

WHEN TECHNOLOGY AND FAMILY LAW COLLIDE

REGINALD A. HIRSCH

1980 Post Oak Boulevard

Suite 2210

Houston, Texas 77056

(713) 961-7800

reghir@swbell.net

State Bar of Texas

34TH ANNUAL ADVANCED FAMILY LAW COURSE

August 11 - 14, 2008

San Antonio

CHAPTER 5

REGINALD A. HIRSCH

Law Office of Reginald A. Hirsch

1980 Post Oak Boulevard, Suite 2210, Houston, Texas 77056
(713) 961-7800 FAX: (713) 961-3453 E-Mail:reghir@swbell.net
WebSite: www.yob.com

BIOGRAPHICAL INFORMATION

DATE OF BIRTH: February 24, 1947, Houston, Texas

MARRIED: Patricia Wicoff, Attorney at Law

Child: Sarah Lauren Hirsch, Age 22, University of Colorado, Boulder

EDUCATION: Lamar High School, Houston, Texas, 1965

Washington University, St. Louis, Missouri, 1965-1967

B.S., University of Houston, 1970

J.D., University of Houston, 1973

Chief Justice Student Court, University of Houston Student Court, 1972-1973

Student Regent to the University of Houston Board of Regents, 1972-1973

PROFESSIONAL EMPLOYMENT:

Assistant Attorney General for State Bar of Texas, Environmental Division, 1973-1974

Balasco, Clark, Hirsch and Stern, 1974 - 1979

Lipstet & Hirsch, 1979 - 2007

Law Offices of Reginald A. Hirsch, 2008-

PROFESSIONAL LICENSES:

State Bar of Texas, 1973

U.S. District Court, Southern District of Texas, 1974

U.S. Court of Appeals, Fifth Circuit, 1974

PROFESSIONAL ACTIVITIES:

Board Certified in Family Law, 1974-2009

President, Harris County Young Family Lawyers Association, 1977

President, Family Law Section, Houston Bar Association, 1980-1981

Member, State Bar of Texas, Family Law Counsel, 1985-1989

Chairman, Houston Volunteer Lawyers Association, 1983-1984

Director, The Association of Trial Lawyers of America, 1985

President Family Law Forum, 1983-1985

Director, Association of Gulf Coast Family Law Specialists, 1989-1990

President, Gulf Coast Legal Foundation, 1986

Texas Association of Family Law Specialists

International Society of Family Law

National Association of Counsel for Children

American Academy of Matrimonial Lawyers

Adjunct Professor, South Texas College of Law, Environmental Law, 1975-1977

Guest Lecturer at Baylor College of Medicine

Guest Lecturer at University of Houston Law School

Guest Lecturer at South Texas College of Law

Guest Lecturer at Texas Southern University College of Law

Member, Chairman's Council, Harris County Democratic Party, 1990

Master, American Inns of Court

Chairperson, Family Law Task Force 2000

Treasurer, American Inns of Court, Burta Raborn Chapter, 2005-2008

President-Elect, American Inns of Court, Burta Raborn Chapter, 2008-2009

Technology Committee, New Family Law Center, 2005-2008

RECENT LAW RELATED PUBLICATIONS, ACADEMIC APPOINTMENTS AND HONORS:

Author/Speaker, 1999 Advanced Family Law Drafting Course, State Bar of Texas, "Hardware and Software to Assist the Family Law Practice"

Speaker, South Texas College of Law, Advanced Marital Property Class, "Net Enhancement", February 16, 2000

Author/Speaker, South Texas College of Law, Indigestion and the Internet, Including Ethical Issues about Lawyer Advertising

On the Web and E-Mail Confidentiality Issues", February 17, 2000

Author, Speaker, 2002 28th Annual Advanced Family Law Course, State Bar of Texas, "Parental Alienation"

Author, Speaker, 2003 29th Annual Advanced Family Law Course, State Bar of Texas, and "Forms of Family Law Practice"

Author, Speaker Fall 2004 Houston Paralegal Association, "Internet Research for Paralegals"

Member, State Bar of Texas, Summer 2005, Texas Family Law Form Book Parent Planning Committee

Author/Speaker -University of Houston, .Fall 2005, Parent Planning Texas Style

Author/Speaker, Texas Chapter Association of Family and Conciliation Courts, September 30- October 1, 2005

Houston, Texas- Panel Interdisciplinary Approaches to Identifying and Addressing Alienation Issues

Panelist, PBS Houston, "The Connection" Response to "Breaking the Silence: Children Stories" October 28th and 30th, 2005

Speaker, Future of Family Law, Burta Raborn Inns of Court, Houston, Tx January, 19,2006.

Speaker, Author, "Tracing Keeping It Simple", Burta Raborn Inns of Court, Houston, Tx February 16, 2006.

Speaker, Author, Investigating Your Client, Family Law Conference for General Practitioner and the Legal Assistant, March 9, 2006, Houston, Tx

Recipient, David Gibson Award, Gulf Coast Family Law Specialist, May 11, 2006 Houston, Tx

Speaker, Co-Author, Parenting Plans, South Texas College of Law, Houston, Tx May 19, 2006

Speaker, Co-Author, Amicus Attorney- Who Represents the Child - Not me." State Bar of Texas 2006 Advanced Family Law

San Antonio, Tx August 16, 2006

Speaker, Co-Author, Origins of Parenting Plans, University of Texas, October 13, 2006 Dallas, Texas and November 3, 2006 Houston, Texas

Speaker, Author, Texas Parenting Plans- How We Got Here, University of Houston, November 10 and 17th, Dallas and Houston,Tx

Recipient, Top Family Lawyer, 2006.,Houston Magazine, August 2006

Recipient, Mentor, Award, Houston Bar Association, Family Law Section, January 3, 2006

Speaker, Author, Parenting Plans, How Did We Get Here, Spring 2006, Dallas and Houston, Tx

Speaker, Author, "Who Represents the Child, Not Me, I am the Amicus Attorney, August 2006, San Antonio, Tx

