP Devices Antitrust Litigation 5*, Computer L. Serv. Rep. 878 (N.D. Cal. 1975); *United States v. American Tel. & Tel. Co.,* 642 F.2d 1285 (D.C. Cir. 1980). Materials which would reflect the selection and compilation of documents by counsel in preparation for pretrial discovery are generally found to be protected work product. *Sporck v. Ped.,* 759 F.2d. 312, 315 (3d Cir.), cert. denied, 474 U.S. 903 (1985). *Also, see IBM Corp. v. Condisco, Inc.*, 1992 WL 52143, at *2 (Del. Super. 1992) (protecting parties from access to computerized defense litigation support systems or other computerized communications including e-mail messages); *But see Minnesota v. Phillip Morris, Inc.,* 1995 Minn. App. LEXIS 1602, at *1-2 (Minn. App. 1995) (refusing to grant work product protection.

IV. TYPICAL LOCATIONS OF HIGH TECH EVIDENCE

There are a number of "locations" where electronic evidence may reside: computer hard drives; portable, removable hard drives; zip drives; floppy diskettes; compact disks; computer tapes; back-up storage devices; DVD disks; remote computing services; and commercial communication systems. By far, the most common electronic storage device for businesses–and possibly for individuals–is the computer disk drive, or hard drive. Almost every stand-alone computer has at least one hard drive, and most workstations or networks have one as well. Hard drives retain information for long periods of time. Personal data assistants (PDA's), such as a Palm-Pilot, also are becoming more and more prevalent.

Companies specializing in data retrieval can search and seek all types of data, from "deleted" information to broken or damaged hard drives. Given the voluminous amounts of information hard drives can retain, handing them over to the other side may be the equivalent of delivering the keys to the warehouse. Moreover, the nature of electronic documents makes searching for the proverbial "needle in the haystack" much easier.

However, it must be noted that software programs are available to ensure that a hard drive is completely purged on a periodic basis and that such purging completely eliminates all data. Such programs may be used in any individual's or business' computer, including stand-alone PC's, network file servers, workstations, personal or employee laptop/portable computers; home

computers, and even portable/removable hard drives.

It may be wise at least to inquire, probably in a deposition, whether the opposing litigant–or his or her business–owns or has used such a program in the recent past. Further, given the enduring quality of most electronic evidence, broken, out-of-service and stored systems may provide worthwhile evidence

.

V. DISCOVERY OF HIGH TECH EVIDENCE

Today, the question of the discoverability of electronic information is no longer a seriously debated issue. Bishop and Horowitz, at p. 5; *see also and cf*., *Bill v. Kennecott Corp*., 108 F.R.E 459, 461 (D. Utah, C.D. 1985) ("[i]t is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure if it otherwise meets the relevancy standard prescribed by the rules, although there may be issues in particular cases as to the form of what must be produced"); *see also*, *State Farm Mut. Auto. Ins. Co. v. Engelke*, 824 S.W.2d 747, 751 (Tex.App.–Houston [1st Dist.] 1992, orig. proceeding) (when State Farm was sued for bad faith in its claim handling process, the trial court ordered the production of computer information concerning other lawsuits in which the same or similar allegations had been made).

As a result, many lawyers now routinely ask for electronic evidence, especially e-mail, in their discovery requests. However, most lawyers have little understanding of how to collect or analyze relevant electronic mail. Fortunately, prudent use of the most common forms of discovery will allow a lawyer to gain the knowledge he or she needs, particularly in divorce cases.

A. Important Texas Rules of Civil Procedure

The Texas Rules of Civil Procedure define the scope of discovery to include electronic information. Specifically, TEX.R.CIV.P. 192.3(b) ("Documents and Tangible Things") provides:

> [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 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..

Furthermore, TEX.R.CIV.P. 196.4 (effective January 1, 1999) provides:

> [t]o 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.

B. The Discovery Process

As might be expected, there is some disagreement among high tech discovery "experts" about the most appropriate starting point for electronic discovery. Whenever actually utilized, the following "steps" are unquestionably important, if not critical, to the successful discovery of electronic evidence.

1. Is Electronic Discovery Called For?

Gaining detailed information about the other side's computer system may not be justified in every case. *See*, Talmage Boston and David M. Tobias, *Finding the Smoking Guns in Cyberspace: A Discourse on Discovery in the Electronic Era,* p. DD-10, ADVANCED PERSONAL INJURY LAW COURSE (1999) [hereinafter referred to as "Boston and Tobias"]. For example, in Texas, most divorces will be Level 2 discovery. In Level 2 cases, it will likely be more difficult to obtain complete information about the other side's computer system because of the limited number of interrogatories available (25) and the time permissible for depositions (50 hours per side). *Id*. Useful alternatives for discovering the desired information include written depositions under TEX.R.CIV. P. 200, a request for inspection of tangible things including disk drives under TEX.R.CIV.P. 196.1, and a request for entry on property in order to inspect designated objects such as computer systems under TEX.R.CIV.P. 196.7. *Id.*

Ultimately, it might be impossible to justify the time and expense needed to discover every aspect of the other side's computer system; in such a case, more directed discovery requests and alternatives to interrogatories and depositions should be considered. *Id*.

Certainly, in almost any divorce, the lawyers will want to know about e-mails between the parties, between the parties and their children, and if paramours exists, between the party involved and the paramour. In more complex cases, perhaps involving large estates, unusual interspousal claims, or successful businesses, expanded electronic discovery is probably required.

2. Is an Expert Needed?

Two commentators have stated that the first question in discovering electronic evidence is whether an expert is needed. Tommy Jacks and Drew Wright, *Discovery of Technology*: *The Rules Have Changed*, p. 4, ADVANCED EVIDENCE AND DISCOVERY COURSE (1999-2000) [hereinafter referred to as "Jacks and Wright"]. An expert may be able to help the lawyer maximize the amount of recoverable data by identifying what data is backed up or saved regularly, where it might be stored, in what format it might be stored, and what part of it might actually be recoverable. *See,* Krause, at p. 51. Perhaps the most important role technical experts play is simply figuring out where relevant documents are likely to be stored. *Id.* Moreover, copying and restoring data can take considerable drive space that most lawyers do not have, but an expert may. An expert may also be able to preserve the chain of custody of relevant electronic evidence and prove authenticity.

All that said, lawyers involved in high tech discovery nevertheless say that caution is needed when working with computer experts. *See*, Krause, at p. 52. Lawyers still need to be active participants in setting search criteria, screening for privileged information, and handling non-technical details. *Id.* In the end, if the experts are given too much power, the lawyers can lose control of the case and costs can escalate. *Id*.

The cost of an expert is a most relevant issue. Typically, forensic review and actual data retrieval from a computer will cost from $150 to $300 per hour. Jacks and Wright, at p. 4.

It should be noted that the *Daubert* factors probably apply to computer experts, and, because of the relative novelty of the field, might be used to exclude an otherwise eminently qualified expert. *Id.* at pp. 8-9.

One final option is a credible, experienced, neutral third-party computer expert to conduct or supervise electronic media discovery. *Id.* at p. 9; *see also and cf*., *Simpson v. Canales*, 806 S.W.2d 802, 811 (Tex. 1991) (the appointment of a master lies within the sound discretion of the trial court).

3. Negotiate with the Other Side

Some lawyers believe that the first rule of electronic discovery is to negotiate with the other side. *See*, Krause, at p. 50. Cost control and the uncertainty of judicial action underpin the argument. *Id*.

One result of successful negotiation early on might be a "data exchange agreement," which identifies timelines and defines details such as the appropriate format for data production. *Id*. Negotiations can also lead to agreements as to the appropriate search terms to be used in scouring a database for documents. *Id*. It is possible that the other side might even agree to make available complete and authenticated copies of its system. *See*, Jacks and Wright, at p. 14.

4. The Notice Letter

One of the first items in any discovery plan should be a notice, or preservation, letter. Since information stored on a computer changes every time a user saves a file or otherwise does just about anything on a computer, it is important that the lawyer, as soon as possible, send a notice letter to the adversary informing the adversary of the type of information to be preserved and the places that such information may exist. Specifically, the opposing party, or the operator of the relevant computer system, if any, should be advised not to initiate any procedures which would alter any active, deleted, or fragmented files.

Certain commentators admire the prompt notice letter not only for its efficacy, but as well for the appearance of impropriety it creates. *See,* Tottenham, *et. al*., at p. 6. Appendix I is an example of the type of notice letter currently in use in many lawyerly circles.

5. Use Discovery to Gain Overview of Systems

Discovery devices should be used to gain an overview of the computer systems involved. It is impossible to effectively plan a discovery strategy without knowing about the target computer system. The lawyer should employ the initial discovery requests to learn about the computer system from which the lawyer ultimately will be seeking information, for example, interrogatories asking the recipient to describe the computer hardware, software, and network systems used at home, or at main and/or branch offices, and depositions.

Naturally, there may be divorces in which electronic evidence is not a factor; there may be as well divorces in which electronic evidence is not that much of a factor, for example, in which e-mail is really the only form of electronic evidence relevant to the case. However, there may be divorces in which more technical issues have arisen, such as spoliation, in which it will be important to gain knowledge of the other side's system.

a. Definition of "Documents"

The definition of "documents" should include all data compilations, e-mail and electronically stored data. For example, the following definition might be used (or modified to meet the needs of the particular case):

> "Document" shall mean any writing, drawing, film, videotape, chart, photograph, phonograph record, tape record, mechanical or electronic sound recording or transcript thereof, *retrievable data* (whether carded, taped, coded, electro-statically or electro-magnetically recorded, or otherwise), or *other data compilation from which information can be obtained*, including (but not limited to) notices, memoranda, diaries, minutes, purchase records, purchase invoices, market data, correspondence, computer storage tapes, computer storage cards, *computer hard drives, hard copies of computer information*, *diskettes, compact discs, backup tapes, zip drives, personal data assistants,* or discs, books, journals, ledgers, statements, reports, invoices, bills, vouchers, worksheets, jottings, notes, recordings, instructions, lists, logs, orders, recitals, telegram messages, telephone bills and logs, resumes, summaries, compilations, and other formal and informal writings or tangible preservations of information.

b. Interrogatories

The following interrogatories will be helpful to learn the computer environment of an adverse party:

> 1. Describe the computer hardware, software, and network systems used by defendant at its main offices and branch office.
> 2. Describe the version and brand name of the electronic mail (email) system used by defendant at its main offices and branch offices.
> 3. Describe the electronic mail retention policy used by defendant at its main office since the date of the contract with plaintiff. To be complete, your answer should include, at least, the type of backup system used, how often your system is backed up, and where such backup materials are stored.
> 4. Describe version and model numbers of the computer software and hardware used to make backup copies of the electronic mail system used by defendant at its main office and branch offices.

The foregoing example interrogatories will requiring some tailoring to be applicable to the routine Texas divorce. For example, the focus in the routine Texas divorce should probably fall on home or personal computers, unless a business is involved in the property of the parties.

c. Requests for Production

Requests for production are the most common discovery device for obtaining electronic evidence. *See*, Boston and Tobias, at p. DD-8. Guidelines for requests for production include:

> 1. be sure to make clear in their request that electronic documents as well as paper are being sought;
> 2. as already discussed, make the definition of "documents" include all data compilations, email and electronically stored data;
> 3. ask for backup tapes as well as for information regarding how the tapes were made; also ask for diskettes or cd's upon which a user may have saved relevant data; and
> 4. ask for an "image copy" that will create a mirror image of the targeted drive.

In light of the paucity of judicial interpretations of the current discovery rules, it might also be a good idea to make separate, specific requests for production for electronic files and data, in addition to requests for other specific, traditional documents, such as:

> all computer, electronic or magnetic data or files containing or relating to [the subject matter], including all current and prior

> copies, drafts, versions or redline/blackline copies, whether created by word processing, spreadsheet, database, editor, presentation, graphic, video, audio, project management, scheduling, calendaring, notes, journal, financial, accounting, billing or other application software.

See, *Id*.

d. Questions to Individuals

The opposing party–and possible other witnesses as well–should be asked about their individual computer use. Such questioning may reveal sources of electronic evidence not otherwise obtained through discovery directed at a workplace computer system. For example, perhaps a party or individual witness uses his home computer for work, or a laptop or palm pilot. In that case, discovery requests should be expanded to include such devices as well.

6. Preserve the chain of custody

Because data can be easily altered, it is important that a chain of custody be established as to any electronic evidence. At a minimum, this requires proof that (a) no information has been added or changed; (b) a complete copy was made; (c) a reliable copying process was used; and (d) all media was secured. Feldman and Kohn, *Essentials of Computer Discovery*, pp. 12-13 (1997). Put another way, every step in acquiring the electronic evidence should be carefully and completely documented, such as how the file was found, what tools were used locate it, where it was found, and how it was transferred to its current format. *See*, Boston and Tobias, at pp. DD-12.

Furthermore, in Texas, at least in criminal cases, there is authority to suggest that a gap in the chain of custody goes to the weight of the evidence, not its admissibility. *See, e.g.*, *Hutchinson v. State*, 642 S.W.2d 537, 538 (Tex.App.–Waco 1982, no pet.) (proper predicate for admission of computer printout did not require showing beyond the requirements for authentication, rather, such a showing would go to weight of the evidence); *Garner v. State*, 939 S.W.2d 802, 804-805 (Tex.App.–Fort Worth 1997, pet. ref'd) (gaps in chain of custody go to weight of the evidence, not its admissibility). It makes no sense to test the applicability of such criminal cases to a divorce case in Texas; preserving the chain of custody will eliminate certain admissibility issues.

7. Timing of the Discovery Process

Whether written discovery precedes or follows a deposition or depositions has been termed a "strategy call." Jacks and Wright, at p. 6. Unlike the usual order of discovery, *i.e.*, written discovery, then depositions, the reverse may be better with electronic discovery, because the initial depositions might reveal exactly what electronic evidence or storage media to inspect. *Id*. On other the hand, however, production of electronic evidence often results in documents which are unintelligible to an "outsider," and, in such a case, a subsequent deposition might be required to "crack the computer code." *Id*.

C. The Form of Information Produced

TEX.R.CIV.P. 196.4 requires a requesting party to "...specify the form in which the requesting party wants it [the electronic or magnetic data] produced." Therein hangs a tale, which involves the cost of using the data once it has been produced, the use of such information at hearings or trial, and protection against alteration after production. *See*, *Id*. at p. DD-9.

1. Paper

The production of electronic data does not necessarily mean the production of electronic data in electronic form. Paper printouts may well suffice, particularly if there is no question as to authenticity, drafts are not at issue, the exact time and date of creation are not crucial, and the electronic documents will be preserved and available if needed.

Paper printouts of electronic data are easier to read, easier to attach to motions, and easier to introduce into evidence, but carry the drawback that paper printouts do not include all of the information contained in the electronic original. *See, Id*. An electronic file may have significant attributes that cannot be printed on paper: as already discussed, for instance, many word processing files have prior edits saved, along with author and typist identification, as well as the dates of editing or accessing, all of which information will not be provided by a paper printout. *Id*.

2. Native vs. Computer Readable

Electronic information can be produced in its native, "as is," electronic form, or in a generic computer format such as "ASCII" text. *Id.* Although generic formats such as ASCII are readily searched by computers, critical information is often lost in the conversion process. *Id*. In contrast, the native, computer readable format is the most versatile form of production, but will require access to compatible hardware and software in order to read and manipulate the data, another instance where the assistance of an expert, who has the hardware to run the software needed for the job, becomes attractive. *Id*.

