ELECTRONIC EVIDENCE DISCOVERY AND ADMISSIBILITY

Jacqueline M. Valdespino, Esquire

I. Electronic Evidence Discovery

The pace of technology always outruns the law designed to regulate it. (In the area of family law, think of assisted reproduction.) Computers in business have been used for fifty years, and yet the Rules of Civil Procedure and Evidence were late to address these forms of document/information storage. Imagine that file cabinets were invented in 1900, but nobody knew how to ask for the information inside of file cabinets until 1950.

Rule 34 of the Federal Rules of Civil Procedure provides that electronically stored information is subject to subpoena and discovery for use in legal proceedings. This rules is the key to making electronic storage grounds for discovery as evidence. Rule 26 provides that each company has the duty to preserve documents that may be relevant in a particular case. Thus, companies are bound to preserve and turn over computer-stored records and computer-generated records.

Rule 1001(1) of the Federal Rules of Evidence defines “writing and recordings” as letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation. The notes to this rule state that considerations underlying this rule “dictate its expansion to include computers, photographic systems, and other modern developments.”

Valdespino & Associates, PA
2641 Abaco Ave, Miami, FL 33133
(305) 442-1200
Jacquie@valdespinopa.com

To keep you apace with the technology that everyone is using, always include in interrogatories and requests for production of documents information that is contained on a computer or electronic storage system (even a digital camera qualifies). Data will commonly be located on individual desktops and laptops, network hard disks, removable media (e.g., floppy disks, flash drives, tapes and CDs) and, increasingly, personal digital assistants (e.g.,IPad's and Kindle Fires). Data may also be in the possession of third parties, such as Internet service providers, and on the computer systems of other peripherally involved entities.

Who

- Think of requesting information from the electronic database storage systems of: the spouse, a closely held company, an employer, friends or relatives, investment firms, other entities specific to the case.
- In a divorce case in Southern California, the husband had given his old computer to the parties' daughter. The wife turned the computer over to Computer Forensics, Inc., and was able to discover more assets than the husband had admitted.

What

- What type of files: word processing files, spreadsheet files with asset lists, budgets, financial plans with projections, historical expenditures, experts' financial models; financial management programs with check, credit card asset and investment data; database files with financial data, contact lists, assets; e-mail programs; calendar programs; browser history files; e-mail, along with header information, archives, and any logs of e-mail system usage; data files

created with word processing, spreadsheet, presentation, or other software; databases and all log files that may be required; network logs and audit trails; electronic calendars, task lists, telephone logs, contact managers.

When

- Set time parameters for the creation of files. Send a spoliation letter to give advance notice so that data is not destroyed early on in the case.

Where

- Hard drives, floppy disks, optical disks, network storage, remote Internet storage, the "cloud", handheld device, backup device; active data storage, including servers, workstations, laptops, offline storage including backups, archives, zip disks, tapes, CD-ROM, and any other form of media.

Why

- Because sometimes it's the only evidence that exists on an issue. Because it may show inconsistencies with hard copy evidence that will lead to new evidence or impeachment. Because it may be easier to search.

How

- When you think that there is electronic evidence worth having, the first thing to do is issue a notice to preserve and retain the data. This spoliation letter should be sent early on in the case.
- Federal Rule of Civil Procedure 26(a)(1)(C) obligates parties to provide opponents with copies of or descriptions of documents, *data compilations*, and tangible things in a party's possession, custody or control.

Valdespino & Associates, PA
2641 Abaco Ave, Miami, FL 33133
(305) 442-1200
Jacquie@valdespinopa.com

- Federal Rule of Civil Procedure 34 permits a party to serve on another party a request to produce *data compilations*.
- Deposition of custodian or electronic records.
- Protective order and order to turn over hard drive.

The resources listed at the end of this article provide form requests for discovery and form requests for retention.