Speaker, Author, Electronic Discovery, Hal-Pc, April 18, 2007, Houston, Tx

Presenter, Burta Raborn Inns of Court, April 19, 2007, Houston., Tx

Recipient, Texas Super Lawyer, 2007, Family Law, Texas Monthly Magazine

Author, Speaker, University of Texas, Austin, Texas, November 8,2007,The Definitive Short Course on Parent Child Relationships, "The World of Court Appointees: Amicus Attorneys. Attorney Ad Litem, Guardian Ad Litem and Social Studies"

Author, Speaker, State of Texas Judicial College, "Electronic Evidence Issues", Richardson , Tx, April 17, 2008

Author, Speaker, Co Panelist, 8th Annual ,Family Law on the Front Line, "Electronic Evidence –Fighting the War of the

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	ELECTRONIC FINGER PRINTS	1
II.	RIGHT OF PRIVACY	1
IV.	DELETED FILES AREN'T REALLY DELETED, INCLUDING FILES ON YOUR MOBILE PHONE. .	2
V.	METADATA	3
VI.	READ NOTIFY	6
VII.	GPS	7
A.	GPS-enabled Cell Phones.	8
B.	Wireless Networks	8
1.	T-Mobile/Cingular/AT&T	8
2.	Sprint/Nextel,	8
C.	Location-Based Services (LBS)	8
D.	Accutracking	8
E.	Sprint's Mobile Locator	8
F.	Mapquest Find Me	8
G.	Wherify Wireless	8
H.	Additional Points to Consider	8
1.	Permissions and Privacy	8
2.	Tracking Application "Persistence"	8
3.	Passive Tracking	9
4.	Assisted GPS (AGPS)	9
5.	Tower reports	9
6.	GeoFencing	9
7.	Speed Alerts	9
8.	Tracking Map Quality	9
9.	Usage Costs	9
10.	Mobile to Mobile Tracking	9
11.	Digital Cameras	10
VIII.	INSTANT MESSAGING	10
IX.	BROWSER HISTORIES	10
X.	COFEE	11
XI.	VOICE OF EXPERIENCE: DANGER IS ONLY A SPLIT SECOND AWAY	12
XII.	CONCLUSION	12
	APPENDIX I	13

WHEN TECHNOLOGY AND FAMILY LAW COLLIDE

I. INTRODUCTION

The effect of technology on family law is pervasive. This paper and presentation will cover a number of topics that family lawyers must be aware of in the proper representation of their clients as well as insuring their own well being. Included in this article are actual news stories which indicate how significant these issues can be. (Believe me this is scary stuff.) And remember, if it's electronic data and you can see it ---- someone else can see it as well.

II. ELECTRONIC FINGER PRINTS

With the evolution and development of electronic devices, almost everyone has the ability to ascertain the identity, location and analysis of both the sender and the receiver of electronic information. The term I use to describe this is "electronic fingerprinting." Although the tools over the last 20 years have become extremely robust in detection, recovery and analysis of electronic data, the counter measures have also increased in sophistication. It truly has become a game of "cat and mouse". As an example of the "cat and mouse game" consider Microsoft's release of various patches to it's software, which is now known in the industry as "Patch Tuesday," followed by "Exploit Wednesday". It has been suggested that the reason for choosing Tuesday is so you can do work on Monday and use the rest of the week to resolve any problems resulting from the patch. For the lawyer and the client it is critically important to be aware of electronic fingerprints, as well as how to find them and make client's aware of how vulnerable their communications can be.

III. RIGHT OF PRIVACY

Any discussion regarding the obtaining, location, extraction and analysis of electronic fingerprints must begin with a review of the "right of privacy." The "right of privacy" remains the cornerstone of our individual liberties but is a right that can be easily waived by unsuspecting lawyers and/or clients.

It may come as a surprise that the word "privacy" is actually never used in the text of the U.S. Constitution, or any of it's amendments. The Texas Supreme Court in *Texas State Employees Union, et al., Petitioners, v. Texas Department of Mental Health and Mental Retardation, et. al., Respondents (Tex.) 746 S.W. 2d 203*; held the following:

While the Texas Constitution contains no express guarantee of a right of privacy, it contains several provisions similar to those in the United States Constitution that have been

recognized as implicitly creating protected "zones of privacy." *Cf. Roe v. Wade*, 410 U.S. 113, 152, 93 S.Ct. 705, 726, 35 L.Ed.2d 147 (1972). Section 19 of the Texas Bill of Rights protects against arbitrary deprivation of life and liberty. TEX.CONST., art. 1, § 19. Section 8 provides the freedom to "speak, write or publish", and section 10 protects the right of an accused not be compelled to give evidence against himself. TEX. CONST., art. 1, §8, 10. Sections 9 and 25 guarantee the sanctity of the individual's home and person against unreasonable intrusion. TEX.CONST., art. 1, §9, 25. Finally, the Texas Constitution protects the rights of conscience in matters of religion. TEX.CONST., art. 1, §6. Each of these provisions gives rise to a concomitant zone of privacy. *Cf. Griswold v Connecticut*, 381 U.S. 479, 484, 85 S.Ct. 1678, 1681, 14 L.Ed.2d 510 (1965). We do not doubt, therefore, that a right of individual privacy is implicit amount those "general, great, and essential principles of liberty and free government" established by the Texas Bill of Rights. TEX.CONST., art. I, Introduction to the Bill of Rights. We hold that the Texas Constitution protects personal privacy from unreasonable intrusion. This right to privacy should yield only when the government can demonstrate that an intrusion is reasonably warranted for the achievement of a compelling govern-mental objective that can be achieved by no less intrusive, more reasonable means."

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

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or in his private affairs or concerns, is

subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. Under Section 625B(N), to recover as a result of an intrusion; on the tort of invasion of privacy, the complainant must show: (1) Conduct in the nature of an intrusion; (2) private nature of the thing or place intruded upon; and (3) the intrusion was substantial and the conduct highly offensive or objectionable to the reasonable person.