3. "Mirror Image Copies"

If there is a concern of electronic spoliation, or if information about the exact usage of the storage device is relevant, a request for on-site inspection or "mirror image" copying may be made. Information is stored on hard drives in particular locations or sectors. A variety of locations may be used to store files. When a copy of the file is made, the information is drawn from the different locations and copied to available space on the copying medium. Erased files are not copied, and other sub-file level information is lost. However, "mirror image" copies of storage devices can be made, which retain the information in the same place when it is copied. This process also copies all the deleted files and pieces of deleted files that are on the original. This allows for a sub-file level forensic examination of the storage device and what data it contains. In addition, this allows for review of any electronic "footprints" contained on the original, i.e., an analysis of who accessed the system, when, and how often (and who did not)

.

This type of production is extremely disruptive, and one should consider demanding the requestor to show good cause why a "mirror image" copy is necessary. Consider demonstrating to the court that this process will require the use of identical storage devices to those subject to discovery, and that this type of production requires a high level of expertise. Alternatively, consider providing for on-site inspection instead of prolific copying. Also, making imaged copies of hard drives may avoid spoliation claims. Although the imaged copies themselves are not provided in direct discovery, they can be made available for *in camera* inspection if a party is accused of withholding evidence.

4. Sample Language: Form Specification

Assuming an IBM compatible PC or a Microsoft Windows based computer with a CD-ROM drive, the following language has been recommended for specifying the form in which electronic data is to be produced:

> Electronic or magnetic data shall be produced in its native computer readable format with an identification of its associated software application and computer system on CD-ROM's readable by PC computers. The data produced must contain an exact and compete image copy of the source hard drives, or other electronic or magnetic media or storage device containing the original data and include not only active files, but all deleted, erased or discarded copies, and prior versions or drafts of the data.

Id. at DD-10.

D. Who Pays For All This?

Not surprisingly, the costs of requesting and responding to computer discovery can be enormous, although the producing party will normally bear the brunt of the initial expense of producing documents and electronic data. *Id*. at DD-15. TEX.R.CIV.P. 196.4 specifically addresses the burden of electronic discovery and requires the court to shift the cost of production to the requesting party if production cannot be accomplished by reasonable efforts. *See*, *Id*. The cost of any extraordinary steps necessary to retrieve requested information will most likely be born by the requesting party, another issue ripe for the intervention and input of opposing experts. *See*, *Id*.

In one recent federal case, *Rowe Entertainment v. William Morris Agency*, 205 F.R.D. 421 (S.D.N.Y. 2002), the court devised an eight-point test to see which of the parties ought to shoulder the cost of electronic discovery. *See*, Krause, at pp. 50-51. The federal magistrate ruled that the plaintiffs should pay for producing the defendants' e-mail, and the defendants should pay for reviewing the production for privileged information. Among the factors the court considered were the cost of producing electronic files, the likelihood of discovering critical information, and the resources available to the respective parties.

Although the court in *Rowe Entertainment* noted that all parties had sufficient resources to pay litigations costs, two factors tipped the balance in favor of the plaintiffs bearing the costs of production: (1) the costs of recovering the e-mail would be substantial; and (2) the discovered material was not likely to provide a "gold mine" of information.

As a final general matter, especially applicable to electronic discovery, always keep in mind that discovery may not be used as a fishing expedition or to impose unreasonable discovery expenses on the opposing party. *See, e.g., K Mart Corp. v. Sanderson*, 937 S.W.2d 429, 431 (Tex.1996).

E. Another Day at the (Federal) Electronic Discovery Office

Despite the fact that electronic data stored on computers falls within the definition of "documents" under the Federal Rules of Civil Procedure, it does not necessarily follow that the information stored on a computer is always discoverable. For example, in moving to compel production of electronic records from a defendant's hard drive, a plaintiff must usually make at least a prima facie showing that there is something on the hard drive worth discovering. A good example of how this requirement can be met is set forth in *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999).

In *Playboy,* the magazine alleged that Welles, a Playmate of the Month model in 1980 and Playmate of the Year in 1981, used the "Playboy" and "Playmate" trademarks on her personal website without authorization from Playboy. During the course of discovery, Playboy learned that in the past Welles had deleted email communications which had been previously requested in discovery by Playboy. Playboy argued that such deleted emails might reflect Welles' knowledge of the "Playmate of the Year" contract and show that she knew the contract required her to obtain written approval from Playboy before she could use the "Playmate of the Year" designation. Playboy also asserted that the deleted emails might negate Welles' emotional distress counterclaim because they would indicate her state of mind regarding issues addressed in the lawsuit. Finally, Playboy asserted that the emails might support its position that visitors to Welles' website would view the website as associated with hardcore pornography.

Welles, on the other hand, contended that her business would suffer financial losses due to the four to eight hour shutdown required to recover information from her hard drive, that any recovered emails between her and her attorneys were protected by the attorney-client privilege, and that the copying of her hard drive would be an invasion of her privacy.

Acknowledging that Welles used her email system for both business and personal communication, the court concluded that the need for the requested information outweighed the burden on Welles, and proceeded to set forth a protocol under which information on the hard drive could be obtained without impinging upon any privileges between Welles and her lawyers or causing her any serious financial difficulty.

The court decided that it would appoint a computer expert specializing in the field of electronic discovery to create a "mirror image" of Welles' hard drive. The parties were required to meet and confer on who the expert should be, or to submit a list of suggested experts if no agreement could be reached. To the extent that the computer specialist had direct or indirect access to information protected by the attorney-client privilege, the court said that such "disclosure" would not result in a waiver of the attorney-client privilege. The court required the computer specialist to sign a protective order currently in effect for the case, and ordered that any communications between plaintiff and/or plaintiff's counsel (who were required to pay the specialist's fees) and the appointed computer specialist pursuant to the order would be produced to defendant's counsel

The parties were to agree on a day and time to access defendant's computer, although only Welles and her counsel could be present during the hard drive recovery. Once the expert had made a "mirror image" of Welles' hard drive and transferred it onto a disk, he was required to give the copy to Welles' counsel, who would then print and review any recovered documents and produce to Playboy those communications that were responsive to any earlier requests for documents and relevant to the subject matter of the litigation. Any documents withheld on the basis of privilege were to be recorded in a privilege log. Lastly, to the extent the documents could not be retrieved from Welles' computer hard drive or the documents retrieved were less than the whole of data contained on the hard drive, Welles' counsel was to submit a declaration to the court together with a written report signed by the expert explaining the limits of the retrieval actually achieved.

VI. RESISTING HIGH TECH DISCOVERY

A. In General

A party seeking to avoid discovery must show particular, specific, and demonstrable injury by facts sufficient to justify protection from discovery. *In re Amaya*, 34 S.W.3d 354, 356-357 (Tex.App.–Waco 2001, orig. proceeding), *citing*, *Masinga v. Whittington*, 792 S.W.2d 940, 940-941 (Tex. 1990) (orig.proceeding). TEX.R.CIV.P. 193.2 provides that a party must make any objection to written discovery in writing–either in the response or in a separate document–within the time for response.

Recall also that TEX.R.CIV.P. 196.4 sets outs the requirements for the discovery of electronic evidence. Under such rule, a number of potential objections, which go far to force the other side to play by the rules, stand out: (1) is the request for electronic or magnetic data specific?; (2) does the request specify the form in which such evidence is to be produced?; and (3) is such form reasonable? *See*, Boston and Tobias, at p. DD-13.

B. "Reasonable Efforts"

TEX.R.CIV.P. 196.4 specifically provides that "[i]f 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." A problem with the "reasonable

efforts" test is the unfortunate possibility of having to sift through thousands of electronic "pages" of data to identify information responsive to a discovery request. *Id*. Such a burden may not be reasonable "in the ordinary course of business," because it will be far easier to identify a specific item to restore from a back up tape than to search through "reams" of back up data for information relevant to a particular subject or request. *Id*.

It is, however, important to have the facts straight before making noises about "reasonable efforts." In *American Bankers Ins. Co. v. Caruth*, 786 S.W.2d 427, 436 (Tex.App.–Dallas 1990, no writ), for example, the party resisting discovery filed a response in which it stated that the information requested in discovery was contained in excess of 30,000 boxes. Later, the resisting party's computer staff testified that the resisting party had a sophisticated data base and computer which contained and could produce a great deal more information than was requested by the other side, and, in fact, could generate such discovery in approximately forty hours. *Id*.

The trial court, understandably, was not amused. It first sanctioned the resisting party $4,500 for its admitted failure to respond to the discovery requests, intentional withholding of requested items, and production of "worthless" documents, and, subsequently, upon continued noncompliance by the resisting party, not only struck its pleadings but conclusively deemed each and every allegation in the adverse party's pleadings to be true and prohibited the recalcitrant party from contesting the deemed truth of those allegations by putting on any testimony of a defense or mitigation of such claims. *Id*. The trial court's discovery sanctions were upheld on appeal. *Id*.

C. Immediately Challenge Protective Orders

A quick and swift response to a request for a non-destruct order should be filed. Usually, these requests are based upon nothing more than cursory and conclusory allegations that wholly fail to establish the opposition's entitlement to such an extraordinary remedy. Arguments that such requests are essentially a request for injunctive relief are being met with success in courts across the country. Parties should make a showing to the court that the opposition has failed to carry both their burden of proof and persuasion to entitle them to an injunction by arguing the following:

1. there is neither pleading nor proof of irreparable injury;

2. the party in question has undertaken efforts to preserve documents relevant to the issues in the litigation;

3. the requestor has an adequate remedy at law for any alleged document destruction issues that arise;

4. the entry of the order would be prejudicial for a number of reasons, including creating the misleading impression that the opposing party has, in fact, been engaged in the willful destruction of documents and records; and

5. there is no substantial likelihood of success on the merits.

Importantly, a party seeking monetary or evidentiary sanctions must still demonstrate that it was prejudiced by the destruction of information, i.e., that the destroyed information had some relevance to the litigation. Fishing expeditions will not be permitted. *See New York Nat'l Org. for Women v. Cuomo,* 182 F.R.D. 30 (S.D.N.Y. 1998).

D. Non-destruct Orders are Requests for Injunctive Relief

Federal courts are correctly perceiving the entry of a preservation order as an extraordinary imposition, to be sparingly utilized. Based on the remedy sought under the terms of the motions — that is, to "restrain and enjoin" the non-movant — the requests are, in essence, injunctions for which a moving party bears the heavy burden of proving its entitlement. *See Pepsi Bottling Co. of Olean v. Cargill, Inc.*, 1995 WL 783610 (D. Minn. 1995); *In re Potash*, 1994 WL 1108312 (D. Minn. 1994). Parties cannot escape the burden of proving entitlement to a preliminary injunction simply by couching the request as a "Preservation Order." *See* e.g., *Carson v. American Brands, Inc.,* 450 U.S. 79, 83 (1980) (Orders having the "practical effect" of granting or denying injunctive relief are considered injunctions for purposes of appeal). The Authors have located no reported Texas case discussing a "preservation order" in any context.

The elements for injunctive relief are: (1) a significant threat of irreparable harm to the moving party if the injunction is not granted; (2) the harm to that party outweighs the injury that granting the injunction would inflict on the non-movant; (3) the probability that moving party will succeed on the merits; and (4) the public interest. *See e.g. Commonwealth Insurance Co. v. Neal*, 669 F.2d 300, 303 (5th Cir. 1982); *Buchanan v. U.S. Postal Serv.*, 508 F.2d 259, 266 (5th Cir. 1975). Texas law is similar. In Texas, injunctive relief is proper where the applicant demonstrates the following four grounds for relief: (1) the existence of a wrongful act; (2) the threat of imminent harm; (3) the

existence of irreparable injury; and (4) the absence of an adequate remedy at law. *See*, *e.g.*, *Hues v. Warren* Petroleum Co., 814 S.W.2d 526, 529 (Tex.App.–Houston [14th Dist.] 1991, writ denied).

The movant bears the burden of persuasion on all four elements. *Neat*, 669 F. 2d at 303. Injunctions will not be issued simply to "allay the fears and apprehensions or to soothe the anxieties of the parties." *Humble Oil & Refining Co. v. Harang*, 262 F.Supp. 39 (E.D. La. 1966). While the *Humble Oil* case addressed the issue in the context of "hard copies," Judge Rubin's astute words in the case are just as applicable to electronic data:

> It is apparent that the plaintiff may be irreparably injured if the evidentiary documents necessary to prove its claim are destroyed or otherwise put beyond the reach of the court. But this is true in every situation in which proof of a claim rests on documentary evidence; the parties may be irreparably injured in the documents are destroyed. *Were the fact that a party to a lawsuit would suffer irreparable injury if a document were destroyed the sole test for the issuance of an injunction to prevent its destruction, injunctions should issue in every case in which important documents are within the control of either party, obviously, this is not done and it cannot and should not be done.* When the party who seeks an injunction shows potential irreparable injury, he has established merely one essential condition for relief.

Humble Oil, 262 F.Supp. at 42-43 (emphasis added).

In *Potash*, the court was asked to impose a preservation order patterned after the form order contained in the Manual for Complex Litigation. The *Potash* court, likening a preservation order to injunctive relief, held that the plaintiffs failed to demonstrate that, absent the entry of the preservation order, "irreparable harm" would result. 1994 WL 1108312 (D. Minn. 1994) at *8. The *Potash* defendants had taken appropriate steps to preserve documents and records for the litigation. *Id.* Under the stringent standard for injunctive relief, the plaintiffs' motion for a preservation order was dismissed.

Similarly, in *Cargill*, a proposed class of plaintiffs argued that, without a preservation order, they would have no guarantee that the defendants would maintain relevant evidence, particularly where there was management reorganization underway at the defendants' business. 1995 WL 783610 (D. Minn. 1995) at *2. The court rejected the argument, noting that, "[s]uch an Order, being in the nature of an injunctive remedy should only issue upon an adequate showing that equitable relief was warranted." *Id.* at *3. The court denied the motion, because the plaintiffs failed to present "[a]ny reliable showing that an irreparable injury could reasonably be expected to ensue." *Id.* at *4.

Be prepared to show that your client has implemented procedures to retain documents, and urge the court to find that there is no need for the burdensome and potentially prejudicial non-destruction order. *See Abdallah v. The Coca-Cola Co.*, No.1:98CV3679-RW, 1999 WL 527835 at *2 (N.D. Ga. 1999)("the Court finds no basis for concern regarding Coca-Cola's efforts to preserve all documents relevant to this lawsuit, and the motion is denied"); *Smith v. Texaco, Inc.,* 951 F. Supp. 109, 112 (E.D. Tex. 1997) (district court modified state court TRO to allow defendant to delete electronic records in ordinary course of business provided hard copies were kept); *In re Potash*, 1994 WL 1108312 at *8 (D. Minn. 1994)(document preservation order denied because defendants had "taken appropriate steps to preserve documents and records"); *Humble Oil & Refining Co. v. Harong*, 262 F.Supp. 39, 42-43 (E.D. La. 1966)(discussed above).Without a showing of need, the movants' motion should be denied. *Pepsi Bottling Co. of Olean v. Cargill, Inc.*, 1995 WL 783610 at *3-4 (D. Minn. 1995)(preservation order denied because plaintiff could not show that one was "needed"). The misleading implications of nefarious conduct on the part of non-movants that a "Non-Destruct" order may create cannot be justified when there is a total lack of proof on the part of the movant.

1. Preservation Order Must be Specific

Parties will often quote the Manual of Complex Litigation for support of the entry of a non-destruct order. They will pattern their proposed order on the model language offered in the Manual at section 41.34. The justifications for entry of such orders are briefly touched upon in Section 21.442 of the Manual:

> Before the commencement of discovery – and perhaps before the initial conference – the court should consider whether to enter an order requiring the parties to preserve and retain documents, files, and records that may be relevant to the litigation.