II. Computer Forensics, or How to Find the Stuff You Just *Know* They're Hiding[1]

Computer forensics is the collection, preservation, analysis and presentation of electronic evidence. As a family law attorney, you can be looking for correspondence, tax and accounting records, addresses and phone numbers, presentation files, business plans, calendaring information, task lists, etc. Any of these records can reside on a computer in the form of text files, graphic files, audio files, hidden files, system files, e-mail, and even deleted files (if not overwritten).

Computer forensics can resuscitate deleted files if not overwritten, determine when the file was created and modified, and when the file was deleted (if it was deleted). Computer forensics can also determine how data may have leaked, how e-mail may have been forged, how the network may have been penetrated, and whether keystroke loggers or any other tracking device have been placed on the system.

Importantly, a computer forensic specialist can obtain a hard drive and establish

---

[1]By employing a computer forensic specialist, you are looking for the "takedown." In 1996, a book bearing the title "Takedown" told the tale of Kevin Mitnick, a hacker who had wrought havoc all over the globe. His capture was called a "takedown," a since then, the word has come to mean "gotcha" for a computer forensic specialist when he or she find a pivotal piece of electronic evidence that will bring someone down. It's the

chain of custody and authentication. It might be important to obtain a hard drive and immediately turn it over to a computer forensic specialist rather than boot up the computer yourself (or have your client do it), because the mere act of booting up changes the registry on about 400-600 Windows files.

III. Evidentiary Issues: Authentication, Hearsay, Privilege

Authentication may be achieved by Requests for Admissions, admissions during deposition, adoptive admission imputed to the recipient of the e-mail, admissions by a party opponent. Hearsay objections as to the contents of the electronic record may be overcome by the business record exception, the contents of the electronic record as a present sense impression, the contents of the electronic record as an excited utterance, the contents of the electronic record as statement against interest, the necessity exception to the rule against hearsay, the contents of the electronic record as relevant to explain conduct, or the contents of the electronic record to establish declarant's intent.

A few cases concerning evidentiary issues of electronic evidence in the family law context provide guidance:

- *Hazard v. Hazard*, 833 S.W.2d 911 (Tenn. Ct. App. 1991): The copy of a letter from the husband to his former attorney stored in the husband's computer in the marital home, to which the wife had complete access, was not privileged.
- *Stafford v. Stafford*, 641 A.2d 348 (Vt. 1993): The wife found on the family computer a file called "MY LIST" which was an inventory and description of the husband's sexual encounters with numerous women. The wife testified she found

smoking gun of the future.

it on the family computer and that it was similar to a notebook that she had discovered the husband's handwriting giving similar accounts. The notebook disappeared. "Plaintiff's testimony of the source of the document as a file in the family computer was sufficient to identify what it was."

- *In re Marriage of DeLarco*, 313 Ill. App.3d 107, 728 N.E.2d 1278 (2000): Testimony of wife's attorney concerning his firm's billing software and procedures for review of records produced by it established adequate foundation under business records exception to hearsay rule for admission of computer- stored billing records in connection with wife's petition for contribution to her attorney fees in dissolution action.
- *Fenje v. Feld*, 2003 U.S. Dist. LEXIS 24387 (N.D. Ill., Dec. 8, 2003): Authentication of e-mail "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). The court also noted that email communications may be authenticated as being from the purported author based on an affidavit of the recipient; the email address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the email communication that is being authenticated.
- *Etzion v. Etzion* 7 Misc.3d 940, 96 N.Y.S.2d 844 (Sup. Ct. 2005): In matrimonial action, wife moved by order to show cause for order permitting her to examine data on husband's personal and business computers. Court held that wife was entitled to copy data from husband's computers and to examine non-privileged business records found therein.