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

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

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

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

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

Liability for invasion of privacy does not depend on any publicity given to the person whose interest is invaded or to his affairs. *Clayton v. Richards*, 47 S.W. 3d.

In the case of *Parker v. Parker*, the jury awarded a million dollars (21% of defendant chiropractor husband's net worth) to the plaintiff when the defendant bugged the telephones of wife's attorneys and engaged in other outrageous conduct. *Parker v. Parker*, 897 S.W. 2d 918, 930 (Tex.App.–Fort Worth 1995, writ denied) overruled on other grounds by *Formosa Plastics Crop. USA v. Presidio Engineers & Contractors, Inc.*, 960 S.W. 2d 41.

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

Here's a typical call I get at least once a month.

Question: My client has accessed the community computer and observed the spouse engaged in _____ activity. [You fill in the blank.] Is that legal and what kind of trouble am I in by just looking at the material?

Let's focus on the right of privacy aspect for now.

Ignoring for a second the Federal and State laws that might or might not be applicable, the real litmus test for claims of invasion of privacy depends on the answer to:

“Was the material or data preserved in a manner to give rise to a reasonable expectation of privacy?”

If the answer is “yes” you may have a claim for invasion of privacy. So we need to ascertain things like:

1. Location of the computer;
2. Was it password protected and if so was the password kept secret and not disclosed;
3. Was the computer used by family members or 3rd parties;
4. Was the computer a personal or business computer;
5. Was the computer used by the other spouse regular or infrequently; and
6. What steps did the user take to secure his or data, etc.

There are many weight factors to consider, but the test again was there a reasonable expectation of privacy. This is the key to understanding the right of privacy.

IV. DELETED FILES AREN'T REALLY DELETED, INCLUDING FILES ON YOUR MOBILE PHONE.

First, an explanation of computer data and what makes it's recovery challenging and somewhat scary to the average person.

A deleted file really isn't deleted.

In the days of DOS (Disk Operating System) it was recognized that deleted data might need to be recovered so the first letter of the file was given a machine code character that made it unreadable except with a recovery utility or program. That is why the recycle bin of the computer under Windows will allow you to “restore” a

file. The machine code is then converted to a readable format, and the deleted file can then be recovered. But in the event that the space occupied by the file is needed and overwritten, then the file is lost, except with specialized tools.

Data like calling information, text messages are readily available to be extracted from cell phones. In fact the iPhone has been shown under version 1.0(+) to not have the ability to delete personal information. So if you are using an iPhone upgrade to version 2.0 which now allows you to delete personal information. This personal information can be stored in electronic memory or on a SIM card, SSD device or harddrive. Advise your clients and be very careful with your own cell phone or device. You never know who might get their hands on it.

V. METADATA

What is metadata and why should a family lawyer be concerned about it? In an article entitled *Beyond Data about Data: The Litigator's Guide to Metadata*, Craig Ball states:

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

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

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

In *Williams v. Sprint/United Mgmt Co.*, the Federal Court ruled that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their

METADATA INTACT,

unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order." 230 F.R.D. 640, 651 (D. Kan. 2005).

Having both embedded application metadata and external system metadata is advantageous because, when

metadata is stored both within and outside of the file, *discrepancies* between the metadata can expose data tampering.

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

Every active file stored on a computer has at least one corresponding external block of system metadata—every one, no exceptions.

Files may also have multiple associated metadata blocks as well as embedded metadata fields. You will never face the question of *whether* a file has metadata—all active files do—instead, the issues are *what kinds* of metadata exist, *where* the metadata resides and whether it's potentially *relevant* such that it must be preserved and produced. Modern operating systems record a ream of data detailing the creation, use and status of files as well as the use and configuration of associated applications. Windows users see a few of these characteristics tracked in the "details" view of a folder. By default, only a file's name, size, type and date modified are displayed; however, right click on the column titles in Windows XP and another thirty-four-odd metadata fields can be displayed, including creation date, author and comments. But even this broad swath of metadata is just *part* of the information about the file recorded by the operating system.

Within the Master File Allocation Table (MFT) are index records used by Windows to track all files, still more attributes are encoded in hexadecimal notation. In fact, an ironic aspect of Windows is that the record used

to track information about a file may be larger than the file itself! Stored within the hives of the System Registry—the “Big Brother” database that tracks attributes covering almost any aspect of the system—are thousands upon thousands of attribute values called “registry keys.” Other records and logs track network activity and journal virtually every action. Within this maelstrom of metadata, some information is readily accessible and comprehensible while other data is so byzantine and cryptic as to cause even highly skilled computer forensic examiners to scratch their heads. To preserve metadata and assess its relevance, you have to know it exists. So, for each category of data subject to discovery, assemble a list of associated metadata. You’ll likely need to work with an expert the first time or two, but once you have a current and complete list, it will serve you in future matters.

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

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

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

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

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

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

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

Because of the design of the FastSave feature, text that you delete from a document may remain in the document, even after you save the document. If you are concerned about deleted text remaining in your documents, follow these steps:

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

Windows Vista Business, Ultimate and Enterprise editions are loved by computer forensic experts because of a feature called “shadow copy.” Let’s see how Microsoft describes this feature:

“Have you ever accidentally saved over a file you were working on? Accidental file deletion or modification is a common cause of data loss. Windows Vista includes a useful innovation to help you protect your data: Shadow Copy. Available in the Ultimate, Business, and Enterprise editions of Window Vista, this feature automatically creates point-in-time copies of files as you work, so you can quickly and easily retrieve versions of a document you may have accidentally deleted. Shadow copy is automatically turned on in Windows Vista and creates copies on a scheduled basis of files that have changed. Since only incremental changes are saved, minimal disk space is used for shadow copies.

Easily access this feature by right-clicking a file or folder and selecting “Restore previous versions.” It enables you to go back in time and access your files and folders as they were on previous dates. You can preview each file in a read-only version to determine which file to restore. Then, to fully restore it, you can just drag the file to a folder, or select it and click “Restore” to restore it to its original location.