Significantly, the Manual goes on to note the dangers in issuing such orders as follows:

> Because such an order may interfere with the normal operations of the parties and impose perhaps unforeseen burdens, the judge should discuss with counsel at the first opportunity the need for a preservation order

> and, if one is needed, what terms will best serve the purposes of preserving relevant matter without imposing undue burdens. *A preservation order may be difficult to implement perfectly and cause hardship when records are stored in data- processing systems that automatically control the period of retention. Revision of existing computer programs to provide for longer retention, even if possible, may be prohibitively expensive (though print–out and retention of hard copies, or duplication of databases at periodic intervals before deletions occur, may be feasible).*

See, § 21.442 (emphasis added).

The Manual also provides that such an order should ordinarily permit destruction after reasonable notice to opposing counsel; if opposing counsel objects, the party seeking destruction should be required to show good cause before destruction is permitted. Further, the manual states that the order may also exclude specified categories of documents whose cost of preservation is shown to outweigh substantially the relevance in the litigation, particularly if copies of the documents are filed in a document depository or if there are alternative sources for the information. If relevance cannot be fairly evaluated until the litigation progresses, the manual advises that destruction should be deferred. As the issues in the case are narrowed, however, the court may reduce the scope of the order.

2. Any Order Should be a Two-Way Street

And of course, such an order should surely apply to the movant as well. Would such an order, for example, allow the non-movants to seek and obtain documents from "others" suing them with whom movants and their counsel have contact and perhaps alliances? What prejudice would non-movants suffer if those "other" non-parties destroy documents while the case is pending?

E. Narrowly Define the Scope of Electronic Discovery

Parties are not entitled to conduct wholesale fishing expeditions under the guise of electronic discovery. The Federal Rules of Civil Procedure prior to 1970 spoke of the right to discover "documents and tangible things," leaving the right to electronic discovery to be fought out on a case-by-case basis. In 1970, Rule 34(a) was amended to clearly encompass electronically stored data. It now provides:

> Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phonorecords, *and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably useable form*), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served..

See, Fed.R.Civ.P. 34 (emphasis added).

The Advisory Committee Note (ACN) to the 1970 amendment stated that:

> [t]he inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made useable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into useable form.

Since the rule change, there is no question that the rule applies to computer records. *See, Crown Life Ins. Co. v. Craig*, 995 F2d. 1376, 1382-83 (7th Cir. 1993) (failure to provide computerized records on grounds that raw data in a computer was not a "document" under Rule 34 resulted in sanctions). "[T]oday it is blackletter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.,* 94 Civ. 2120, 1995 W.L. 649934 (S.D.N.Y. 1995). The amendment to Rule 34 to add "data compilations" was intended,

however, to extend only to "ordinary business records" kept by computers. *See, Pearl Brewing v. Jos. Schlitz Brewing*, 415 F. Supp. 1122, 1136 (S.D.Tex. 1976); Manual for Complex Litigation (Third), Section 21.446 ("information generated and maintained in the ordinary course of business").

F. Seek Limitations on the Scope of Discovery

The discovery rules of the Federal Rules of Civil Procedure and of most states allow for discovery to be limited by the court if it determines, on motion or on its own initiative and on reasonable notice, that:

> 1. the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; or
>
> 2. the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

See, Federal Rules of Civil Procedure 26(b)(2).

Moreover, the recent changes to the Federal Rules of Civil Procedure, effective December 1, 2000, include revisions to Rule 26 which incorporate the cost-bearing analysis provision into Rule 26(b)(2) rather than having such analysis referenced only in Rule 34(b). With the availability of Rule 26(b)(2), courts can and do balance likely benefits of the proposed discovery against the burden of production and may require requesting parties to pay some or all of the extraordinary costs associated with that production. *See, Sattar v. Motorola Inc.,* 138 F. 3d 1164, 1171 (7th Cir. 1998) (district court affirmed in decision to allow defendant to download 210,000 pages of e-mail messages into a readable format disk as opposed to printing them out, or alternatively, requiring Defendant and Plaintiff to split costs of paper printouts if e-mail is not readable in downloaded form); *see also*, *Playboy Enterprises, Inc.,* 60 F. Supp. 2d at 1054 (court required requesting party to bear cost of having forensic expert make mirror image of defendant's hard drive); *Zonaras v. General Motors Corporation*, 1996 U.S. LEXIS 22535 (S.D. Ohio 1996) (requiring Plaintiff to pay half the cost of producing data regarding test documentation). [Note some attorneys like to argue that the limitations should not be imposed until they have made several attempts to obtain all that they deem exists, citing an additional provision in Rule 26(b)(2) which provides: "(ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the discovery sought . . . ."]

Many courts have limited e-discovery requests based on FRCP 26(b)(2). *See, Fennell v. First Step Designs, Ltd.,* 83 F.2d 526, 534 (1st Cir. 1996) (affirming district court's decision not to permit access to a party's hard drive in order to investigate the date on which a document had been created or modified); *Van Westrienen v. Americontinental Collection Corp.,* 189 F.R.D. 440, 441 (D. Ore. 1999) (holding that "Plaintiffs are not entitled to unbridled access [of] defendants' computer system... . Plaintiffs should pursue other less burdensome alternatives, such as identifying the number of letters and their content"); *Symantec Corp. v. McAfee Assocs., Inc.,* 1998 WL 740807, at *3-4 (N.D. Cal. 1998) (holding that plaintiff's request for the production of copies of all hard drives that had access to a specific server was unduly burdensome); *Strasser v. Yalamanchi,* 669 So.2d 1142, 1144-45 (Fla. Dist. Ct. App. 1996) (holding that while plaintiff's request to search defendant's computer system was within the scope of Florida's discovery rules, the inspection sought by the plaintiff was overly broad since the order sought by the plaintiff would have been given the plaintiff unfettered access to defendant's entire computer systems which could cause defendant irreparable harm); *In re Brand Name Prescription Drug Antitrust Litig.*, No. 94-987, 1995 U.S. Dist. LEXIS 8281, at *7-8 (N.D. Ill. June 13, 1995) (narrowing broad requests of plaintiffs and requiring parties to agree upon meaningful limitations on the scope of any e-mail search); *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F.Supp. 11, 13-14 (S.D.N.Y. 1994) (quashing a grand jury subpoena for all computer hard drives and floppy disks as unreasonably broad).

The court in *Marker v. Union Fidelity Life Insurance Company,* 125 F.R.D. 121, 122-23 (M.D.N.C. 1989), also followed the principles of FRCP 26(b)(2). In that case, the party seeking discovery showed that production of data could be done inexpensively due to computer storage, but the court still found the seeking party failed to show a particularized need for past litigation and claims history of the insurance company when the case involved only coverage and not bad faith. Also, in *Lawyers' Title Insurance Company v. United States Fidelity & Guaranty Company,* 122 F.R.D. 567, 570 (N.D. Cal. 1988), the district court took a very strong position in favor of protecting computerized information systems when an insured filed a coverage claim against an insurance company. The court concluded that without some showing that the insurance company failed to respond to discovery requests, it would not require disclosure of a computerized system of information management. "The mere possibility that a party might not produce all relevant, unprotected documents, is not a sufficient basis for ordering such a party to disclose its entire computerized system of information management."

However, in *Momah v. Albert Einstein Medical Center*, 164 F.R.D. 412 (E.D.Pa. 1996), the plaintiff in a Title VII case was permitted to discover the defendant's "computer list files screen" which would display information about the dates on which documents were created and last edited. *See also, Playboy Enterprises, Inc. v. Welles,* cited and discussed, *infra,* in which the court fashioned an elaborate protocol to be followed in the production of files from defendant's hard drive. This protocol was also used in *Simon Property Group v. MySimon, Inc.,* 2000 WL 863035 (S.D. Ind. 2000).

G. Demonstrate the Data Exists in Other Form

It might be possible to demonstrate to the trial court that the requested data exists in a form other than electronic evidence (*e.g.*, paper documents). In other words, the requesting party should be required to prove that the electronic data is relevant to the case. *See*, TEX.R. EVID. 402 ("[a]ll relevant evidence is admissible....[e]vidence which is not relevant is inadmissible"); *see also*, *Prestige Ford Co. Ltd. Partnership v. Gilmore*, 56 S.W.3d 73, 80 (Tex.App.–Houston [14th Dist.] 2001, pet. denied) (computer printout listing all employees and their birthdates was relevant and admissible evidence in an age discrimination action by an employee alleging he had been terminated as result of his age, since such evidence could be used to demonstrate that the employer retained other similarly-situated employees who were as old or older than the former employee).

The capability to reconstruct the past in minute detail using electronic documentation does not necessarily imply a need to do so in every case. Such reconstruction may only be justified when the attempted deletion of electronic documents is itself an issue in every case. *See, e.g., Playboy Enterprises, Inc.*, 60 F. Supp. 2d 1050. For instance, if discovery of deleted documents will only reveal that the readily-available electronic documents were preceded by drafts, or that in the normal course of business, prior to litigation or the anticipation thereof, many routinely generated docuents were considered non-essential, is the expense of reconstruction justified.

If electronic evidence is not a relevant, substantive piece of evidence, then the discovery of such is an improper expansion of the scope of permissible discovery. *See, e.g.*, *Fennell v. First Step Designs, Ltd.,* 83 F.3d 526 (1st Cir. 1996) (the court denied a discharged employee's motion to permit discovery of the contents of his employer's hard drive; the plaintiff had failed to demonstrate a "particularized likelihood of discovering appropriate information," and any alleged benefit was outweighed by the substantial risks and costs of the process, including the risk of exposing confidential information).

VII. ADMISSIBILITY OF HIGH TECH EVIDENCE

A. Foundation

One of the most common reasons courts have rejected computerized evidence is lack of sufficient foundation. One court in particular has displayed outright hostility to the use of information obtained from the Internet, seeing it as inherently untrustworthy:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in Fed.R.Civ.P. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form from the United States Coast Guard or discover alternative information verifying what Plaintiff alleges.

St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F.Supp.2d 773, 774-75 (S.D. Tex. 1999). While most practitioners may not encounter this extreme of a response when trying to get electronic evidence admitted at trial, it illustrates the skepticism and reticence with which many courts address this issue.

1. Satisfy Appropriate Accuracy Standards

Courts and commentators have voiced concerns about the reliability, accuracy, and authenticity of computer records. For example, the Manual for Complex Litigation notes that the accuracy of computerized records may be impaired

as the result of computer programming errors, equipment malfunction, and data entry errors. *See,* Manual for Complex Litigation §21.446 (3d ed. 1995). The Manual also notes that due to the volume of relevant electronic data courts may receive in any given case, the court's ability to verify the accuracy and truth of the data may be impaired. In order to confront these concerns head-on, lawyers must be prepared to satisfy the established accuracy standards when presenting electronic evidence.

Courts in a few early cases were skeptical about electronic evidence. Due to concerns about the veracity and accuracy, courts set out more extensive foundation requirements for electronic data than for conventional records. In *United States v. Scholle*, the court held the proponent of the electronic data must specify "the original source of the computer program . . . . and the procedures for input control including tests used to assure accuracy and reliability" as part of the foundation to assure reliability. *United States v. Scholle,* 553 F.2d 1109, 1125 (8th Cir. 1977). Other courts have rejected printouts of such electronic data in a similar fashion. *See, Potamkin Cadillac Corp. v. B.R.I. Coverage Corp*., 38 F.3d 627, 631 (2nd Cir.1994). The court in *Potamkin* denied admission of a printout generated by the defendant's computer because the defendant failed to establish that it was prepared from original computer data and compiled in accordance with regular business practice. Furthermore, there was insufficient evidence of the reliability of the information in the printout. *Id.*

However, more recently, some courts have relaxed foundation standards. In *United States v. Vela*, the Fifth Circuit affirmed the admission of electronic evidence even though the proponent's foundation witness failed to identify the exact computers used to create the records and did not verify that the computers were operating properly at the time. *United States v. Vela,* 673 F.2d 86, 90 (5th Cir.1982). The court stated the "failure to certify the brand or proper operating condition of the machinery involved does not betray a circumstance of preparation indicating any lack of trustworthiness." *Id.*

In criminal matters, the Texas Rules of Criminal Evidence do not appear to contemplate any particular predicate for the introduction of computer generated evidence. *Ly v. State*, 908 S.W.2d 598, 606, n. 3 (Tex.App.–Houston [1st Dist.] 1995, no pet.). The proper analysis for the introduction of computer generated evidence thus would be the balancing test of TEX.R.CRIM.EVID. 403, as to whether such evidence, though relevant, had probative value which was not substantially outweighed by the danger of unfair prejudice, confusion of the issues, misleading the jury, or considerations of undue delay or needless presentation of cumulative evidence. *Id.*

2. Utilize the Proper Foundation Witness

Proper foundation for admitting a computer printout as a business record should establish, through the testimony of the custodian of the computer-kept records or other person familiar with the manner in which the records were processed and maintained, the following:

1. the reliability of the data processing equipment used to keep the records and produce the printout;
2. the manner in which the basic data was initially entered into the system (for example, keyboard, cards, teletype, etc.);
3. that the data were so entered in the regular course of business;
4. that the data were entered within a reasonable time after the events recorded by persons having personal knowledge of the events;
5. the measures taken to insure the accuracy of the data as entered;
6. the method of storing the data (for example, magnetic tape) and the safety precautions taken to prevent loss of the data while in storage;
7. the reliability of the computer programs and formulas used to process the data;
8. the measures taken to verify the proper operation and accuracy of these programs and formulas; and
9. the time and mode of preparation of the printouts.

See, William A. Fenwick, Gordon K. Davidson, *Admissibility of Computerized Business Records*, 14 Am. Jur. Proof of Facts 2d 173, §17 (Supp. 2000).

In another example, *U.S. v. Catabran*, a prosecution for concealing assets during a bankruptcy proceeding, the district court admitted into evidence the general ledger computer printouts and a summary chart compiled from them under the business records exception through the testimony of a bookkeeper. *U.S. v. Catabran*, 836 F.2d 453 (9th Cir.1988). The bookkeeper from the insolvent company laid the foundation for their admissibility,

testifying that she entered the sales, inventory, payroll and tax information on a current basis, the printouts accurately set forth that information, the business produced these printouts as a regular practice each month, and that she manually checked the information put into the computer for accuracy. *Id.*

In some cases, the witness need not necessarily have personal knowledge of the data as input into the system, or personal knowledge of the actual operation of the computer system. All that is required is that the witness is familiar with the methods employed by the company in processing the business records. *American Oil Co. v. Valenti,* 179 Conn. 349, 426 A.2d 305 (1979). However, in other cases, courts have required that an employee with knowledge of the way in which records are created and kept in the ordinary course of business provide the foundation for the admissibility of electronic records into evidence. In one such case, a Tenth Circuit court held the proper foundation was laid by two IRS employees who testified a taxpayer's computer-generated records were kept in the ordinary course of business and it was a regular IRS practice to keep such records. *See*, *U.S. v. Hayes,* 861 F.2d 1225, 1228 (10th Cir. 1988).

In a Ninth Circuit opinion, the court found that a bookkeeper who routinely kept general ledger accounts laid a proper foundation for their admission into evidence. The court noted the following facts were relevant: (1)she entered the sales, inventory, payroll and tax information on a current basis; (2)the printouts accurately set forth that information; (3)the business produced these printouts as a regular practice each month; and (4)she manually checked the information put into the computer for accuracy. *See, U.S. v. Catabran*, 836 F.2d 453 (9th Cir.1988). In another case, the court allowed a manager from Southwestern Bell to establish the reliability and foundation of AT&T's records of telephone calls. *See, State v. Dunn*, 7 S.W.3d 427 (Mo. App. W.D. 1999). The court found Southwestern Bell regularly keeps telephone records for long distance companies and bills customers on their behalf. *Id.*

The party testifying to or offering the record need not be the author of the record. *Hardison v. Balboa Ins.*, No. 00-6100, 2001 U.S. App. LEXIS 2409 at *13 (10th Cir. February 16, 2001). The foundation for the business records exception to the hearsay rule may be established by anyone demonstrating sufficient knowledge of the record-keeping system that produced the document. *Id.* Some courts have required even less.