- *Bill S. v. Marilyn S.*, 8 Misc.3d 1013(A), 801 N.Y.S.2d 776 (Table) (Sup. 2005): During the course of that discovery, the Husband has served undated Subpoenas Duces Tecum on, inter alia: Nextel Communications, pertaining to telephone records of non-party Michael R. identified by the Husband as one of the Wife's paramours; AT & T Wireless, pertaining to the Wife's phone number and non-party Jose B.'s number identified as another of the Wife's paramours; America Online ("AOL") Legal Department, seeking three years of "instant messenger chat logs" between the Wife and Mr. R.; and finally, Trac-Fone Wireless, seeking the Wife's telephone records for the past three years. The reason set forth in the Subpoenas for production of said material is merely that "the non-party witness has material and relevant information for the prosecution and defense of issues raised in the action." Held: Although the body of the electronic messages themselves may be discoverable for financial purposes, they are not so to establish the merits of the matrimonial action.
- *Miller v. Meyers*, 2011 WL 210070 (W. D. Ark. 2011): Finding husband civilly liable under the SCA and Ark. state computer trespass statute for divorce-related email theft with a keylogger. As a matter of law, at summary judgment stage, H admitted the theft and there was no defense. Also potentially liable under the CFAA but material issues of fact still existed regarding the $5,000 damages threshold. Under wiretap act, court holds: The covert installation of an automatic recording device would be more likely to violate the FWA, while eavesdropping on a telephone conversation using an extension line has been found to be an

exception to liability under the FWA. See id. The Court finds that Defendant's monitoring of internet traffic on his own home network is analogous to the latter. For instance, Plaintiff has presented no evidence that Defendant recorded any information during the course of his monitoring, and there is some indication that Plaintiff was aware, or should have been aware, that Defendant was monitoring her. Defendant's monitoring activity should be excepted from liability under the FWA. Furthermore, the key logger only allowed Defendant to learn passwords, which were used to access Plaintiff's e-mails. Defendant did not obtain e-mails contemporaneously with their transmission, and thus, the FWA does not apply. See *Bailey v. Bailey*, 2008 U.S. Dist. LEXIS 8565, *12 (E.D.Mich.2008) (finding FWA did not apply to case in which ex-husband used keylogger to access his then wife's e-mails). The Court finds, as a matter of law, that Defendant's conduct in monitoring internet traffic on his home network and in using a keylogger program to access his then wife's e-mails was not a violation of the FWA. Defendant's Motion for Summary Judgment is therefore granted as to Plaintiff's claims under the FWA.

- *Griffin v. State*, 419 Md. 343, 19 A.3d 415 (2011) (not a family law case, but interesting): Applied the rules of evidence to reject authentication of a MySpace page. Held: The state did not sufficiently authenticate pages that allegedly were printed from defendant's girlfriend's profile on a social-networking website, and thus the pages, which allegedly contained a statement by the girlfriend that “snitches get stitches,” were inadmissible at a murder trial, even though the pages contained a picture of the girlfriend, her birth date, and her location; the

state did not ask the girlfriend whether the profile was hers and whether its contents were authored by her, and the picture, birth date, and location were not authenticating distinctive characteristics, given the prospect for abuse and manipulation of a social-networking website by someone other than the purported creator or user.

- *Parnes v. Parnes* 80 A.D.3d 948, 949, 915 N.Y.S.2d 345, 348 (N.Y.A.D. 3 Dept. 2011): Plaintiff [wife] apparently discovered a page of one of the e-mails on defendant's [husband's] desk and, while searching for the remainder of the letter, discovered the user name and password for defendant's e-mail account. She used the password to gain access to defendant's account, printed the e-mails between him and Van Ryn [his divorce attorney], and turned them over to her counsel. Plaintiff averred that she discovered a single printed page of a five-page e-mail on a desk in the marital residence. The parties acknowledge that this desk was located in a room used as an office and the parties, their nanny and babysitters all used that room. Defendant contends that the desk contained only his papers and plaintiff had her own desk in the same room, but plaintiff appears to disagree. Regardless of whether the parties had separate desks, by leaving a hard copy of part of a document on the desk in a room used by multiple people, defendant failed to prove that he took reasonable steps to maintain the confidentiality of that page. However, defendant took reasonable steps to keep the e-mails on his computer confidential. Defendant set up a new e-mail account and only checked it from his workplace computer. Leaving a note containing his