It works on single files as well as whole folders. When restoring a file, all previous versions that are different from the live copy on the disk are shown. When accessing a previous version of a folder, users can browse the folder hierarchy as it was in a previous point in time.”

See: <http://www.microsoft.com/windows/products/windowsvista/features/details/shadowcopy.mspx>.

As you can readily see, the ability to examine shadow copies is a tool as they say to “drool over” from a legal and forensic standpoint.

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

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

- Turn off Fast Save. This feature speeds up saving a document by saving only changes made to a document. However, text that you delete from a document may still remain. Microsoft recommends turning off this feature to eliminate any chance of deleted text remaining in the document. Click Tools, then Options. Click the Save tab. Clear the "Allow fast saves" check box and click OK.
- You can remove personal information from a document when you save it. In Word 2002 and 2003, click Tools, then Options. Click the Security tab. Under Privacy options, select "Remove personal information from file properties on save" and click OK. In Word 2000, click Tools, the Options. Select the User Information tab. Clear the information in Name, Initials and Mailing Address and click OK.
- Turn off the Track Changes tool. In Word 2002 and 2003, click Tools, then Track Changes. In Word 2000 and earlier versions, click Tools, Track Changes, Highlight Changes. Click to clear the check mark in the "Track Changes while editing" box.

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

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

- Finally, a free Microsoft tool removes hidden data from Word, Excel and PowerPoint. The Remove Hidden Data add-in tool (snipurl.com/3osw) will delete hidden text and comments from individual files or a batch of files at once.

Wow is that a potential area for discovery.

That is a partial answer as to why the recovery of metadata can be so important. But the issue has gotten to be a huge problem with metadata and the information it can provide.

In Florida, the President-Elect of the Florida State Bar reported that partner of his firm was apparently tricked into providing a file that contained metadata to an opposing lawyer. Gary Blakenship, The Florida Bar News, What’s in Your Document? Jan. 1, 2006.

In what must have been a mind blowing discussion, the following was reported to have occurred:

President-elect Hank Coxe gave the board a graphic example of what that means. A senior partner in his firm was working on a brief which was requested by another firm for a case it was working on. When the partner finished the brief, he offered to fax it, but the other firm asked that it be e-mailed.

That firm then mined it for metadata. What they got, Coxe said, was a history showing every change that had been made to the document, as well as who had worked on it. At one point, the client had been e-mailed for input and the client had replied by e-mail. Both had been attached to the document as it was being prepared and later deleted; and both communications were recovered by the other law firm.

As a result, the Florida Bar has an ethics opinion concluding that:

“a lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer.”

Any such metadata is to be considered by the receiving lawyer as confidential information which the sending lawyer did not intend to transmit. Professional Ethics of the Florida Bar, Opinion 06-02 (September 16, 2006). The Florida opinion also notes an obligation on sending attorneys to protect confidential information, including information that might be revealed in hidden data. It also notes that this “may necessitate a lawyer’s continuing training and education in the use of technology in transmitting and receiving electronic documents in order to protect client information.” The Florida opinion specifically does not address what a lawyer’s obligations about hidden data are with regard to discovery of electronic documents in litigation; however, New York had come to a similar conclusion in 2001, holding that

“(a) lawyer may not make use of computer software applications to surreptitiously “get behind” visible documents or to trace e-mail.” New York State Bar Association Op. 749 (December 11, 2001). A second New York ethics opinion holds that lawyers have an obligation under disciplinary rules to avoid transmitting hidden data that is confidential. New York State Bar Association Op. 782 (December 8, 2004), online at <http://www.nysba.org/Content/NavigationMenu/AttorneyResources/EthicsOpinions/Opinion782.htm>.

And if you think only lawyers and citizens are ones to be concerned about this issue consider this factoid: Editing information can show the revision history of a document. One of the most useful features of modern word processors is redline functionality which shows what portions of a document were changed between drafts. Comments can be made to documents that will not show up when the document is printed. Unfortunately, unless affirmative steps are taken to eliminate the redlines and comments, these can be passed along to adverse parties along with the electronic file. What you see is not necessarily what you get: the last thing you see on the screen or printed document may not be all of what a user on the other end can see. It has been told that the Lubbock Court of Appeals recently released opinions on their website that showed red line editing. The opinions were taken down after the problem was reported. See *Selected Legal Malpractice and Ethical Issues in the Use of Current Technology* by Jett Hanna, State Bar of Texas, November 8 – 9, 2006 Dallas.

Recently (March 2008) even the U.S. Department of Justice was embarrassed by the failure to protect metadata. In a pdf document released to the public entitled, “*Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation.*” which disclosed that federal tax dollars were allocated to telecommunications companies after 911 to allow U.S. governmental agencies like the FBI to conduct electronic surveillance. The problem was the document had been supposedly redacted because it contained “sensitive information”. Yet by running your mouse over the redacted fields metadata was revealed and by turning on a view feature in Adobe Acrobat further sensitive information was revealed. The NSA had even published a document on how to prevent this from happening. It is entitled: “*Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to Pdf.*” So a lesson to the wise, if the federal government cannot conceal metadata - the average citizen and lawyer must be extraordinarily careful to protect themselves.

As reported:

“Once again, supposedly sensitive information blacked out from a government report turns out to be visible by computer experts armed with the Ctrl+C keys – and that information turns out to be not very sensitive after all. This time around, University of Pennsylvania professor Matt Blaze discovered that the Justice Department’s Inspector General’s office had failed to adequately obfuscate data in a March report (.pdf) about FBI payments to telecoms to make their legacy phone switches comply with 1995 wiretapping rules. That report detailed how the FBI had finished spending its allotted \$500 million to help telephone companies retrofit their old switches to make them compliant with the Communications Assistance to Law Enforcement Act or Calea– even as federal wiretaps target cell phones more than 90 percent of the time.”

See <http://ww.wired.com>, May 19, 2008 blog.

VI. READ NOTIFY

How many remember the following story about how an HP investigator used the services of ReadNotify.com to trace an e-mail sent to reporter Dawn Kawamoto in an attempt to uncover her source in a media link? Fred Adler, an HP security employee, said during testimony before a U.S. House of Representatives subcommittee, how the company bugged the e-mail it sent to Kawamoto. Moreover, Adler said that it's still company practice to use e-mail bugs in certain cases.