With regard to the admission of evidence found on a web-site, a federal district court held it was sufficient for a witness with knowledge to attest to the fact that the witness logged onto the web-site and described what he or she saw. *See, Van Westrinien v. Americontinental Collection Corp.*, 94 F.Supp.2d 1087, 1109 (D. Or.2000). Finally, a Connecticut court held that the testimony of an asset analyst regarding computer evidence of the amount of mortgage debt in a foreclosure action could establish foundation because the analyst had sufficient knowledge of the reliability of the evidence. *SKW Real Estate Limited Partnership v. Gallicchio*, 716 A.2d 903 (Conn. App. 1998).

3. Establish Authenticity

TEX.R.EVID 901 mandates authenticity; the requirement that a record be authenticated seeks to assure that a record is what it is purported to be. Failure to authenticate a document renders it inadmissible, even if it otherwise is relevant and admissible. *See, e.g., Castro v. Sebesta*, 808 S.W.2d 189, 195 (Tex.App.–Houston [1st Dist.] 1991, no writ).

Rule 901 provides a variety of methods to authenticate evidence. Although the authentication of electronic evidence is not specifically provided for in Rule 901, it is possible that electronic evidence could be authenticated by the testimony of a witness with personal knowledge (Rule 901(b)(1)), or by other means. Rule 901 does not limit the manner in which evidence may be authenticated. However, because evidence must be authenticated, a lawyer should take care to preserve a chain of custody, as discussed below. It should be noted that an expert may be critical if issues arise about authenticity or the capacity to "accurately" retrieve information. *See*, Boston and Tobias, at p. DD-12.

In *City of Mesquite v. Moore*, 800 S.W.2d 617, 619 (Tex.App.–Dallas 1990, no writ), the defendant objected to a computer printout of payroll information, the underlying information for which had been provided to the plaintiffs by the defendant during discovery. However, held the Dallas Court of Appeals, the cover letter to such calculations stated that the defendant had furnished the calculations to the plaintiffs, and hence, the defendant itself had sufficiently identified the computer printout for purposes of admission. *Id.* Recall that TEX.R.CIV.P. 193.7 provides that if a party produces a document in response to written discovery, then such document is authenticated, with few exceptions, against the producing party (the most important exception is that the document is authenticated unless the producing objects to its authenticity within ten days of notice that such document will be used in pre-trial proceedings or at trial). It has been said that, read in conjunction with TEX.R.CIV.P. 192.3(b), Rule 193.7 will self-authenticate computerized documents produced in discovery. *See*, Jacks and Wright, at p. 9.

On the other hand, some courts have found certain electronic evidence inadmissible because it lacks authenticity. For example, web postings introduced as evidence regarding responsibility for racist mailings were inadmissible because defendant failed to show the postings were authentic and created by a third party. *See, U.S. v. Jackson,* 208 F.2d 637 (7th Cir. 2000). However, in *People v. Foley*, a trooper's testimony regarding the accuracy

and authenticity of a computer disk containing notes of conversations between the trooper and defendant was sufficient to admit the disk. *People v. Foley*, 257 A.D.2d 243, 692 N.Y.S.2d 248 (N.Y.A.D. 1999).

Occasionally, courts have allowed electronic evidence to be self-authenticating. In a recent Eleventh Circuit case, the court allowed for the authentication of an e-mail by reference to its appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with surrounding circumstances. *See, U.S. v. Siddiqui,* 215 F.3d 1318, 1322 (11th Cir. 2000). The court found the following dispositive: (1) the e-mail contained sender's email address; (2) the address matched that of e-mail used by defendant's counsel in cross-examination; (3) the use of the reply function by its recipient automatically called up defendant's address; and (4) the use of defendant's nickname in the e-mail. *Id*. E-mail may also be self-authenticating either under FED. R. EVID. 902(7) for trade inscriptions or the like when the name of company or organization appears in the email address, or when produced by the party opponent during discovery. *See, Superhighway Consulting, Inc. v. Techwave, Inc*., 98 CV 5502, 1999 WL 1044870, at *2 (N.D.Ill. Nov.16, 1999).

Other arguments to utilize when trying to authenticate evidence obtained from a web-site include: (1)the evidence consists of information that is typical of the information on the web-site; (2)the general content of the web-site consists of information that nobody but the claimed author would likely to put there; (3)the client's lack of computer sophistication and inability to have tampered with the evidence; (4)the length of time the evidence was on the web-site, if the lawyer can document that it was there for a long time; and (5)the evidence is still on the web-site and can be viewed by the judge, if that is the case. *See,* James L. Dam, *Lawyers Are Getting Web-sites Admitted as Evidence at Trial: Cheaper and Faster Way to Prove a Case*, LAW. WKLY. USA, May 28, 2001, at 18.

B. Hearsay

Computer records, like other written documents, are created out of court and are considered hearsay. Therefore, computer records cannot be admitted unless they should fall under one of the exceptions to the hearsay rule.

1. Business Record Exception

Gradually, because of the present day importance and necessity of keeping records in computerized format, legislatures and courts have extended the business records exception to the hearsay rule to include computer records. However, proponents of electronic evidence still encounter difficulties in utilizing the business records exception.

To take advantage of this exception, proponents of the evidence must show the record was: (1)made by someone with personal knowledge, or from information provided by someone with personal knowledge, and a duty to report; (2)made in the regular course of business, at or near the time the recorded event occurred; and (3)the type of record the business regularly makes. *See generally*, FED. R. EVID. 803(6). Under this rule, courts may admit any "memorandum, report, record, or data compilation, in any form" that satisfies the foundation requirements. *Id*. The Advisory Committee notes recognize "'data compilation' is used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage." FED. R. EVID. 803(6) Advisory Committee's Note.

In the landmark case of *Transport Indemnity v. Seib*, the court recognized that the business records exception was broad enough to authorize admission of computer records. *Transport Indemnity v. Seib*, 132 N.W. 2d 871 (Neb. 1965). In *Seib*, the plaintiff insurance company attempted to introduce a computer printout to prove the premiums due on a policy. The director of accounting testified to the accuracy of the printout including the fact that he had manually verified each of the calculations. His foundational testimony took up 141 pages of the record. The court admitted the entire printout.

An Illinois court provided a detailed analysis of e-mail evidence under FED. R. EVID. 803(6) in *Rick v. Toyota Industrial Equipment Co.* No. 93 C 1331, 1994 WL 484633 (N.D.Ill.Sept. 2, 1994). The court considered the admissibility of an e-mail inventory list under the business record exception. Although the court rejected the evidence because it was prepared in anticipation of litigation, was not prepared at or near the time of the event, and was not prepared by someone with knowledge, the court did recognize e-mail could qualify under the business record exception. Several other courts have considered this problem. *See e.g.*, *People v. Markowitz*, 721 N.Y.S. 2d 758 (NY Supp. 2001) (computerized records of deposits at a toll bridge were maintained in the regular course of business); *see also, Commonwealth v. McEnany*, 732 A.2d 1263 (Pa. Super. Ct. 1999) (computer records of cell phone company were not prepared for litigation, but kept in the ordinary course of business).

In another recent example, *U.S. v. Ferber*, the offering party attempted to introduce an e-mail under the business records exception. *U.S. v. Ferber*, 966 F.Supp. 90 (D.Mass.1997). An employee, Carey, sent an e-mail to his superior. The e-mail recounted a conversation between Carey and the defendant, Ferber, in which Ferber inculpated himself. The e-mail revealed the inculpating remark. Carey also noted in the e-mail that he had consulted with a co-worker concerning this conversation. In support of the argument that the e-

mail was a business record, Carey testified that it was his regular course of business to report such activities via e-mail to his superiors. The court refused to admit the e-mail finding insufficient evidence that the employee was required to maintain such records.

2. Excited Utterance and Present Sense Impression

In *U.S. v. Ferber*, supra, after failing to get the e-mail admitted under the business records exception, the government sought to admit the e-mail by utilizing the excited utterance exception in FED. R. EVID. 803(2). The government argued the employee wrote the message shortly after his conversation with the defendant and the employee felt "upset and panicked" following the conversation. The court refused to admit the e-mail under FED. R. EVID. 803(2) finding that this was not the typical outburst that qualifies as an excited utterance.

After unsuccessfully attempting to admit the e-mail under the business records and excited utterance exceptions, the government finally tried the present sense impression exception. Under this exception, "[a] statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter," even though the statement would normally be hearsay and the declarant is available as a witness. FED. R. EVID. 803(1). The court admitted it into evidence, finding that the nature and tone of the e- mail and the circumstances surrounding its composition qualified as a present sense impression.

3. Public Records

Over twenty years ago, in *United States v. Orozco*, the Ninth Circuit held that certain government computer records qualified as public records and thus were admissible under FED. R. EVID. 803(8). *United States v. Orozco*, 590 F.2d 789, 793-94 (9th Cir.1979). More recently, the Ninth Circuit also held that computer generated Internal Revenue Service documents were admissible as public records. *Hughes v. United States,* 953 F.2d 531, 539-40 (9th Cir. 1992).

4. Market Reports and Commercial Publications

A federal district court has recently held that prime rates published on the Bloomberg website satisfied the market reports and commercial publications exception to the hearsay rule See *Elliott Assocs., L.P. v. Banco de la Nacion*, 194 F.R.D. 116, 121 (S.D.N.Y. 2000); *see also*, FED. R. EVID. 803(17). Also, the blue-book value of a vehicle obtained from a web-site was admissible to prove the value of a vehicle under the market reports, commercial publications exception. *See*, *State v. Erickstad*, 620 N.W.2d 136, 145 (N.D. 2000) citing *Irby-Greene v. M.O.R., Inc.*, 79 F.Supp.2d 630, 636 n.22 (E.D. Va. 2000).

5. General Catch-All

Some courts and litigants also rely on a general "catch-all" hearsay exception. In *Palmer v. A.H.Robins Co*., the Colorado Supreme Court admitted computer records into evidence under the common law "general hearsay exception." *Palmer v. A.H. Robins Co*., 684 P.2d 187, 202 (Colo. 1984). The court explained that the data, while not a business record, was sufficiently reliable to be admitted into evidence. The Federal Rules of Evidence includes a catch-all hearsay exception. See FED. R. EVID. 807.

6. Admission By Party Opponent

Lawyers have also attempted to maintain that electronic evidence is an admission by party opponent A Vermont court held that e-mails in the form of an insured's intra-company correspondence indicating that expert reports were not conclusive on an issue in dispute with the insurer were admissions by a party opponent and therefore not hearsay. *See, Vermont Elec. Power Co., Inc. v. Hartford Steam Boiler Inspection & Ins. Co.*, 72 F.Supp.2d 441, 448-49 (D. Vt.1999); see also FED. R. EVID. 801(d)(2). Another court held that representations made by the defendant on the defendant's web-site were admissible as admissions of a party opponent under Federal Rule of Evidence 801(d)(2)(A). *See, Van Westrinien v. Americontinental Collection Corp*., 94 F.Supp.2d 1087, 1109 (D. Or. 2000). Lawyers have also begun to utilize the admission by party opponent method as an alternative to the business records exception. One court held computerized business records that were inadmissible under the business records exception when offered by the owner of the records may be admissible as an admission by a party opponent. *See, Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.,* 38 F.3d 627, 633-34 (2nd Cir. 1994).

C. Best Evidence

A party attempting to prove the contents of a writing must produce the original writing, if available, as the "best evidence" of what the writing states. Although the objection may prove to be futile, parties should object to computer printouts as not consisting of the best evidence of what is written on the printout. For example, a party could object the printout is merely a copy of the original data recorded in the computer memory or on computer tape. However, as one court has recognized, the recorded data would be impossible for humans to read, and a printout is the best evidence of the data recorded in the memory or on tape. *King v. State ex. Rel. Murdock Acceptance Corp.*, 222 So.2d 393 (Miss. 1969). Furthermore, Federal Rule of Evidence 1001(3) states a computer printout is an original copy of the record. In another example, computer printouts of travel bookings stored on computer tape were admissible where the party

provided proper foundation that the printouts were accurate reflections of the stored data. *United Air Lines, Inc. v. Hewins Travel Consultants, Inc.*, 622 A.2d 1163 (Me. 1993).

Another possible objection might be that a computer printout of records stored on the computer is not the best evidence because the information was obtained from another source, such as invoices, and then entered into the computer. However, where the original paper records have been destroyed in the regular course of business, courts have held that the computer printout of the records is the best evidence. For example, a computer printout of prior misdemeanor convictions was admitted where the district court clerk testified the printout was true and accurate and the old case jackets had been archived or destroyed once the information was entered into the computer. See *Hill v. Commonwealth*, 779 S.W.2d 230 (Ky. App. 1989).

D. Voluminous Writings

Additionally, courts have permitted parties to introduce an extracted summary or part of the information contained in the record under the "voluminous writings" exception in the Federal Rules of Evidence 1006. In a recent case involving attorneys' fees, the court allowed computer printouts of summaries of billing records to be admitted as long as the full volume of original documents was made available to the opposing party at its request. *In re: Marriage of DeLarco,* 728 N.E.2d 1278 (Ill. App. 2000).

VIII. SPOLIATION

Certain commentators have written that the first step in discovery of electronic evidence is to "learn the law spoliation." *See*, Tottenham, *et. al.*, at p. 5. Such commentators may well be correct, for reasons which will become more evident hereinbelow.

A. In General

The concept of spoliation of evidence existed long before the proliferation of computers in modern commerce and modern day to day existence. Spoliation refers to the destruction, significant alteration or non-preservation of evidence that is relevant to pending or future litigation. *See*, Bell, Koesel, and Turnbull, 29 Ariz. St. L.J. 769, 770 (1997). It is a broad concept that generally encompasses all discoverable evidence without regard to its admissibility at trial. *See*, Gorelick, Marzen & Solum, *Destruction of Evidence*, §1.1, pp. 4-5 (2d ed. 1989).

When spoliation occurs, it gives rise to an inference that the destroyed evidence was harmful to its destroyer. *See, e.g., Trevino v. Ortega*, 969 S.W.2d 950, 953 (1998). The inference arises in the context of the lawsuit in which the spoliation occurs, not in a separate suit, and allows the fact finder to deduce that the destroyed evidence was incriminating and that the accused therefore is guilty. *Id.* at 952.

The spoliation inference, can be traced as far back as the 1600's. *See, Rex. v. Arundel*, 1 Hob. 109, 80 Eng. Rep. 258 (K.B. 1617). Since that time, the spoliation inference has been one of the primary tools used by courts to remedy spoliation. A sample spoliation instruction to a jury might read:

> You are instructed that if the plaintiff has established by a preponderance of the evidence that the defendant or its agents or employees destroyed, negligently misplaced, or discarded any evidence, then you must presume that the missing evidence would have been unfavorable to the defendant and favorable to the plaintiff.

See, Brewer v. Dowling, 862 S.W.2d 156, 159 (Tex.App.–Fort Worth 1993, writ denied); *see also, Watson v. Brazos Electric Power Cooperative, Inc.*, 918 S.W.2d 639, 643 (Tex.App.–Waco 1006, writ denied).

A few states have created independent tort causes of action for spoliation. The majority, however, continue to rely on more traditional remedies. *See, Trevino*, 969 S.W.2d at 952, n.3. Texas follows the majority position and has declined the opportunity to create a new cause of action for spoliation of evidence. *Id*.