user name and password on the desk in the parties' common office in the shared home was careless, but it did not constitute a waiver of the privilege. Defendant still maintained a reasonable expectation that no one would find the note and enter that information into the computer in a deliberate attempt to open, read and print his password-protected documents *(see Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp.2d 548, 560-562 [S.D.N.Y.2008]). Plaintiff admits that after she found the one page, she searched through defendant's papers in an effort to find the rest of the document, instead found the note, then purposely used the password to gain access to defendant's private e-mail account, without his permission, to uncover the remainder of the e-mail. Under the circumstances, defendant did not waive the privilege as to the e-mails in his private e-mail account (*see Leor Exploration & Prod., LLC v. Aguiar*, 2010 WL 2605087, *18, 2010 U.S. Dist. LEXIS 76036, *63-65 [S.D. Fla.2010]; cf. *Stengart v. Loving Care Agency, Inc*., 201 N.J. 300, 321-324, 990 A.2d 650, 663-665 [2010]).

This case is good support for the notion that if you put a password on something, you have a right of privacy; and the mere fact that someone found your password through extraordinary effort does not show waiver. Wife was allowed to look at the surface of the general marital desk, she was not allowed to dig into the papers on it.

IV. A Sure Way for Evidence *Not* to Be Admitted: Cyber-Misconduct

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 - 2522, generally prohibits the interception of wire, electronic, and oral communications. Title 18 U.S.C. § 2511(1)(a) applies to the person who willfully intercepts such wire, electronic, and oral communications, and subsection (c) to any person who, knowing or having reason to know that the communication was obtained through an illegal interception, willfully discloses its contents. The Electronic Communications Privacy Act of 1986, 100 Stat. 1848 enlarged the coverage of Title III to prohibit the interception of "electronic" as well as oral and wire communications. By reason of that amendment, as well as a 1994 amendment which applied to cordless telephone communications, 108 Stat. 4279, Title III now applies to the interception of conversations over both cellular and cordless phones. Although a lesser criminal penalty may apply to the interception of such transmissions, the same civil remedies are available whether the communication was "oral," "wire," or "electronic," as defined by 18 U.S.C. § 2510 (1994 ed. and Supp. V).

Importantly, an "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12) (1994 ed., Supp. V).

Key to a number of family law cases dealing with “spousal snooping” of electronic mail is that accessing e-mail *that is already stored on a computer* is *not* an interception

of e-mail in violation of the Act. Interception comes only with transmission. *See Fraser v. Nationwide Mutual Insurance* Co., 352 F.3d 107 (3d Cir. 2003); *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457 (5th Cir. 1994); *see also U.S. v. Councilman*, 245 F.Supp.2d 319 (D. Mass. 2003); *Wesley College v. Pitts*, 974 F.Supp. 375 (D. Del.1997), summarily aff'd, 172 F.3d 861 (3d Cir.1998).

Finally, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, applies to three types of computers: (1) computers owned by the United States; (2) computers storing certain types of sensitive information; and (3) any "protected computer." Sensitive information includes information relevant to national defense or foreign policy, records of financial institutions, or consumer credit information. 18 U.S.C. § 1030(a)(1, 2).

A protected computer is any computer which is used in interstate or foreign commerce or communication. Since almost every computer is used at some time to send a communication to someone in another state, and is used to receive communications from other states via the internet, the definition of protected computer is quite broad.

The Act prohibits three actions: (a) intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining . . . information from any protected computer if the conduct involved an interstate or foreign communication; (b) knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and by means of such conduct furthers the intended fraud; (c) intentionally accessing a protected computer

without authorization, and as a result of such conduct, causes damage. In family law cases, the key concept in § 1030 is use "without authorization."