"That was and still is current policy," he said. "It still is sanctioned by my management as an investigative tool, we have used it in the past for investigations, for determining the locations of stolen product and what-not, and we have also assisted law enforcement."

The tracking mechanism provided by ReadNotify would allow investigators to see who opened the file attached to the e-mail, Adler said. The objective was to determine whether the journalist would forward the e-mail to her source, and to then determine the source of the leaks of HP confidential information.

Through ReadNotify, investigators would see when the e-mail attachment was opened and the Internet Protocol, or IP, address of the computer it was opened on, Adler said. An IP address can disclose the geographic location of a recipient, as well as the Internet service provider used to connect to the Internet.

"We suspected it would be Mr. Keyworth that would be the recipient," Adler said, referring to George

Keyworth, the HP board member who has admitted he leaked information to the media.

During a press conference at HP headquarters last week, Michael J. Holston, a lawyer hired by HP, said that bugging e-mail did not yield results in this case.

ReadNotify, which operates as an online service, provides a free trial that lets anyone send 25 bugged e-mails, according to its Web site. Subscriptions are offered starting at \$24 per year. A premium \$36-a-year subscription is required to bug files such as Office and PDF documents. A similar service operates as MailTracking.com.

ReadNotify's service makes bugging e-mail a matter of pointing and clicking. The ReadNotify Web page will generate a document with an image. This image, a green check mark, can simply be dragged and dropped into the document that needs to be traced. The check mark becomes transparent after being dropped.

"ReadNotify uses a combination of up to 36 different simultaneous tracking techniques," Chris Drake, the company's Sydney, Australia based chief technology officer said in an e-mail interview. "One or more of these usually works in all different e-mail clients and operating systems, making us the most powerful and reliable tracking service on the Internet."

In short, ReadNotify uses more technologies than simple Web bugs, Drake said. "All good e-mail programs have blocked these now and most anti-spam programs reject them too, so we no longer rely on this simplistic tracking idea."

In the terms of use posted on its Web site, ReadNotify stipulates that its services should be used for "lawful purposes only." The company goes on to say that its product should not be used to transmit "intentionally deceptive e-mail messages."

And I love this comment:

"Occasionally, we're asked about privacy and legal issues," Drake said. Essentially, ReadNotify believes an e-mail author can do whatever he pleases with the message, including tracking it. "It is important to understand firstly that just because an e-mail comes into your inbox, it does not make it yours. When a person puts the effort into thinking up an e-mail and composing it: that e-mail is theirs."

"Some experts have questioned whether such technology is legal under American law, but Mr. Drake says "e-mail tracking is legal because e-mail is 'owned' by the author." See "How HP bugged E-Mail" by Joris Evers at <http://www.news.com/How-HP-bugged-e-mail/2100->

[1029_3-6121048.html](http://www.news.com/How-HP-bugged-e-mail/2100-1029_3-6121048.html) and New York Times, "In the E-Mail Relay, Not Every Handoff Is Smooth", June 15, 2008

CAVEAT EMPTOR: Email and documents can be tracked not only as to whom it was sent to, when it was received, and when it was opened, and where they are located, but also who else it was forwarded to and when they opened it and for how long.

VII. GPS

Until recently, tracking people with Global Positioning System technology required purchasing expensive hardware and software. Now, complete solutions are available through cellular service providers. Here is background information and a few options for keeping up with the whereabouts of your family, friends and employees.

Locating People in an Emergency. The increased demand for enhanced 911 (e911) emergency calling capabilities, stimulated by the events of September 11, 2001, has pushed forward GPS tracking technology in cell phones. At the end of 2005, all cell phone carriers were required to provide the ability to trace cell phone calls to a location within 100 meters or less.

To comply with FCC requirements, cell phone carriers decided to integrate GPS technology into cell phone handsets, rather than overhaul the tower network. However, the GPS in most cell phones are not like those in your handy GPS receiver that you take hiking. Most cell phones do not allow the user direct access to the GPS data. Accurate location determination requires the assistance of the wireless network, and the GPS data is transmitted only if a 911 emergency call is made. So, in general, you can not track someone using their cell phone, unless the person you want to track has the right kind of cell phone, connected to the right network, with the right service.

A. GPS-enabled Cell Phones.

Motorola and Blackberry were the first GPS-enabled phones to proliferate the United States. Initially, Motorola "iDEN" phones were commonly used for employee tracking on the business-oriented Nextel network. Then GPS enabled Blackberry phones, once used almost exclusively by corporate and government VIPs, began to penetrate the consumer market stimulated by the demand for phones with advanced messaging capability. Next came specialty devices produced under the names of "Disney Mobile" and "Wherify Wireless" targeting use by children and elderly. Now in 2008, a variety of GPS-enabled phones and tracking services are available.

B. Wireless Networks.

In the United States, the wireless networks used for GPS tracking are primarily those operated by cell phone carriers. It is not likely that an individual will negotiate network access with a carrier. It is more likely that an individual will select a solution including a cell phone provisioned to communicate in a certain way on a specific wireless network. Listed below are a some recommended carriers for use with GPS cell phones and services.

1. T-Mobile/Cingular/AT&T

The Global System for Mobile (GSM) communications as adopted by these carriers represents the network with the largest coverage footprint. Roaming agreements between these carriers provide end users with service throughout the country. GSM is also the prominent cellular network abroad.

2. Sprint/Nextel.

not so much because of coverage, but because of their emphasis on data. Nextel has created their own data formats and communication protocols for high bandwidth mobile electronics applications. This company, who gave new meaning to the term "walkie-talkie", provides the most flexibility for the communication of GPS data between cell phones and location-based service providers. Recent co-operation between Sprint and Nextel has increased this network's footprint.