Additionally, the Dallas Court of Appeals recently declined to recognize an independent cause of action against third parties for spoliation. *See*, *McIntyre v. Wilson*, 50 S.W.3d 674, 686 (Tex.App.–Dallas 2001, pet. denied); *see also, Scolaro v. State ex rel. Jones*, 1 S.W.3d 749, 755 (Tex.App.–Amarillo 1999, no pet.) (the doctrine of spoliation only applies to the conduct of the parties).

Spoliation is a very operative concept in today's family law litigation. Anecdotes abound, from the simple but intentional deletion of emails to a boyfriend or girlfriend to the egregious, actual destruction of family hard drives.

B. Spoliation in Texas: *Trevino v. Ortega*

In *Trevino*, Ortega filed a medical malpractice action against his daughter's doctor for negligent care during birth. When Ortega was advised that his daughter's birth medical records had been destroyed, he filed a separate action alleging that the records had been intentionally, recklessly or negligently destroyed, and thus, as a result, he would suffer an "insurmountable hardship in the preparation of his medical malpractice suit." *See, Ortega v. Trevino*, 938 S.W.2d 219 (Tex. App.–Corpus Christi 1997), *rev'd and rendered,* 969 S.W.2d 950 (1998). Ortega sought damages in the amount that would have been recovered in the

medical malpractice action, but for the destruction of the medical records. Trevino specially excepted to Ortega's petition arguing that it failed to state a cause of action, *i.e*., that Texas did not recognize an independent cause of action for intentional or negligent spoliation of evidence. The trial court sustained the special exception and dismissed the lawsuit. *Id*. at 220.

According to the Corpus Christi Court of Appeals, even though Texas courts discourage spoliation of evidence by pre-trial sanctions and by instructing the jury to infer that destroyed evidence is presumed to have favored the opposing party, such traditional remedies are not always sufficient to deter spoliation or to compensate the party wronged. *Id*. The Corpus appellate court noted that other jurisdictions recognize an independent tort for intentional spoliation of evidence. The Thirteenth Court of Appeals also recognized that, while there were no Texas cases allowing recovery for a separate tort of spoliation of evidence, certain legal concepts might support the adoption of an independent tort. *Id*. at 22-223. For instance, noted the court, Texas recognizes a claim for money damages in a civil lawsuit as an interest in property belonging to a plaintiff. Therefore, by destroying a plaintiff's ability to prove their claim through the destruction of evidence, the spoliator has destroyed a property interest which Texas law would otherwise protect as an asset of the plaintiff. Thus, the Corpus Christi appellate court concluded: "we see no reason why Texas should not protect a plaintiff's property right in a prospective civil claim in a similar action by adopting the independent tort for spoliation of evidence in an appropriate factual situation." *Id*. at 223. The Corpus Christi Court of Appeals therefore held that Trevino's special exception that Texas did not recognize the tort of intentional or negligent spoliation of evidence was overly broad, and it was therefore error for the trial court to dismiss Ortega's lawsuit based solely on that ground. *Id*.

The Texas Supreme Court, however, disagreed. The Court noted that spoliation causes no injury independent from the cause of action in which it arises, and that any resulting damages are speculative. *Trevino*, 969 S.W.2d at 952. The Texas Supreme Court concluded that ensuring the finality of judgments and avoiding duplicative lawsuits outweighed the need to create a new cause of action, specifically acknowledging that, if a new and independent cause of action were created, it could allow a plaintiff to collaterally attack an unfavorable judgment. *Id*. Even though the Court expressed its concern that there must be adequate remedies to balance the parties' rights when spoliation occurs, the court concluded that existing remedies were sufficient. *Id*.

For example, the Texas Supreme Court pointed to the broad discretion of trial courts to impose a variety of sanctions, ranging from the striking of pleadings to including a spoliation instruction in the jury charge. *Id*. Consequently, the Court concluded that the more practical and logical approach would be to address the spoliation issue in the context of the lawsuit in which it occurred, through the use of traditional remedies, rather than creating a new cause of action. *Id*.

Justice Baker, in his concurring opinion, provided a helpful and detailed scheme for analyzing if spoliation has occurred, and the application of an appropriate sanction, if any. According to Justice Baker, if a party believes that another has improperly destroyed evidence, it should either move for sanctions or request a spoliation presumption instruction; it then becomes the trial court's duty to determine whether a sanction is appropriate. *Id*. Justice Baker continued to state that the legal inquiry involves determining whether there was a duty to preserve the evidence, whether the spoliator acted negligently or intentionally, and whether the spoliation prejudiced the non-spoliator's ability to present its case or defense. *Id*. at 954.

Currently, Texas trial courts may punish those who engage in the spoliation of evidence by using the full range of sanctions available to trial courts under Rule 215 including: death penalty sanctions, the exclusion of evidence or testimony, the rendition of a default judgment, and/or the payment of fees and costs associated in remedying the abusive conduct. In addition, courts may also give the jury the spoliation inference instruction.

C. Spoliation in the Electronic Age

Electronic evidence is invisible; it exists as electronic impulses, or bits, in a computer, represented by a series of "on" (1) or "off" (0) conditions. Put another way, such on/off options mean that all representations use the binary numbering system (base 2 as contrasted with the decimal numbering system that most of us learned in school, base 10, or the number 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9). Characters or numbers are represented by a series of on/off combinations. Generally, eight bits (electronic impulses) make a character. For example, the capital letter M is represented by these eight bits "1101 0100" and the small letter m is represented by these eight bits "1001 0100."

Thus, one can easily see that changing one bit will alter the character representation. Because minor changes can have a dramatic impact on the electronic information, spoliation, whether intentional or unintentional, may occur more easily. Not only can the information itself be changed, but the dates within the computer can be altered as well. Altering dates within the computer itself may also lead to the easy destruction or alteration of electronic evidence.

For instance, these Authors handled a divorce case in which the husband, in an effort to avoid the effect of a court order for the preservation of electronic evidence on his computer, changed the computer's clock and then deleted a mountain of emails to his paramour, intending that the wrongful alteration would then appear to have been made prior to the court's order. However, it availed him naught. Modern technology has virtually ensured

that data which was previously thought to have been deleted from a computer may still actually be recovered, as this particular opponent later, and painfully, learned.

Indeed, it is often startling to note the lengths that parties will go to ensure that data on a particular hard drive is not recoverable. In *Illinois Toolworks, Inc. v. Metro Mark Products Ltd.,* 43 F. Supp. 2d 951 (N.D. Ill. 1999), for example, the District Court entered an order requiring that all defendants preserve the integrity of all computers that were at issue without any spoliation of information contained therein. The court was very specific about what its order meant: "...don't push the delete button....don't change the C drive....don't pull the plug at the wrong time....don't take a sledge hammer to it....I don't want it spoiled in any way, ok, so don't limit it." *Id*. at 954.

Nevertheless, the evidence revealed that, during the course of attempted discovery of information stored on one Packard Bell computer belonging to the defendant, the computer had been struck by a falling air compressor, had fallen off of a desk on four separate occasions in the span of two years and had been dropped by the defendant immediately prior to its inspection at the plaintiff's offices. There was additional evidence that the cables connecting both the hard drive and the floppy drive to the motherboard had been completely disconnected, thus giving the appearance that the computer did not work. Given this incredible evidence, the court was quick to find deliberate spoliation on the part of the defendants and sanctioned them. It should also be noted that, despite the damage to the computer, the parties were ***still*** able to obtain a good portion of the relevant documentary evidence from the computer's hard drive.

When electronic information is destroyed during the course of litigation, and sanctions are thereafter requested, trial courts will often examine whether the destruction occurred by accident, by negligence, or intentionally. In *In re Cheyenne Software, Inc.,* 1997 WL 714891 (E.D.N.Y. 1997), the defendants failed to preserved documents on their hard drives, despite a court order to do so. In arguing against sanctions, counsel for the defendants claimed that the company could not "freeze" its business by maintaining all hard drives inviolate during the litigation, but instead had to erase and reformat the drives as people left and as business needs dictated.

The trial court found that the defendants truly believed that they could not comply with the court order, and so did not give the adverse inference charge. Instead, the trial court fined the defendants $5,000.00, and assessed against them $10,000.00 in attorney's fees. The trial court noted that the information should have been downloaded from the hard drives, or a request for relief from the preservation order should have been made; mere disobedience was not acceptable.

Cheyenne Software should be contrasted to several analogous Texas cases (although none of the Texas cases actually involve high tech 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 televison 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 televison station adequately defended against an assertion of negligent or intentional destruction. *Id*.

In *Scolaro*, 1 S.W.3d at 755, the non-party State Bar presented evidence which would rebut any spoliation presumption against it by showing that the destruction of evidence was not with a fraudulent intent. The evidence showed that it was the normal business practice of the State Bar to destroy original correspondence after one year, and only retain electronic records of such correspondence. *Id*. For such reason, the Amarillo Court of Appeals noted that the documents involved were not singled out for destruction, and that, moreover, at the time of the destruction, there was no contemplation of litigation relevant to those records by the State Bar or the parties. *Id*.; *see also, Ordonez v. M.W. McCurdy & Co., Inc*., 984 S.W.2d 264, 273 (Tex.App.–Houston [1st Dist.] 1998, no pet.) (the court held that evidence of the destruction of a driver's log books after six months was part of a normal business practice, and therefore the presumption from spoliation was inapplicable.

On the other side of the spoliation coin, proving spoliation may prove no laughing matter. In *Gates Rubber Co. v. Bando Chemical Indus. Ltd.,*167 F.R.D. 90 (D. Col. 1996), the parties took up almost four years of the court's time with sanctions motions concerning the alleged spoliation of evidence. The case involved theft of trade secrets, and in particular, misappropriation of certain computer programs reportedly used in the manufacturing of industrial belts. During a deposition, a representative of the defendant admitted that he had "cleaned up" the word processing files on his computer by deleting certain materials which he had previously stored there. He

qualified that remark by saying that he did not erase any materials which were relevant to the litigation. Both parties' experts conceded that deleted files remain on a hard drive and only disappear in pieces, in a random fashion, as other data is written over the files, so the district judge gave plaintiff the opportunity to copy the hard drive of the computer at issue in order to obtain as much information as was available with regard to the deleted files.

In capturing this data, however, plaintiff made three critical mistakes. First, the plaintiff's expert unnecessarily copied the hard drive recovery program onto the actual hard drive being recovered, thereby overwriting 7 to 8% of the hard drive before commencing any efforts to copy its contents. Second, the plaintiff's expert did not obtain the creation dates of certain of the files which overwrote the deleted files. Such information would have assisted in determining the deletion dates of some files. If a deleted file had been overwritten by a file which was created prior to the institution of the litigation, for example, the defendant would have been relieved of suspicion as to spoliation of that file. Finally, plaintiff did a "file-by-file" backup of the hard drive, which copied only existing, non-deleted files, as opposed to an "image backup" (or mirror image) of the hard drive, which would have collected every piece of information on the hard drive, whether the information was allocated as a file or not. In light of the mistakes, the court concluded that the plaintiff had failed to preserve evidence in the most appropriate manner, thereby limiting its ability to recover sanctions for any alleged spoliation of evidence. *Id*. at 112.

Lawyers should have a good understanding of basic spoliation concepts. As we continue to rely on computers more and more each day, the use of electronic evidence will become more and more inevitable. The potential for spoliation to occur with computer evidence is greater than with traditional paper documents, given the nature of electronic evidence and the ease with which such evidence can be manipulated. Therefore, lawyers must be prepared to handle spoliation issues if and when they arise.

Lawyers must also handle spoliation–or pre-spoliation–issues with competence, since attorney negligence can also result in sanctions. In *GTFM, Inc. v. Wal-Mart Stores, Inc.,* 2000 WL 335558 (S.D.N.Y. 2000), the defendant's counsel incorrectly represented to the plaintiff and to the trial court that the defendant was unable to retrieve computerized information reflecting the sale and purchase of plaintiff's products, except for one specific date. About a year later, a vice president of the defendant admitted during a deposition that a full year's worth of information could have been retrieved, but at the time of the deposition, it had become unretrievable. The trial court held that the defendant's counsel should have known enough to interview the vice president before the information was lost, rather than simply relying on representations that no records existed. Thus, the trial court ordered the defendant to pay the expenses incurred by the plaintiff and its experts, together with the defendant's own computer personnel, in an on-site examination of the defendant's computer facilities, in order to determine what information, if any, could be retrieved.

It should be noted that several Texas Courts of Appeals have adopted the position presented by Justice Baker in his concurrence to *Trevino v. Ortega*, holding that a party has a duty to exercise reasonable care to preserve relevant information if it either actually or reasonably should anticipate litigation. *See, Wal-Mart Stores, Inc. v. Johnson*, 39 S.W.3d 729, 730 (Tex.App.–Beaumont 2001, no. pet. history), *citing*, *Offshore Pipelines, Inc. v. Schooley*, 984 S.W.2d 654, 667 (Tex.App.–Houston [1st Dist.] 1998, no pet.); *Whiteside v. Watson*, 12 S.W.3d 614, 622 (Tex.App.–Eastland 2000, vacated for settlement); *Clements v. Conard*, 21 S.W.3d 514, 523 (Tex.App.–Amarillo 2000, pet. denied); *In re Dynamic Health, Inc.*, 32 S.W.3d 876, 885 (Tex.App.–Texarkana 2000, orig. proceeding).

With regard to pre-spoliation issues, it has been suggested that no fewer than two authenticated, electronically verified back ups be made of whatever electronic evidence is produced by the other side, one from which to work, and one to seal. Jacks and Wright, at p. 14. Such task will be relatively easy to accomplish–with the aid of an expert–and may well safeguard against later complaints of tampering with the evidence. *Id*.

D. An Alternative Approach?

Despite the ease with which electronic data can be recovered as a technological matter, at least one federal judge believes that electronic information should not be recoverable as a ***legal*** matter. In his article, "In Defense of the DELETE Key," Judge James M. Rosenbaum, a United States District Judge for the District of Minnesota, put forth the notion that there ought to be a six month "statute of limitations" on the recoverability of "deleted" computer files. Acknowledging that nothing is ever "deleted" from a computer because of technology's current ability to preserve and recover this information, and noting that in a world of imperfect human beings, people often have bad ideas, which they might pass on in an email to another, Judge Rosenbaum reminds us that mere evidence that a person has done "A," but once expressed "B," does not prove that the person is lying or deceitful.

Nevertheless, lawyers continue to engage in fishing expeditions for deleted emails in deleted files which supposedly prove the "truth" of some particular proposition. Despite the fact that a recovered email or computer file might just have been a bad idea, properly rejected, and subsequently deleted, many go so far as to suggest that this deleted material is the electronic equivalent of finding that damning "second set of books," completely ignoring the fact that it is not the conception of bad documents which establish their

relevance, but rather the actual use of the information. The fact that one conceives of something—even something improper—does not necessarily mean that it was acted upon.

For Judge Rosenbaum, however, the unlimited recoverability of deleted computer information presents a far greater problem: the notion that free speech will be chilled because of a developing fear that mere expression will be judged tantamount to the act. While it is true that the First Amendment only legally protects the speaker from state rather than private regulation, Judge Rosenbaum believes that one of the fundamental tenets of free speech is the right for people to express their thoughts, good or bad, in a "marketplace" of ideas, where the good thoughts will be accepted and the bad thoughts discarded by those who hear them, not by an elite group of attorneys and judges. People who recognize that whatever you say in a computer "can and will be used against you" will ultimately end up avoiding saying anything "dangerous" via a computer, thus chilling the notion of free speech.