Some cases in the family law context have addressed these issues:

- In *Jessup-Morgan v. AOL*, 20 F. Supp.2d 1105 (E.D. Mich. 1998), the husband's paramour posted an Internet message on an electronic bulletin board inviting readers to telephone the estranged wife to seek sexual liaisons. The message said "I'm single, lonely, horny, and would love to have either phone sex or a in person sexual relationship with someone other than myself…." *Id.* at 1106. The estranged wife was deluged with unwanted telephone solicitations for sex while living at her parents' home with her two young children. AOL responded to wife's subpoena and divulged the identity of its subscriber who had perpetrated this harassment in violation of the AOL subscriber agreement. The subscriber (Husband's lover and then second wife) sued AOL under the ECPA, for breach of contract and for invasion of privacy, seeking $47 million in damages. She claimed damages from disclosure that affected her own child custody hearing as well as her future husband's divorce. The Court held that the ECPA was inapplicable because the disclosure was not of content, but merely the identity of the author of the communication. The case was dismissed.
- *Conner v. Tate*, 130 F. Supp.2d 1370 (2001): A woman sued her lover's wife for illegally intercepting and taping phone and voice mail messages between the lovers and then distributing the information to the local police department. Paramour stated cause of action.
- *U.S. v. Scarfo*, 180 F. Supp.2d 572 (D. N.J. 2001): Keystroke programs are not in

violation of any law, because they do not intercept communications, they do not access the computer in an unauthorized manner, and they cause no harm to the computer or user.

- *Hazard v. Hazard*, 833 S.W.2d 911 (Tenn. Ct. App. 1991): The copy of a letter from the husband to his former attorney stored in the husband's computer in the marital home, to which the wife had complete access, was not privileged.
- *Stafford v. Stafford*, 641 A.2d 348 (Vt. 1993): The wife found on the family computer a file called "MY LIST" which was an inventory and description of the husband's sexual encounters with numerous women. The wife testified she found it on the family computer and that it was similar to a notebook that she had discovered the husband's handwriting giving similar accounts. The notebook disappeared. "Plaintiff's testimony of the source of the document as a file in the family computer was sufficient to identify what it was."
- *Byrne v. Byrne*, 168 Misc. 2d 321, 650 N.Y.S.2d 499 (1996): The computer in this case was a laptop that was owned by the husband's employer, Citibank, and used by the husband as part of his employment. The computer was also used by the husband for personal financial information unrelated to work. The wife took the laptop and gave to her attorney. The husband and employer asserted that the computer could not be accessed by the wife's attorney.

> The *Byre* court held, "The computer memory is akin to a file cabinet. Clearly, [the wife] could have access to the contents of a file cabinet left in the marital residence. In the same fashion, she should have access to the contents of the computer. [The wife] seeks access to the computer memory on the grounds that [the husband] stored information concerning his finances and personal business records in it.

Such material is obviously subject to discovery."

- *White v. White*, 344 N.J. Super. 211, 781 A.2d 85 (2001): In a divorce action, the husband filed a motion to suppress his e-mail that had been stored on the hard drive of the family computer. The court held that the wife did not unlawfully access stored electronic communications in violation of the New Jersey wiretap act, and wife did not commit the tort of intrusion on seclusion by accessing those e-mails. Here, the wife hired Gamma Investigative Research, which copied the files from the hard drive. The files contained e-mails and images he had viewed on Netscape. The company sent the wife a report on the contents of the files. The husband's e-mail program, on AOL, requires a password.

  > Key to this decision is that once e-mails are downloaded from the e-mail server, they are not stored for the purpose of electronic transmission, and they are thus outside the protections of the wiretap act. Further, the wife was able to access the files without a password by going through other files.