C. Location-Based Services (LBS)

LBS providers have agreements with the wireless network carriers to receive data from a cell phone and make it accessible to you via an Internet web site or call center. Most all LBS providers will be able to tell you the approximate last known location, but beyond that, services offered will vary, depending on the type of cell phone and the capabilities of the service provider.

D. Accutracking

Accutracking is a full-featured low-cost LBS provider using Motorola, Boost Mobile and Blackberry phones operating on the Sprint/Nextel network. See Accutracking.com

E. Sprint's Mobile Locator

Nextel's Mobile Locator is a service used in conjunction with Nextel calling plans using Nextel GPS-enabled phones. Mobile locator allows you to view and monitor your people's location in real-time, either singly or within a group, on a zoomable, online map. The web interface allows you to view location history, based on your most recent queries. See: [Sprint Mobile_Locator](http://Sprint_Mobile_Locator) web site for more information.

F. Mapquest Find Me

Using certain models of Nextel phones, you can view a group of your peoples' locations on one map, or you can view a track of an individual's location history. Powered by uLocate, Mapquest provides a web interface for mobile devices like PDAs as well cell phones. Other features include in-depth location history detail. See www.mapquestfindme.com.

G. Wherify Wireless

Developers of the "Wherifone" designed specifically for children, seniors, and business users. The Wherifone is supported solely by Wherify's Global Location Service Center. See: Wherify.com

H. Additional Points to Consider

Here are some other things to keep in mind.

1. Permissions and Privacy

Simply put, tracking someone without their knowledge can get you in trouble. Typically, the subscriber must give permission and the cell phone must be enabled for tracking. Consult with the service provider for more detail.

2. Tracking Application "Persistence"

Again, the tracking application on a cell phone typically must be enabled by the user. Depending on the equipment, the application may persist - remaining enabled when the phone is turned on after having been turned off. This feature is particularly handy if you do not want to instruct the person using the phone on how to turn tracking on and off.

3. Passive Tracking

Some tracking devices will record location data internally so that it can be downloaded later. Also referred to "data logging," which can provide location data even when the device has traveled outside the wireless network. Passive tracking is not a common feature built-in to cell phones (at the time this article was published), but more sophisticated java-enabled cell phones, PDAs, and other mobile devices may have this feature. Consult with the LBS provider to see if their application can accommodate passive tracking data from the more sophisticated tracking devices.

4. Assisted GPS (AGPS)

Some cell phones can receive ephemerid information on the GPS satellites, which speeds up the initial position fix. AGPS information may also help in finding satellites and getting positions in difficult conditions. To have AGPS features, services must be set up to provide AGPS information to the cell phone and the cell phone must be able to process AGPS

information. Note, the new Apple IPHONE version 2.0 uses AGPS.

5. Tower reports

In the absence of an accurate GPS location, service providers may record the location of the nearest cell tower. Check with the LBS to determine if Tower locations are used to determine cell phone locations.

6. GeoFencing

GeoFencing is a term used to describe a feature that enables the cell phone to only start tracking when it has entered or exited a predefined region, avoiding unnecessary tracking when your people are close to home, office, or school. Or GeoFencing may also mean that an alert is sent when their phone crosses a virtual fence. For example, AccuTracking will send email or SMS message when they move across the designated areas.

7. Speed Alerts

Some LBS providers provide email or SMS message alerts when specified speed limits are exceeded.

8. Tracking Map Quality

Most location services do not produce their own maps. Instead they purchase or license mapping products from other companies. Several popular services use Mapquest maps. Indeed, Mapquest can produce a map for just about anywhere in the world, but the service provider's license may be limited to United States. Microsoft MapPoint and Tiger map data are also popular for applications in the United States. If choosing between LBS providers, compare what the maps will look like. Aerial photos – street names are not available from an aerial photo but there is a better idea of the surrounding environment. The better location services will provide both maps and aerial photos.

9. Usage Costs

The costs associated with using the GPS for people tracking, include equipment costs, setup/activation fees, and usually network access subscriptions. In addition, the location service may charge for each location report or allot a limited number of reports and charge a premium for overages. For example Disney Mobile includes 5 location reports each month, but unlimited reporting is available as an optional plan.

10. Mobile to Mobile Tracking

Some tracking solutions enable access to tracking maps on a mobile device. The ability to track someone using a cell phone, by using another cell phone, conjures

up a chase scene from an old movie, where our hero is sitting in the back seat of a moving car with a radar-type device in a briefcase, shouting turn-by-turn directions to the driver in hot pursuit of evil villains. See, <http://www.travelbygps.com/articles/tracking.php> and <http://support.accutracking.com/docs/bbsetup.html>.

CAVEAT EMPTOR: A husband buys a new cell phone for his wife and activates a real time GPS plan. The program is hidden on her phone or Blackberry and the wife has no idea that wherever she goes she can be tracked.

In one of my favorite stories, a wife noted her husband going out at night on a regular basis, allegedly to his office, and she became suspect about her Husband's activities. The wife remembered that the husband had installed an EZTAG on their car. When the wife checked the online log it showed that while the husband's office was located South on the Hardy Toll Way; the husband was always headed North on the Hardy Toll Way every evening he claimed he was going to his office!

Occasionally a client will inquire about hiring a Private Investigator to place a GPS device on the spouses' car. Please be advised it is a violation of Texas law to install a tracking device on a vehicle unless the vehicle is registered in the client's name. See Occupations Code Chapter 1702, Section 1702.332. Also see Section 16.06 of The Texas Penal Code which states as follows:

- (b) A person commits an offense if the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person. © An offense under this section is a Class A misdemeanor.

Note that the same rules may not apply to law enforcement as revealed in *United States of America, Plaintiff-Appellee, v. Bernardo Garcia, Defendant-Appellant*. United States of Appeals for the Seventh Circuit, No. 06-2741, January 10, 2007, Argued-February 2, 2007, Decided 474 F.3d 994, wherein the police attached a GPS device to a suspect and the 7th Circuit found no violation of the suspect's constitutional rights.