To rectify these perceived injustices, Judge Rosenbaum suggests that courts recognize the existence of "cybertrash." He suggests that if an idea was merely a lousy one or was an isolated cyber utterance, and the actor/author did not manifest some untoward behavior, the email setting forth that idea would be deemed "deleted" as a matter of law, and hence undiscoverable. If, however, there was an objective continuation of the challenged conduct, or a continuing pattern of wrongful acts, the "cyberstatute of limitations" would be tolled just like any other. Rosenbaum believes that his suggestion is feasible given that computers internally record the date on which a "document" is created. Thus, once the limitation period has passed, documents would, according to Judge Rosenbaum, be "legally consigned to the cyber wastebasket." The idea is one which might take hold in the future, given people's rising concerns over their privacy rights on the Internet.

IX. PRIVILEGES AND HIGH TECH EVIDENCE

Several privileges limit discovery in Texas. Among such privileges, the work product and attorney-client privileges are frequently applicable to electronic evidence, particularly since the unique aspect of electronic transmission creates a greater risk of interception or misdirection of the communication. *See*, Boston and Tobias, at p. DD-13.

A. Work Product

Pursuant to TEX.R.CVI.P. 192.5(a), work product comprises:

> material prepared or mental impressions developed in anticipation of litigation or for trial by or for a party or a party's representatives, including the party's attorneys, consultants, sureties, indemnitors, insurers, employees, or agents; or a communication made in anticipation of litigation or for trial between a party and the party's representatives or among a party's representatives, including the party's attorneys, consultants, sureties, indemnitors, insurers, employees, or agents.

Under TEX.R.CIV.P. 192.5(b), "core work product," that is, the work product of an attorney or an attorney's representative that contains the attorney's or the attorney's representative's mental impressions, opinions, conclusions, or legal theories, is not discoverable, while any other work product is discoverable, but only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the material by other means. For discovery purposes, an assertion that material or information is work product is an assertion of privilege. TEX.R.CIV.P. 192.5(d).

In general, the work product privilege shelters the "mental processes, conclusions, and legal theories of the attorney, providing a privileged area within which the lawyer can analyze and prepare his or her case." *Owens-Corning Fiberglas Corp. v. Caldwell*, 818 S.W.2d 749, 750 (Tex. 1991). It has also been stated that Rule 192.5 protects mechanical compilations of fact, to the extent such compilations reveal the mental impression and/or legal conclusions of the case. *See*, Bishop and Horowitz, at p. 10.

As Rule 192.5 makes clear, the work product privilege applies not only to documents generated by the attorney, but to memos, reports, notes, and summaries of interviews prepared by others for an attorney's use. *Keene Corp. v. Caldwell*, 840 S.W.2d 715, 719 (Tex.App.–Houston [14th Dist.] 1992, orig. proceeding). The privilege extends to the entire document, not merely the specific portions relating to legal advice, opinions, or mental analysis. *Pittsburgh Corning Corp. v. Caldwell*, 861 S.W.2d 423, 425 (Tex.App.–Houston [14th Dist.] 1993, orig. proceeding). If a document is privileged or exempt from discovery, the fact that information within the document may be discoverable through other means does not defeat the privilege. *Keene* Corp. 840 S.W.2d at 720.

Although decided before the 1999 amendments to the Texas Rules of Civil Procedure which created the concept of "core" work product, *In re Bloomfield Mfg. Co.*, 977 S.W.2d 389 (Tex.App.–San Antonio 1998, orig. proceeding) affords an example of the applicability of the work product privilege to electronic evidence. In *Bloomfield*, the plaintiff in a personal injury suit served a request for production which included the following request:

> [a]ny and all product liability logs, claim logs or records of any kind regardless of the terminology used within the company relating to claims or personal injuries allegedly sustained as a result of the handle of a Hi-Lift Jack flying up and striking a person.

Id. at 390. The plaintiff later specifically asked for a computer database the plaintiff alleged fell within the scope of the request for production. *Id*. at 391. The defendant objected to producing the computer database on the grounds, among others, that the database was work product because information in the database was created by an attorney to monitor and categorize litigation against the plaintiff, and that the database memorialized the attorney's thought processes, outlined strategies, and categorized claims and the interrelationship between the claims. *Id*. at 391-392. The trial court found that some of the attorney impressions contained in the "description of incident" portion of the database were privileged, but that the balance was not. *Id*. at 391.

In an original mandamus proceeding, the San Antonio Court of Appeals found that the database contained a description of how each incident that led to a claim against the defendant happened, and that such descriptions were extracted by an attorney or at an attorney's direction from various legal documents, depositions, and interviews. *Id*. at 392. Thus, because the descriptions reflected an attorney's analysis of claims filed against the defendants, of the contents of certain documents, and of the interrelationship of the claims made against the defendants, they were protected by the attorney work product privilege, and the entire database was precluded from discovery. *Id*.

Again, *Bloomfield* was decided before the inception of the "core" work product concept. Under the current discovery rules, the holding in *Bloomfield* would not end the analysis because it was clear that parts of the database were not "core" work product; thus, it is possible that the non-core portions of the database might have been subject to discovery if the requisite showing of substantial need and undue hardship had been made. *See*, Boston and Tobias, at p. DD-14.

B. Attorney-Client Privilege

1. In General

"A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client." TEX.R. CIV. EV. 503(b). The purpose of the attorney-client privilege is to secure the free flow of information between attorney and client on matters involved in litigation, without the fear that details of their communication will be disclosed. *See, e.g., Boring & Tunneling Co. of Am., Inc. v. Salazar*, 782 S.W.2d 284, 289 (Tex.App.–Houston [1st Dist.] 1989, orig. proceeding). For an instrument to be protected by the attorney-client privilege, it needs to constitute a communication between an attorney and client and owe its existence to an effort to transmit information from one to the other. *Suddarth v. Poor*, 546 S.W.2d 138, 141 (Tex.Civ.App.–Tyler 1977, writ ref'd n.r.e.).

In *Bloomfield*, the defendants also argued that the requested database was protected from discovery under the attorney-client privilege. 977 S.W.2d at 390. However, according the San Antonio appellate court, the defendants offered no proof that the database was a communication, and therefore they failed to offer proof that the database was protected by the attorney-client privilege. *Id*. at 392. The only evidence the defendants offered was the database itself and the uncontroverted affidavit testimony of one its representatives, who stated "there is a list of claims document that was created by counsel in an effort to manage claims which is also work product and attorney-client privilege," but such affidavit was not proof that the database was a communication between relators and counsel. *Id*.

2. Privileged Documents Within Electronic Data

As in any large document production, *i.e.*, in any big dollar or messy divorce, the producing party bears the burden of identifying and segregating any attorney-client privileged documents from electronic production. With regard to electronic discovery, the risk that an electronic document or communication will be inadvertently produced is greatest when a "mirror image" copy has been produced.

One precaution against inadvertent disclosure might be a court order restricting forensic examination of the mirror image disk to certain parts, and to prohibit the examination of any privileged documents. Additionally, an agreement might be obtained that, after the mirror image copy is made, an opportunity will be provided for privileged files to be deleted and then purged from the disk.

As with traditional paper document production, documents stored on back up tapes or computer hard drives may also contain privileged attorney-client information or work product. TEX.R.CIV.P. 193.3(d) ("Privilege Not Waived by Production") protects such privileged information by providing:

> 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.

X. E-MAIL REDUX

A. Overview of E-Mail

E-mail can be defined as "[a] document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as world processing and other electronic documents, which may be transmitted with the messages." *See,* 36 C.F.R. §1234.2 (2001). Thus, modern day business and personal email messages cover everything from intimately personal matters to the drudgery of routine commerce.

One commentator has identified several characteristics that make e-mail an excellent source of evidence: (1) most people use e-mail informally and candidly; (2) many people believe that an e-mail is impermanent; (3) e-mail is more difficult to get rid than most users believe due to the ease of copying and forwarding, the fact that most e-mail systems require a two-step process to permanently delete e-mail from a system, and undeleted e-mail my be captured on system backups. *See*, Joan E. Feldman, *The Basics of Computer Forensics*, p. 19, PRAC. LITIGATOR (March 2001). In the end, its seems as if e-mail, as "all powerful messages" are used to prove or support almost anything. Despite some of the problematic qualities of e-mail, as have already been discussed, e-mail is also a undeniably wonderful tool for impeachment.

1. Chat Rooms

One form of e-mail is termed "real time" or a "chat room." In a "chat room," people participate by communicating with each other in what has been termed "instantaneous cyber-conversation." *See,* Janice L. Green, *Unusual Evidence Issues,* p. Q-4, 22ND MARRIAGE DISSOLUTION INSTITUTE, (1999) [hereinafter referred to as "Green"], *citing,* David K. McGraw, *Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail,* 21 RUTGERS COMPUTER AND TECH. L.J. 491, 494 (1995) [hereinafter referred to as "McGraw"]. Chat rooms are normally open to an unlimited number of correspondents, and recently have been much in the news as the effective tool of many undesirable social elements, such as pedophiles.

For example, *Taylor v. State*, 54 S.W.3d 21 (Tex.App.–Amarillo 2001, no pet.), a recent Texas criminal search and seizure case, illustrates the workings–and pitfalls–of the "chat room." In *Taylor*, according to the police, the defendant allegedly entered a chat room maintained by "America on Line" (AOL), in which a topic of ongoing discussion in the chat room was "sexual activity involving children." *Id*. at 22. Furthermore, alleged the police, the participants were using a computer program entitled "Listmaker.exe," which purportedly allowed a list to be compiled of persons in the specific chat room. *Id*. In this manner, AOL subscribers could allegedly place and remove their names from the list at will, and thereafter the list could be transmitted through email to every AOL subscriber on the list. *Id*. Thus, with such program, AOL subscribers "with the same or similar interests" could then contact each other. *Id*. In *Taylor*, the defendant allegedly placed his name on the list and soon began receiving email containing photographic file attachments from AOL subscribers depicting both adult and child pornography. *Id*.

However, what the defendant apparently didn't realize was that AOL maintained records of persons using their service, including the name, address, telephone numbers, and other identifying information of subscribers. *Id*. The police then obtained a search warrant permitting him to discover from AOL "subscriber information" applicable to those who allegedly sent the pornography. *Id*. Ultimately, the police obtained an "Online Account Profile" for the screen name "MeNu441," that led the police to the defendant. *Id*. at 23.

2. Bulletin Boards

Another type of e-mail is termed a "computer bulletin board." A bulletin board is an Internet site designed for, and geared to, a particular interest or topic shared by people who visit the site. A person interested in the bulletin board topic may leave a message for others, who have "hit" that particular bulletin board, to read.

Bulletin boards are also big with those who have interesting sexual proclivities. In *Chen v. State*, 42 S.W.3d 926, 927 (Tex.Crim.App. 2001), for instance, the defendant placed an advertisement on an America Online computer bulletin board stating: "A nude dancer needed for discreet pleasure. I am generous and rich. You must be very attractive and young." Of course, to the eventual discomfort of the defendant, a Dallas police officer working on a specialized crime task involving child exploitation, discovered the advertisement and answered it.

3. Direct E-Mail

Finally, there is "direct e-mail," sent from one individual to another, which is not intended to

be read by anyone other than the recipient. Although the sender of direct e-mail may have some expectation of privacy and anonymity, the e-mail server has the capability of identifying the sender of the message. Several different types of "direct e-mail" exist.

a. E-mail "Post Office"

To send e-mail, the sender must direct his or her message through an internet or systems "server," such as AOL, Prodigy, CompuServe, or Hotmail. The sender, an internet or service subscriber, is assigned an e-mail "address" and can also gain access to chat rooms or bulletin boards by means of the service provider.

b. Inter-office E-mail

It is common for a business or office to have an inter-office server that connects employees with each other.

c. Encrypted Messages

Encryption is a "lock and key" technology. In an effort to maintain confidentiality, the participants use two "keys," one to encrypt the message, and the other to decrypt the message upon receipt.

B. Expectations of Privacy and Security

The degree to which e-mail carries with it an expectation of privacy is very much in doubt. It is frequently said that e-mail is simply not private or secure. *See, e.g.,* Michael Swaine, *Protecting Your Privacy Online,"* MACUSER, 135 (November 1996) ("[e]-mail is about as private as a conversation on a bus"). One of the serious considerations concerning the privacy of e-mail stems from the fact that most users treat e-mail very informally; e-mail often contains sentiments and opinions that would never have been expressed in so direct a fashion in a traditional document like a personal or business letter. *See,* Michael Overly, *Finding the Needle in the Haystack: Discovering Electronic Evidence,* LAN Magazine (February 17, 1997); *see also,* McGraw, at 496 (a perceived anonymity causes e-mail messages to be more blunt and direct than traditional communication methods, and the language used may be more harsh and crude than that normally used in face-to-face conversation or letters).

In contrast, other commentators state that is encrypted e-mail does carry an expectation of privacy.

> ...if a person who transmits an encrypted message reasonably believes that only the intended recipient will have a key to decode the message, it would seem that encrypted messages over the Internet would be made with a reasonable expectation of confidentiality. If an unauthorized person decoded the message, it would seem no different than, for example, had a Federal Express employee opened a sealed envelope containing a confidential document. Encrypted e-mail messages are confidential.

David Hricik, *Confidentiality & Privilege in High-Tech Communications,"* 60 TEX. BAR J. 114 (1997).

Issues of confidentiality abound in the use of e-mail. Does a person who uses a laptop or personal computer for personal or business use have a reasonable expectation that the communication will be protected from the curious, such as a spouse? Does it matter whether that person transmits an e-mail message from home, as opposed to his or her place of employment? At least one Texas judge has stated that "if the communication is posted to a chat room or bulletin board, then any argument of privacy or confidentiality has been waived." Marilea W. Lewis, *Invasion of Privacy–Illegally Obtained Evidence,* p. G-9, 22ND MARRIAGE DISSOLUTION INSTITUTE (1999).

On the other hand, if the communication is a personal message to a family member or a friend, it is reasonable to believe that only the intended recipient will have access to the communication? Does it matter if the sender uses his or her real name in the message, instead of an alias? What is the effect of one spouse accidently sending to his or her estranged spouse an e-mail intended for the sending spouse's paramour?

In 1999, an Austin American-Statesman front-page article addressed and illustrated the use of e-mail messages in the context of a divorce. The article discussed a pending divorce case (including issues of child custody) in which a Washington-area lawyer, in words that "flowed without inhibition," sent e-mail messages to his friends and even strangers that described his homosexual trysts, "gushed about his partners and agonized over cheating on his wife." *When Marriages Are Deleted, E-mail Can Become Evidence*, AUSTIN AMERICAN-STATESMAN, May 10, 1999, at A-1. As might be expected, his wife discovered and produced such messages in the divorce. *Id.* The wife contended that she found the messages on a computer disk stuffed in a drawer; the husband argued that the wife forged the messages. *Id.* The article noted that when spouses share a computer, messages can be written under the other spouse's name, and existing files (containing saved messages) can be altered.

The article continued by quoting one lawyer who said: "You're going to say things to your e-mail that you wouldn't say to your priest in confession." *Id.* at A-8. Another lawyer was quoted as saying that even the most sophisticated husbands and wives let their guard down when they sit at their keyboards: "[t]here are people who wouldn't think about

leaving an envelope open on their desk, yet they leave a computer that has their love letters or pornography or chat room talk." *Id.*

According to the article, the now commonplace hunt through e-mail records "is sort of replacing the old looking through the trash can for discarded notes." *Id.* The article concluded with the statement by a Fordham University communications professor: "I think we need to look at e-mail as something that has to be protected....[h]istorically, the law has always been limping behind the technology." *Id.*

Other commentators agree with the thrust of the American-Statesman article. For example, one Texas commentator has written that "[o]rdinarily canon and case law provide the answers to problems in the legal arena, but case law is playing catch up in a field that is charging swiftly through uncharted waters." Patricia J. Lasher, *Internet and E-mail Matters Relevant in the Divorce Practice,* p. U-9, 21ST MARRIAGE DISSOLUTION INSTITUTE (1998) [hereinafter referred to as "Lasher"].