- *Zepeda v. Zepeda*, 632 N.W.2d 48 (S.D. 2001): Husband installed software on home computer to covertly monitor wife's keystrokes. He discovered that she engaged in highly erotic discussions in Internet chat rooms. Husband separated from wife and later accepted a job in Texas. Husband believed wife was an Internet addict and that this led her to have sex with a man in the family home while the child was sleeping. A temporary custody order prohibited wife from using the Internet unless required by her employment. At trial, husband introduced computer log-on records to show substantial use of the Internet in the household. The court pointed out that these records did not show which member of the household used the computer or whether it was just left

logged on.

- *State v. Appleby*, 2002 WL 1613716 (Del. Super. 2002): After the husband and wife co-mingled their computer hardware, using it freely as each saw fit, its ownership and possession were joint. Each spouse was entitled to the equipment as much as the other. Under the circumstances, where the hard drive was left broken, uninstalled and in the estranged wife's possession and where the hard drive once was installed in the estranged wife's computer, she had complete access to it while it was working and hundreds of her personal documents remained on it, the hard drive was "theirs" in every sense.
- *Evans v. Evans*, 610 S.E.2d 264 (N.C. Ct. App. 2005): Sexually explicit e-mails that wife had sent to physician, offered by husband in divorce action in support of grounds for divorce and in support of denying post-separation spousal support to wife, were not illegally intercepted in violation of federal Electronic Communications Privacy Act (ECPA), where interception of e-mails was not contemporaneous with transmission; e-mails were stored on and recovered from hard drive of family computer.

V. CASE LAW ON DISCOVERY OF SOCIAL NETWORKING INFORMATION

- *Mackelprang v. Fidelity Nat'l Title Agency of Nevada, Inc.*, No. 06-788, 2007 WL 119149, at *8 (D. Nev. 01/09/07): The court denied the defendant's motion to compel production of private messages on the plaintiff's MySpace page, which defense counsel claimed constituted “the same types of electronic and physical relationships she [the plaintiff] characterized as sexual harassment in her Complaint.” The court's rationale was that the defense had “nothing more than suspicion or speculation as to what information might be contained in the private

messages." The court did, however, allow discovery into e-mail messages that would be relevant to the emotional-distress claims.

- *Beye v. Horizon Blue Cross Blue Shield*, No. 06-5377 (D. N.J.) (Order dated 12/14/07 (Dkt. # 84) at 5 n.3) and Order dated 10/30/07 (Dkt. #57) at 8); *Foley v. Horizon Blue Cross Blue Shield*, No. 06-6219 (D. N.J.) (Order dated 11/01/07) (Dkt. # 48) at 8): In two consolidated cases relating to insurance coverage for eating disorders, a federal magistrate judge ruled that minors' writings shared with others on social networking sites were discoverable. Plaintiffs sued an insurer on behalf of minors who were denied insurance coverage for their eating disorders. The insurer sought production of all e-mails, journals, diaries, and communications concerning the minor children's eating disorders or manifestations and symptoms of the eating disorders. The plaintiffs argued that disclosure of such materials would be harmful to the minors and negatively impact their recovery. The court ordered production of all entries on web pages, such as Facebook and MySpace, which the minors had shared with others, reasoning that the "privacy concerns are far less where the beneficiary herself chose to disclose the information."
- *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-1958, 2009 WL 1067018, *2 (D. Colo. 04/21/09): Federal magistrate judge denied a motion for a protective order regarding subpoenas defendants had issued to social networking sites. The plaintiffs were seeking damages for alleged injuries arising out of an electrical accident at a Wal-Mart store. Wal-Mart's attorneys discovered through internet

searches that the plaintiffs had posted information that related to and discounted their damage claims on the publicly available portions of social networking sites. Wal-Mart subpoenaed information from the social networking sites regarding the private areas of the plaintiffs' accounts. The court rejected the plaintiffs' arguments that their social networking account information was privileged and held that "the information sought within the four corners of the subpoenas issued to Facebook, My Space, Inc., and Meetup.Com is reasonably calculated to lead to the discovery of admissible evidence a[nd] is relevant to the issues in this case."