Here is an example of a blackberry or Windows Mobile program that provides GPS tracking and hides the program so that the user is unaware of its presence. See, <http://www.skylab-mobilesystems.com/en/products/mobiletracker.html> which costs \$24.00. While it does not provide real time, it does maintain a log and with Google Earth, can pinpoint location and time relatively

easily.

11. Digital Cameras

Finally be aware that some digital cameras now provide GPS information (called tagging) and this information can be extracted to show the exact coordinates and times the photo was taken.

FACTOID: What mobile phone is most popular with the MIB and why?

VIII. INSTANT MESSAGING

How secure is Instant Messaging and can messages sent by Instant Messaging be retrieved?

Appendix 1 is a table which was created as a result of CNET's investigation of IM providers. See Page 15.

IX. BROWSER HISTORIES

A web browser is a software application which enables a user to display and interact with text, images, videos, music and other information typically located on a Web page at a website on the World Wide Web or a local area network. Text and images on a Web page can contain hyperlinks to other Web pages at the same or different website. Web browsers allow a user to quickly and easily access information provided on many Web pages at many websites by traversing these links. Web browsers date back to 1991 and were developed by Tim Berners-Lee. See http://en.wikipedia.org/wiki/Web_browser.

Web Browsers leave another trail on the internet that can be followed. In April 2008, the American Academy of Matrimonial Lawyers reported the following in an article entitled

“Married Browsers Beware: Top Divorce Lawyers Note Soaring Use of Internet and Spyware Evidence”:

CHICAGO, April 21 -- An overwhelming 79% of the nation's top divorce attorneys reported an increase in the frequency of Internet browser histories being used as evidence in divorce cases during the past five years, according to a recent survey of American Academy of Matrimonial Lawyers (AAML) members. In addition, 44% of the respondents also cited a noticeable increase in evidence taken from Spyware programs.

"Many spouses will use the Internet in order to act anonymously, but in many ways it's the most public thing someone can do," said

James Hennenhofer, president of the AAML. "Internet activity can provide valuable glimpses into the kinds of hidden activities that a husband or wife might be trying to conceal and Spyware programs can help to make this kind of monitoring extremely easy to conduct."

While 79% of AAML members who responded said Internet browser histories were a main source of information in divorce cases throughout the past five years, none of the respondents reported a decline in this information being used. Additionally, 21% saw no change in how often a spouse used these records for evidence during this time period.

Internet tracking through software was also noted as an increasingly popular means of gathering evidence. In all, 44% of AAML attorneys said that Spyware was used more often than not in divorces over the last five years. Only 2% of AAML members noticed it had been used less frequently than in previous years.

There has been a substantial increase in the examination of browser histories, leading to questions of "where have you been and why?" Again, much of the difficulty of these histories and computer use issues are authenticating the actual individual who was using the computer at that time. Remember that sometimes it is not just the issue of where and what has been accessed but the actual time on the computer. Computer and internet usage can be addictive and when large amounts of time at home are consumed on the computer it can be an important issue in discussion and trial of allocation or lack of allocation for "parenting time".

X. COFEE

Ever heard of COFEE? Probably not, but most law enforcement personnel and/or FBI agents have.

"Microsoft is now talking about COFEE, a tool they have released to some law enforcement agencies to let them take a look at Windows computer in a faster, less intrusive way that's easy to use. COFEE stands for "Computer Online Forensic Evidence Extractor" and details about what it can do are thin on the ground. That's understandable from a law enforcement perspective but when you combine a lack of hard facts to a distrust of Microsoft and some government agencies you get plenty of rumor, guesswork and outright paranoia all across the Internet.

See, Benjamin J Romano at the **Seattle Times**, who

has good overall coverage of the story quoting facts not supposition and guesswork. Microsoft says the tools come on a USB 'stick' which can be inserted into any running Windows computer - a series of scripts can gather information about what's on the machine and save it directly to the hard drive. It's said the tool is useful because it can be used to gather information while the machine is powered on-site and before it's turned off and removed. Of course that also means that COFEE could be used on a covert basis to quickly 'peek' into a computer and gather information without the owner knowing. Great for corporate spying on rival companies. Microsoft says that COFEE is meant for use "by law enforcement only with proper legal authority" but they can't be so naive as to believe the tools won't spread to other people and be used without legal approval. After all, Microsoft hasn't been able to control piracy of their other products. It may be that COFEE simply gives easy access to information that a computer professional can already gather. However it's that ease of access that makes COFEE a concern to some people - it increases the availability of private information to people with less computer skills but the interest (legal or not) in what's on someone else's computer. The speed benefit alleged with COFEE makes it more useful for secret spying on a computer compared with traditional tools." See <http://news.office-watch.com>

The website Betanews in a followup on COFEE reported the following:

In earlier accounts, COFEE had been variously explained as either a set of software tools or a series of about 150 commands. As previously reported, COFEE controversy started last week when some bloggers started rumors that Microsoft was handing out "backdoor keys" to Windows security. The blogs got sparked by an article published in the Seattle Times based on an interview with Brad Smith, Microsoft senior VP and general counsel. Last week, Smith gave a talk at a law enforcement conference in Seattle, where he characterized COFEE as a "Swiss army knife for law enforcement officers." In the Times article, reporter Benjamin J. Romano wrote that COFEE can "decrypt passwords and analyze a computer's Internet activity as data stored in the computer" -- words that soon touched off tirades among several incensed bloggers. In an update to his article, Romano said a Microsoft spokesperson had later written to him describing COFEE as "a compilation of publicly available forensics tools, such as password security auditing technologies." Although an initial statement to BetaNews contained no mention of the password tools, a

second e-mail from Microsoft provided the information that COFEE does "include password security auditing tools." Subsequently, last Thursday, BetaNews asked Microsoft to identify the kinds of passwords that might be audited or recovered by police using COFEE - Windows OS passwords, network passwords, or application passwords, for example.

And look at who developed it: COFEE was first conceived in 2006 by Anthony Fung, formerly of the Hong Kong Cybercrime Police Unit, as a way to simplify the collection of critical volatile evidence at computer crime scenes. With important support from both Microsoft and fellow law enforcement personnel, COFEE achieved a limited release in the summer of 2007 and is now used by forensic examiners in countries the world over."