C. Unlawful Interception or Disclosure of E-mail

"As a practical matter, the interception of e-mail seems more likely to occur in the home or office setting than through the intervention of cybersleuths. Like its telephone counterpart, Internet e-mail utilizes phone lines, wire cables and fiber optic cables, passing through a myriad of private and public routes and computers before it comes to rest in the resident 'in box.' While the possibility of interception exists, it is generally believed that the technical difficulty of locating and isolating the individual bits of messages that travel in may parts over many places makes interception an unlikely prospect." Lasher, at U-11. Nevertheless, both Texas and federal law prohibit the interception of e-mail.

1. Texas Law

Under TEX.PENAL CODE ANN. §16.02(b) (Vernon Supp. 2000) ("Unlawful Interception, Use, or Disclosure of Wire, Oral, or Electronic Communications"), a person commits a criminal offense if he or she:

> (1) intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication;
>
> (2) intentionally discloses or endeavors to disclose to another person the contents of a wire, oral, or electronic communication if he knows or has reason to know the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (3) intentionally uses or endeavors to use the contents of a wire, oral, or electronic communication if he knows or is reckless about whether the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (4) knowingly or intentionally effects a covert entry for the purpose of intercepting wire, oral, or electronic communications without court order or authorization; or
>
> (5) 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 when the device (A) is affixed to, or otherwise transmits a signal through a wire, cable, or other connection used in wire communications; or (B) transmits communications by radio or interferes with the transmission of communications by radio.

An offense under §16.02 is a second degree felony. TEX.PENAL CODE ANN. §16.02(f) (Vernon Supp. 2000).

TEX.PENAL CODE ANN. §16.04 (Vernon Supp. 2000) ("Unlawful Access to Stored Communications") provides:

> (a) In this section, "electronic communication," "electronic storage," "user," and "wire communication" have the meanings assigned to those terms in Article 18.21, Code of Criminal Procedure.
>
> (b) A person commits an offense if the person obtains, alters, or prevents authorized access to a wire or electronic communication while the communication is in electronic storage by:
> (1) intentionally obtaining access without authorization to a facility through which a wire or electronic communications service is provided; or
>
> (2) intentionally exceeding an authorization for access to a facility through which a wire or electronic communications service is provided.
>
> (c) Except as provided by Subsection (d), an offense under Subsection (b) is a Class A misdemeanor.

> (d) If committed to obtain a benefit or to harm another, an offense is a state jail felony.
>
> (e) It is an affirmative defense to prosecution under Subsection (b) that the conduct was authorized by:
>
> (1) the provider of the wire or electronic communications service;
>
> (2) the user of the wire or electronic communications service;
>
> (3) the addressee or intended recipient of the wire or electronic communication; or
>
> (4) Article 18.21, Code of Criminal Procedure.

There are no Texas authorities specifically addressing the issue of the interception of e-mail. Many commentators, however, analogize possible scenarios involving such interception to "traditional" wiretap cases, of which there are several reported in Texas. *See, e.g.,* Lasher, at U-10- U-11 ("...it seems unlikely that an uninvited e-mail interception of a similar communication would granted that [sic] a domestic exemption status....[a]lthough these cases [*i.e., Parker v. Parker,* 897 S.W.2d 918 (Tex. App.-Fort Worth 1995, writ denied), and *Collins v. Collins,* 904 S.W.2d 792 (Tex. App.-Houston [1st Dist.] 1995, writ denied)] deal with telephone calls, their application to e-mail in which one has an expectation of privacy seems appropriate"); Green, at Q-6 ("[w]hile *Parker* and *Collins* dealt with taping phone calls, they would be applicable to interception of e-mail communication").

It should also be noted that TEX.CIV.PRAC.& REMEDIES CODE ANN. §123.001 *et. seq.* (Vernon 1997) makes interception of a "communication," 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, an actionable civil tort (with mandatory attorney's fees, minimum damages, as well as potential punitive damages. *See*, Lasher, at U-11. Since e-mail is transmitted through phone lines, wire cables, and\or fiber optic cables, Chapter 123 of the Texas Civil Practice and Remedies Code arguably applies to the interception of e-mail. *See,* Lewis, at G-9.

2. Federal Law

According to Judge Patricia Lasher, the federal government has been in the forefront of computer related legislation, an understandable result given the inherent intra-jurisdictional nature of computer communications and the Internet. Lasher, at U-12. In 1986, federal lawmakers passed the Stored Wire and Electronic Communications and Transactional Records Act, 18 U.S.C. §§2701-2711. In 1998, such act was amended by congress and became Title II of the Electronic Communications Privacy Act (ECPA). Title II of the ECPA specifically addresses e-mail and stored communications.

The Electronic Communications Privacy Act, 18 U.S.C. §§2701-2711, provides as follows:

> (I) Section 2701 makes it a crime to intentionally access, without authorization, an electronic communications server facility (*e.g.,* America Online or CompuServe).
>
> (ii) Section 2702 makes it a violation for a server to divulge the contents of stored communications to an unauthorized person or entity.
>
> (iii) Section 2703 sets forth the requirements, such as a warrant or court order, for the government to access stored communications under the control of the server.
>
> (iv) Section 2704 provides that the governmental entities may include in a subpoena or court order a requirement that the server make back-up copies of the contents of stored communications.
>
> (v) Section 2706 creates a civil cause of action for service providers, subscribers or customers who have been aggrieved by any violation of the Act. Relief includes equitable or declaratory relief, damages including actual damages and ill-gotten profits of the violator, but in no event less than $1,000.00 in reasonable attorney's fees and litigation costs. Civil actions under section 2706 must be commenced within two years from the date the violation was or reasonably should have been discovered.

See, Lasher, at U-12-U-13.

3. Federal Case Law

In *Jessup-Morgan v. America Online, Inc.,* 20 F.Supp.2d 1105, 1106 (E.D. Mich. 1998), Terry Jessup and Phillip Morgan began an illicit relationship some time prior to January, 1996, while Phillip Morgan was still married to another woman, Barbara Smith, although a divorce action was pending between the two.

On January 11, 1996, Jessup (then an America Online ("AOL") member) used her AOL account to post publicly on the Internet a message, under the "screen name" (*i.e.*, alias) of "Barbeeedol," meant to harass and injure Barbara

Smith. In pertinent part, the message read as follows:

> Call me ..... I'm single, lonely, horny and would love to have either phone sex or a [sic] in person sexual relationship....My name is Barbara and I'm a single white female looking for just about any kind of sex I can have with someone other than myself ...If you can help, call me at (810) 977-9476.

The listed telephone number was the phone number of Barbara Smith's parents' home, with whom Barbara Smith and her two young children were residing pending resolution of the divorce. Jessup posted the message in an Internet usenet newsgroup entitled "alt.amazon-women.admirers," a public electronic bulletin board containing messages accessible to, and read by, potentially 40 million persons worldwide.

As intended by Jessup, posting this message resulted in persons Barbara Smith did not know calling her parents' home to request sexual liaisons with "Barbara." This gravely disturbed and distressed Barbara Smith and her parents. From the nature of the calls, and from the information callers supplied about how they obtained her parents' home phone number, Barbara Smith concluded that she was the intended target of the person(s) who posted the message on the Internet.

Ultimately, Barbara Smith determined that the sender was another AOL member, and requested that AOL identify the person who posted the message. AOL reviewed Smith's complaint and the "Barbeeedol" message, and determined that the posting originated from Jessup's AOL account, which constituted an egregious breach of the AOL Member Agreement signed by Jessup. *Id.* at 1106-1107. AOL, therefore, terminated its contract with Jessup and closed her AOL account. AOL's records list the grounds for this termination as "excessive USENET abuse." *Id.* at 1107. The same day, AOL sent Smith two messages. The first message explained that, for confidentiality reasons, AOL could not disclose information about actions it took against other AOL members. The second message explained that as a matter of AOL policy, information identifying the AOL member who posted the offensive message could only be released in response to a subpoena. Barbara Smith's divorce attorney then served AOL with a civil subpoena for information which would identify the AOL member who authored the injurious message. In compliance with the subpoena, AOL produced a document which identified Jessup as the person who had posted the offensive message.

Subsequently, Jessup brought suit against AOL claiming, among other things, that AOL's compliance with the subpoena and release of stored electronic information violated section 2707 of the Electronic Communication Privacy Act ("ECPA"), 18 U.S.C. §2707. In her suit, Jessup requested damages in excess of $47 million. Jessup did not deny that she perpetrated the offense against Barbara Smith (by posting the fraudulent Internet message), but nevertheless she complained that AOL's disclosure that she committed the offense affected her child custody hearings (she was involved in legal proceedings involving a child), "her future husband's [Phillip Morgan's] divorce hearing, and other personal matters," as well as her "reputation in the community...and her reputation among her friends." AOL responded by filing a motion for judgment on the pleadings on the grounds that Jessup's pleadings failed to state a claim upon which relief could be granted. *Id.* at 1108.

The federal district court held that the prohibitions of the ECPA, 18 U.S.C. §§2701 *et seq*., were inapplicable. *Id.* The federal court noted that the ECPA prohibits disclosure of the contents of an electronic communication to any person or entity (18 U.S.C. §2702) or to the government (18 U.S.C. §2703) without first meeting certain restrictions. *Id.* Further, according to the district court, 18 U.S.C. §2711 states that the definitions in 18 U.S.C. §2510 apply to the ECPA's provisions, and that 18 U.S.C. §2510(8) provides that "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication," [not information concerning the identity of the author of the communication]. *Id.* The district court held that the "content" of a communication under the ECPA was not at issue in the case; rather disclosure of information identifying an AOL electronic communication account customer was at issue, and such information was specifically acknowledged as separate from the "content" of electronic communications by the ECPA. *Id, citing,* 18 U.S.C. § 2703(c)(1)(C). In other words, the ECPA actually authorized AOL's disclosure. *Id.* Thus, because the prohibitions of the ECPA did not apply to the AOL disclosure, Jessup's claim that AOL violated the ECPA failed, and the district court dismissed the claim. *Id.*

In 1999, the Houston Chronicle reported a situation similar to that in *Jessup-Morgan.* The Chronicle reported that Landry's Seafood Restaurant Chain "wants to know who's saying nasty things about it on the Internet," and has requested a court order that Yahoo–an Internet service provider–reveal the identity of people posting "unlawful messages" on the Yahoo site. *Landry's asks judge for Yahoo identities / Chain alleges defamatory Net postings*, HOUSTON CHRONICLE, April 23, 1999. The article states that Landry's is seeking the identities to determine if a lawsuit should be filed. *Id.* Landry's alleges that some of the postings suggest knowledge of "inside" information detrimental to the chain, its investors, and the stock market as a whole. *Id.*

According to the Chronicle article, messages posted recently on the Yahoo site revealed

an animosity toward users known as "Sockscats" and "Imitation." *Id.* One message posted by "Sockscats" read as follows: "I better go see about getting some glasses. Am I reading this right. Landry's operating income was only 400K? And the stock is up today anyway?" *Id.* A message posted the following day stated: "My boss (T-Man) would like me to cut you to pieces [referring to Landry's chairman, Tilman Fertilla]." *Id.*

In *United States v. Simons,* 29 F.Supp.2d 324 (E.D. Va. 1998), the Defendant, who was charged with receiving and possessing materials containing child pornography, moved to suppress evidence obtained from his office computer. The Defendant was employed as an electronic engineer within the Foreign Bureau of Information Services ("FBIS"), a component of the CIA. *Id.* at 325 (further factual references to the same page of the opinion are omitted.) The Defendant had access to a government computer system owned and operated by the CIA, and he had access to the Internet
.

The manager of the computer network for FBIS was responsible for monitoring Internet connections through a device called a "firewall," which logs all traffic going outside of the networks, and indicates which computers have accessed the outside. In a routine check of the firewall system, the manager discovered that the firewall log was very large. Consequently, he conducted a search for the keyword "sex," and determined that there were a significant number of "hits" on Internet web sites, most of which traced back to the same work station. *Id.* at 326. Since such use of the system was prohibited, the manager contacted his Network Branch Chief, and ultimately the Chief and others determined that the web site accessed was pornographic ("www.xratedpictures.com"). FBIS then investigated whether any pictures had been downloaded to the work station involved, and found that over 1,000 files had been downloaded that contained pictures. After the FBIS and the others involved copied the Defendant's hard drive, the FBI was called in because certain files appeared to depict child pornography. The FBI obtained a warrant and made copies of the Defendant's hard drive and floppy disks. The Defendant moved to suppress the evidence.

The federal district court ultimately held that the Defendant lacked a reasonable expectation of privacy with regard to any Internet use, because the FBIS had official policies regarding such use, which provided, in part, that official business use, incidental use, lawful use, and contractor communications were permitted, that audits would be implemented to support identification, termination, and prosecution of unauthorized activity, and that audits would be capable of recording web sites visited. *Id.* at 327-28.

The Defendant also argued that the searches conducted without a warrant produced evidence that could not be used at trial, since the government's interception of his personal e-mail was equivalent to electronic interception of personal phone calls, which violates 18 U.S.C. §§2515-2516. *Id.* at 329. However, the federal district court noted that there was nothing in the record suggesting that the Defendant's e-mail was obtained while it was being transferred. *Id.* Instead, stated the district court, the Defendant's e-mail was copied while it was in storage, and therefore sections 2515-2516 did not apply. *Id.* Accordingly, the district court denied the Defendant's motion to suppress. *Id.*

In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 458-59 (5th Cir. 1994), the Fifth Circuit addressed a case that arose when the federal government, under a warrant, seized a computer system used by an employee of Steve Jackson Games, Inc. (SJG). The employee was suspected of hacking into a Bell Telephone computer system. *Id.* The seized computer system included an electronic bulletin board service provided to subscribers of SJG. *Id.* at 458. During the course of the government's investigation of the hacking incident, the stored, and as yet undelivered, bulletin board e-mail was read by U.S. Secret Service agents, who also deleted some of the information. *Id.* at 459.

Subsequently, SJG and several individuals whose e-mail had been seized and read filed suit against, among others, the Secret Service and the United States, claiming, *inter alia*, violations of the Federal Wiretap Act, as amended by Title I of the ECPA, 18 U.S.C. §§2510-2521 (proscribing, *inter alia*, the intentional interception of electronic communications), and Title II of the ECPA, the Stored Wire and Electronic Communications and Transactional Records Act, 18 U.S.C. §§2701-2711 (proscribing, *inter alia*, intentional access, without authorization, to stored electronic communications). *Id.*

The trial court held, and the Fifth Circuit concurred, that the government had not violated Title I of the ECPA, the Federal Wiretap Act. *Id.* at 460-461. On appeal, the sole issue was very narrow–whether the seizure of a computer on which was stored private e-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients–constituted an "intercept" proscribed by 18 U.S.C. §2511(1)(a). Agreeing with the trial court, the Fifth Circuit held that the government had not illegally "intercepted" the e-mail, as the term "intercept" is defined and used in Title I of the ECPA (the Federal Wiretap Act), because the government's acquisition of the contents of the electronic communications was not "contemporaneous with the transmission of those communications" (the seized e-mail had already been stored). *Id.* at 460-461.

The trial court also held that the government had violated the statutory requirements of Title II of the ECPA (the Stored Wire and Electronic Communications and Transactional Records Act) because no notice of the proposed seizure was given, as mandated by Title II of the ECPA, and no back-up copies of the deleted e-mail were made. *Id.* at 459. The Fifth Circuit upheld the trial court's award of $1,000.00 to each plaintiff.

Monotype Corp. PLC v. International Typeface Corp., 43 F.3d 443 (9th Cir. 1994), involved a dispute between a typeface designer and one of the designer's licensors in which the designer claims that the licensor copied some of the designer's typefaces. At trial, the designer attempted to introduce as evidence e-mail correspondence from an employee of the licensor to an employee of another corporation. *Id.* at 450. The plaintiff argued that the e-mail constituted business records and should be admitted; the trial court excluded the e-mail on the grounds that its prejudicial nature outweighed its relevancy. *Id.*

On appeal, the Ninth Circuit distinguished e-mail from computer printouts, which are admissible as evidence, on the grounds that "E-mail is far less of systematic business activity than a monthly inventory printout," with e-mail being an ongoing electronic message and retrieval system, whereas electronic inventory recording system is a regular, systematic function of a bookkeeper prepared in the course of business. *Id.* Thus, the Ninth Circuit held that the trial court had properly excluded the e-mail correspondence. *Id.*

D. Discoverability of E-Mail

In *In re Monsanto Co.,* 998 S.W.2d 917, 920 (Tex.App.–Waco 1999, orig. proceeding), farmers and farming entities brought action against the patent holder and manufacturer of genetically engineered cotton seed to recover damages caused by a lack of insect resistance. The trial court ordered discovery of most documents as to which the patent holder and manufacturer claimed a privilege, after which the patent holder and manufacturer petitioned for writ of mandamus. *Id.* at 921.

The Waco Court of Appeals held that the attorney-client privilege protected, among other things, copies of electronic mail since many of the e-mails between attorneys and representatives of the clients asked for "suggestions," "review," and "input," and, although some documents listed many persons as recipients, all recipients were the corporation's employees or attorneys. *Id.* at 93-931.

1. Attorney-Client Confidentiality

TEX. DISCIPLINARY R.PROF.CONDUCT 1.05 (1998) generally provides that a lawyer shall not reveal confidential client information, whether such information is privileged or unprivileged, to anyone other than the client without the express authorization or consent of the client. Neither Texas case law nor any ethical opinion has addressed the issue of the use of e-mail by a lawyer to communicate with or about a client. *See*, Lasher, at p. U-10.

However, the American Bar Association Committee on Ethics and Professional Responsibility recently issued a formal opinion stating that a lawyer does not violate Model Rule of Professional Conduct 1.6(a) [in Texas, Rule 1.05] by sending a client information in unencrypted e-mail, provided the lawyer takes reasonable precautions to guard against disclosure of the information. ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413 (March 1999) (protecting the confidentiality of unencrypted e-mail); *see also, Red-Letter Day for E-Mail*, 85 A.B.A.J. 79 (June 1999).

The opinion concludes that e-mail poses "no greater threat of interception or disclosure" than traditional communication methods, such as phone calls or letters, which are accorded a reasonable expectation of privacy. 85 A.B.A.J. at 79. However, the Committee also recommends that an attorney check with his or her client about highly sensitive information before sending such information to the client. In addition, the attorney should take reasonable steps to safeguard the security and privacy of e-mail communications, although the Committee does not detail or explain what such measures might be. *Id.* According to the ABA Journal, the Committee's opinion reflects the trend of the majority of state bar associations across the country. *Id.*

Additionally, it should be noted that the Texas Attorney General has issued a number of opinion letters in which, for the purposes of the Texas Open Records Act, emails have been found to have been covered by the attorney-client privilege and therefore exempt from disclosure. *See*, *e.g.,* Tex.Att.Gen.Op. OR2001-5694 (December 6, 2001).

Even so, as already stated, in Texas, the issue of whether information remains confidential when it is communicated between an attorney and client by the use of e-mail has not be definitively decided. *See, e.g.,* Green at Q-5. Some commentators take the position that information communicated via e-mail is confidential and does not lose its privileged character: "[a]s a general principle, otherwise privileged information does not lose its privileged character merely by being intercepted or reviewed while being transmitted as a electronic communication over the Internet." Hricik at 106.

Other commentators urge caution, pointing out that either the client or the attorney may inadvertently waive the attorney-client privilege, for example, by forwarding copies of the e-mail message to friends or family for purposes of discussion, or accidentally forwarding the message too all members of the client's book-of-the-month club. In addition, a client may save an e-mail, which might allow another person to review the communication at a later date, for instance, just before trial. Lasher, at U-10. Consequently, at least one commentator believes that, "[u]nless and until the client and attorney have a clear understanding about the protection of information that passes over the Internet, that tool is best left for general, non-confidential communication of court dates, parenting classes and appointments." *Id.*

One commentator has argued that there are two things a lawyer, who intends to communicate with clients by email, should inform his or her client. Margaret Graham Tebo, *A Treacherous Path,* ABA Journal, p. 98 (February 2000). First, potential problems, such as interception, should be discussed, and a disclaimer should be attached to every email communication stating the nature of the attorney-client privilege applicable to such communication. *Id*.. Second, clients should usually be advised against archiving old e-mail for more than a few weeks. *Id.* Tebo states that in all but the most regulated businesses, records can be destroyed on a regular schedule, as long as they are not the subject of a current discovery request. *Id.*

2. Privacy Issues

Professor William L. Prosser cataloged 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. *Cain v. Hearst Corp*., 878 S.W.2d 577, 578 (Tex. 1994), *citing,* 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. *Cain,* 878 S.W.2d at 578; *see also,* RESTATEMENT (SECOND) OF TORTS §652A (1977).

Texas did not recognize any of the four types of invasion of privacy until the Texas Supreme Court's decision in *Billings v. Atkinson*, 489 S.W.2d 858, 860 (Tex.1973), which involved the first category of invasion of privacy as developed by Prosser and recognized by the Restatement: an intrusion into the plaintiff's seclusion. *Cain,* 878 S.W.2d at 578. "Intrusion" is the form of invasion of privacy most application to the interception of e-mail. Lasher, at U-17; Green, at Q-8. In fact, language used by the Texas Supreme Court in *Billings* seems particularly applicable to the modern technology used in computer communications:

> One of the principal arguments advanced in support of the doctrine of privacy by its original exponents is that the increased complexity and intensity of modern civilization and the development of man's spiritual sensibilities have rendered man more sensitive to publicity and have increased his need of privacy, while the great technological improvements in the means of communication have more and more subjected the intimacies of his private life to exploitation by those who pander to commercialism and to prurient and idle curiosity. A legally enforceable right of privacy is deemed to be a proper protection against this type of encroachment upon the personality of the individual.

Billings, 489 S.W.2d at 860, *quoting*, 62 AM. JUR. 2D *Privacy* § 4.

However, it should be noted that RESTATEMENT (SECOND) OF TORTS §652B (1977) defines "intrusion" as the intentional invasion into a person's physical seclusion or private affairs in a manner ***highly offensive to a reasonable person***. Whether a fact-finder would conclude, for example, that the reading of a spouse's e-mail is "highly offensive" to a reasonable person is a question unanswered in Texas law. Green, at Q-8. The issue may turn on the efforts made by the sender and the recipient to guarantee privacy, such as encryption.

In *Smyth v. The Pillsbury Co.,* 914 F.Supp 97, 98 (E.D. Pa. 1996), the Pillsbury Company maintained an electronic mail communication system ("e-mail") in order to promote internal corporate communications between its employees (further references to facts from the same page of the opinion are omitted). Pillsbury repeatedly assured its employees, including the Plaintiff, that all e-mail communications would remain confidential and privileged, and further assured its employees, including the Plaintiff, that e-mail communications could not be intercepted and used by Pillsbury against its employees as grounds for termination or reprimand.

In October 1994, the Plaintiff received certain e-mail communications from his supervisor over Pillsbury's e-mail system on his computer at home. Relying on Pillsbury's assurances regarding the confidentiality of the e-mail system, Plaintiff responded and exchanged e-mails with his supervisor. Subsequently, contrary to the assurances of confidentiality it had made, Pillsbury intercepted the Plaintiff's private e-mail messages made in October 1994. On January 17, 1995, Pillsbury notified Plaintiff that it was terminating his employment effective February 1, 1995, for transmitting what it deemed to be inappropriate and unprofessional comments over Pillsbury's e-mail system. *Id.* at 98-99.

The Plaintiff sued Pillsbury, but since he was an at-will employee, he had to prove that his dismissal violated a clear mandate of public policy. *Id.* at 99. Consequently, the Plaintiff claimed that his termination violated "public policy which precludes an employer from terminating an employee in violation of the employee's right to privacy as embodied in Pennsylvania common law." *Id.* at 100.

However, in applying the law regarding the tort of "intrusion upon seclusion" to the facts of the case before it, the federal district court found that the Plaintiff failed to state a claim upon which relief could be granted. *Id.* at 101. The district court

stated that, unlike urinalysis and personal property searches, there was no reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system, notwithstanding any assurances that such communications would not be intercepted by management. *Id.* According to the federal court, once the Plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e- mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. *Id.*

Moreover, continued the district court, even if it did find that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, it could not then find that a reasonable person would consider Pillsbury's interception of such communications to be a substantial and highly offensive invasion of his privacy. *Id.* The federal court noted that, by intercepting such communications, Pillsbury was not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. *Id.* Further, according to the district court, Pillsbury's interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system outweighed any privacy interest the employee may have in those comments. *Id.* Therefore, the Plaintiff's lawsuit was dismissed.

XI. OTHER ETHICAL CONSIDERATIONS

TEX. DISCIPLINARY R. PROF'L CONDUCT 3.04(a), reprinted in TEX. GOV'T CODE ANN., tit. 2, subtit. G (Vernon 1998), provides that a lawyer shall not:

> unlawfully obstruct another party's access to evidence; in anticipation of a dispute unlawfully alter, destroy or conceal a document or other material that a competent lawyer would believe has potential or actual evidentiary value; or counsel or assist another person to do any such act.

According to Comment 2 of Disciplinary Rule 3.04, paragraph (a) specifically applies to "computerized information." Two commentators have concluded that, under Rule 3.04(a), a lawyer is expected to preserve, as well as have his or her client preserve, "pertinent information regarding matters in dispute where litigation is foreseeable." Boston and Tobias, at p. DD-4.

It is likely that more and more divorce lawyers will be receiving notice or preservation letters in the future. But, even in the absence of an explicit notice letter, with the onset of family litigation, it will probably be prudent for the Texas practitioner to advise his or her client of preservation issues.

XII. CONCLUSION

One attorney, who also doubles as an "e-discovery" consultant, has gone on the record to say:

> E-discovery is the most significant challenge we have to the rules of evidence....[u]nless you're aggressive and know how to handle it, you will get beaten up.

Bill Speros, *quoted in*, Krause, at p. 53.

Obviously, few, if any attorneys relish the possibility of coming out on the losing end of a discovery fight. The simple reality is, however, that in today's world, computers rule. In today's litigation environment, electronic evidence may well soon "rule." It stands to reason that lawyers should become very familiar with the issues involved, or risk the consequences. It is the hope of the Authors that the present discussion will assist Texas lawyers in such a familiarization process.

Appendix I

To: "Defense Counsel"

Re: "Drug & Medical Device Litigation"

Gentlemen:

Plaintiffs consider electronic data to be a valuable and irreplaceable source of discovery and/or evidence in this matter. The laws and rules prohibiting destruction of evidence apply to electronic data with the same force as they apply to other kinds of evidence.
Pending further discovery concerning the layout and configuration of defendants' computer systems and electronic data sets, and pending any further agreement of the parties as to preservation of electronic evidence, the following safeguards against destruction of evidence should be maintained by your client until the final resolution of this issue.

Please provide a copy of this letter to the person or persons whose job responsibilities cover the matters addressed herein.

1. ***Electronic Data To Be Preserved***

The following types of your electronic data and/or the electronic data of your subsidiaries, divisions, agent or employees should be preserved, in accordance with the steps set for the in ¶¶ 2-8 below:

a. All electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail systems usage) sent or received by anyone relating to [drug or medical device];

b. All other electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail system usage containing information about [drug or medical device];

c. All data bases (including all records and field structural information in such databases), containing any reference to and/or information about [drug or medical device];

d. All logs of activity on any computer system which may have been used to process or store electronic data containing information about [drug or medical device];

e. All word processing files and file fragments containing information about [drug or medical device];

f. With regard to electronic data created by application programs which process financial, accounting and billing information, all electronic data files and file fragments containing information about [drug or medical device];

g. All files and file fragments containing information from electronic calendars and scheduling programs regarding [drug or medical device];

h. All electronic data files and file fragments created or used by electronic spreadsheet programs where such data files contained information about [drug or medical device];

i. All other electronic data containing information about [drug or medical device].

2. ***On-Line Data Storage On Mainframes Mini-computers PCs and Laptops:***

With regard to on-line storage and/or direct access storage devices attached to defendants' mainframe computers and/or minicomputers PCs and Laptops: do not modify or delete any electronic data files existing at the time of this letter's delivery, which meet criteria set forth above, unless a true and correct copy of each such electronic data file has been made and steps have been taken to assure that such a copy will be preserved and accessible for purposes of this litigation. The copy should be an exact mirror.

3. Off-Line Data Storage, Backups, and Archives, Floppy Diskettes, Zip Drives, and Zip Files, Tapes, Compact Diskettes, Laptops, Palm Held Devices, Disconnected Hard Drives, and other Removable Electronic Media:

With regard to all electronic media used for off-line storage, including magnetic tapes and cartridges and other media, which contained any electronic information meeting the criteria listed above, stop any activity which may result in the loss of such electronic data, including rotation, destruction, overwriting, and/or erasure of such media in whole or in part This request is intended to cover all removable electronic media used for data storage in connection with defendants' computer systems, including magnetic tapes and cartridges, magneto-optical disks, compacts disks, floppy diskettes and all other media, whether used with personal computers, minicomputers, laptops, notebooks, palm held devices, or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data meeting the criteria listed above.

4. ***Replacement of Data Storage Devices***

Do not dispose of any electronic data storage devices and/or media which may be replaced due to failure and/or for other reasons that may contain electronic data meeting the criteria listed above.

5. ***Fixed Drives on Stand-Alone Personal Computers and Network Workstations***:

With regard to electronic data meeting the criteria listed above, which existed on fixed drivers attached to stand-alone microcomputers and/or network workstations at the time of this letters delivery: do not alter or erase electronic data and do not perform other procedures (such as data compression and disk re-fragmentation or optimization routines) which may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listing (including hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve such copies during the pendency of this litigation.

6. ***Programs and Utilities***

Preserve copies of all application programs and utilities which may be used to process electronic data covered by this letter.

7. ***Log of System Modifications***

Maintain an activity log to documents modifications made to any electronic data processing system that may affect any system's capability to process any electronic data meeting the criteria listed above, regardless of whether such modifications were made by employees, contractors, vendors and/or any other third parties.

8. ***Personal Computers Used by Employees, Contractors and Others under the Control of Defendants and/or their Secretaries and Assistants:***

The following steps should immediately be taken in regard to all personal computers used by such persons:

a. As to fixed drives attached to any such personal computers:

i. A true and correct copy should be made of all electronic data on such fixed drives relating to [drug or medical device], including all active files and file fragments;

ii. Full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and

iii Such copies and listings should be preserved until this matter reaches its final resolution.

b. All floppy diskettes, magnetic tapes and cartridges, compact disks, zip drives, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to [drug or medical device] should be collected and put into storage, available for inspection, for the duration of this lawsuit.

9. ***Evidence Created Subsequent to This Letter:***

With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence should not be destroyed and defendants should take whatever steps are appropriate to avoid destruction of such evidence.

I would also like to arrange a time in the near future when we can have access to the defendants' computer system and set up a deposition of appropriate MIS representatives. If you require a formal request to inspect, I will provide you one.

Further, this request is deemed to apply not only to domestic United /states facilities and persons, but also to international entities of the defendants.

Please do not hesitate to contact me if you have any questions.