XI. VOICE OF EXPERIENCE: DANGER IS ONLY A SPLIT SECOND AWAY

Instead of explaining the risk of using technology in family law cases, the following case indicates the dangers associated with the improper intersection of technology and family law.

United States District Court for the Central District of California, February 2005, Grand Jury, United States of America, CR No. 05-1046 © -RMT, Plaintiff v. Anthony Pellicano, Mark Arneson, Rayford Earl Turner, Kevin Kachikian, Robert Pfeifer, Abner Nicherie, Daniel Nicherie, and Terry Christensen, Defendants,

(Third) Superseding Indictment)

18 U.S.C. §1962(c): (Racketeer Influenced and Corrupt Organizations (RICO)); 18 U.S.C. §1962(d): (RICO Conspiracy); 18 U.S.C. §§ 1343, 1346 (Honest Services Wire Fraud); 18 U.S.C. § 1030 (a) (2) (B),(c) (2) (B) (I): (Unauthorized Computer Access of United States Agency Information); 18 U.S.C. §1028 (a) (7): (Identity Theft); 18 U.S.C. §1030 (a) (4): (Computer Fraud); 18 U.S.C. §371 (Conspiracy); 18 U.S.C. § 2511 (1) (a), (d): (Interception of Wire Communications); 18 U.S.C. §2512 (1) (b): (Possession of Wiretapping Device); 18 U.S.C. §1001 (a) (2): (False Statements); 18 U.S.C. §1512(b) (3): (Witness Tampering); 18 U.S.C. §1512 © (1): (Destruction of Evidence); 18 U.S.C. §2: (Aiding and Abetting and Causing an Act to Be Done); 18 U.S.C. § 1963 (RICO Forfeiture).

Pellicano was the "PI for the Stars" and after 9 days of jury deliberation (he represented himself) was

convicted on 76 of the 77 charges contained in the indictment against him. The last name in the indictment was a lawyer, Terry Christensen, who according to a February 20, 2008 article in the LA Times stated:

“Christensen is accused of paying Pellicano \$100,000 to wiretap the former wife of Christensen’s longtime client, Kirk Kerkorian, to gain a tactical edge in a bitter child-support case between the billionaire investor and his wife, Lisa Bonder Kerkorian. Christensen had long helped Kerkorian, one of the nation’s richest people and a Hollywood fixture for more than 30 years, oversee a vast empire that includes the MGM Grand and Bellagio hotels and, until last year, the MGM studio.

According to the indictment, the wiretapping of Lisa Kerkorian began March 15, 2002, when an attorney called Pellicano and told him to contact Christensen about “going after” the wife’s attorney in the child-custody dispute. During snippets of alleged conversations included in the indictment, Pellicano alluded to eavesdropping on conversations between Lisa Kerkorian and her attorneys that could help Christensen with a court hearing. Pellicano also told Christensen to “be careful” about the information he was receiving from the private eye because “there is only one way for me to know this,” the indictment said.

To add to Christensen’s problems, Pellicano is reported to have recorded his conversations with Christensen. See Vanity Fair, June, 2006.

If you ever needed to know what Federal Laws apply to wire tapping, just review the U.S.C. sections contained in this indictment.

As lawyers we have a duty to sue due diligence in the hiring and oversight of private investigators. In the case of *Noble vs. Sears, Roebuck and Co.*, 33 Cal.App 3rd 654, (July 25, 1973) the California Court concluded that Sears and it’s attorney’s may have vicarious liability for the acts of its agents, i.e., the private detective agency. The California Court found actionable “invasion of privacy” and ‘neglect entrustment of agents” claims by the Plaintiff.

The Court also noted: “The Florida Supreme Court recognized that an investigation done by trailing and shadowing a claimant could amount to an actionable invasion of privacy, if it is unreasonably intrusive. (*Tucker v. American Employers’ Insurance Company* (Fla.App. 1965) 171 So.2d 437 [13 A.L.R.3d 1020].)

It is uncertain as to whether Texas would follow a vicarious liability theory, but caution should be taken when employing private investigators.

Also remember, Intentional Torts are not covered by malpractice insurance. See Parker and Pine, *The Pellican’s Mess, Ethical Considerations for Attorney’s*

Who Hire Private Investigator’s in the Wake of Pellicano, June, 2006, <http://www.pmmlaw.com>

XII. CONCLUSION

Simply stated:

Forewarned is Forearmed.

APPENDIX I

	Secure logging-in	Secure conserv-ations	Logs kept of user logins	Logs kept of message content	For How Long	Government Wiretapping
AOL AIM	Yes	Yes	Yes	No	Won't say	Won't say
AOL ICQ	Yes	No	Yes	No	Won't say	Won't say
Facebook Chat ¹	No	No	Refused to Answer	Refused to Answer ²	Refused to Answer	Refused to Answer
Goggle Talk	Yes	Yes ³	Yes	No ⁴	Four Weeks	Won't Say
IBM Lotus Sametime	Yes	Yes	Yes	Configurable	Configurable	N/A
Microsoft's Windows Live Messenger	Yes	No ⁵	No	No	N/A	Won't Say
Skype	Yes	Yes	Yes	No	"A short time"	Cannot comply with wiretaps ⁶
Yahoo Messenger	Yes	No	Yes	No	"As long as necessary"	Won't say

¹ Over the course of a week, Facebook refused to reply to questions.

² Facebook has said both that chat history "is not logged permanently" and that it is archived for 90 days.

³ Encryption is on by default for the downloadable client, off by default for the Web, and not supported with the Google Talk Gadget.

⁴ Configurable: users can choose to log conversations in their Gmail chat archives if they wish.

⁵ Conversations are unencrypted, but files exchanged via Windows Live Messenger are encrypted.

⁶ Skype was the only IM company that said it could not perform a live interception if presented with a wiretap request: "Because of Skype's peer-to-peer architecture and encryption techniques, Skype would not be able to comply with such a request."