- *Moreno v. Hanford Sentinel, Inc*., 172 Cal. App. 4th 1125, 1130-31 (Cal. Ct. App. 2009): An author who posted an article on MySpace had no expectation of privacy regarding the published material, even if the author expected only a limited audience. The Moreno court concluded that by publicizing her opinions on MySpace, "a hugely popular" social networking site, "no reasonable person would have had an expectation of privacy regarding the published material" and that the author "opened the article to the public at large. Her potential audience was vast."

VI. FLORIDA SPECIFIC CASES AND RULES

Cases

- *Castellano v. Winthrop,* 27 So.3d 134 (Fla 5th DCAA 2010): a lawyer was disqualified for receiving reviewing and using the opposing party's USB flash drive which contained electronic files including attorney/client communications, client litigation notes and attorney work product.

- *Minakan v. Husted,* 27 So.3d 696 (Fla. 4th DCA 2010): Petition for Cert granted and a disqualification order reversed and remanded for further proceedings because the trial court did not hear the Wife's evidence before entering the order of disqualification. The case arises from an attorney receiving an email from the opposing party to his lawyer obtained because the client hacked into her husband's email account.
- *Nova Southeastern University, Inc. vs. Jacobson,* 25 So.3d (Fla. 4th DCA 2009): (not a family case but instructive on obtaining privileged information): Motion for protective order denied and case remanded for further proceedings because trial court did not apply correct law in evaluating the privilege claim.
- *Young v. Young*, 96 So.3d 478 (Fla. 1st DCA 2012): Wife's conduct of changing husband's e-mail password, appropriating his e-mails, and including information from them in a filing in dissolution of marriage proceeding did not amount to "cyberstalking," as would support a domestic violence injunction against her, although it was improper behavior, where her conduct did not include electronic communications of words, images, or language directed at husband. *See also Murphy v. Reynolds*, 55 So.3d 716 (Fla. 1st DCA 2011) (implicitly approving the finding that "offensive email, hacking into another person's email account, deleting email or changing an email signature," could be grounds for a repeat-violence injunction under section 784.046(2), Florida Statutes (2009), though not in that case).
- *France v. France*, 90 So.3d 860 (Fla. 5th DCA 2012): Ex-wife, who was North

Carolina resident, was subject to personal jurisdiction in Florida in ex-husband's action for violation of Florida Security of Communications Act based upon ex-wife's alleged illegal recording of telephone calls between ex-wife, who was in North Carolina, and ex-husband, who was in Florida.

- *Holland v. Barfield*, 35 So.3d 953 (Fla. 5th DCA 2010): Trial court departed from the essential requirements of law causing irreparable harm to defendant in a wrongful death action by ordering defendant to produce to plaintiff her computer hard drive and cell phone; there was no evidence of destruction of evidence or thwarting of discovery, the electronic media was sought only as a back-up for information sought in other discovery requests as to which a compromise was reached between the parties, and discovery order allowed complete access to the information on the hard drive and phone without regard to defendant's constitutional right of privacy, her right against self-incrimination, or any applicable privileges.
- *O'Brien v. O'Brien*, 899 So.2d 1133 (Fla. 5th DCA 2005): Wife illegally "intercepted" husband's electronic communications with another woman via electronic mail and instant messaging, within meaning of Security of Communications Act, when she installed spyware program on computer which simultaneously copied electronic communications *as they were being transmitted*.

VII. Ethical Opinions: (Practice Tip: There are no ethics opinions specifically on spyware and the installation of spyware. However, there have been investigations by the Florida Bar of lawyers whom have advised clients to install

spyware. This is an area full of uncertainty. Many of the cases deal primarily with issues of how information is obtained as a threshold issue.

- ***PROFESSIONAL ETHICS OF THE FLORIDA BAR OPINION 10-2 September 24, 2010***: A lawyer who chooses to use Devices that contain Storage Media such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition, including: (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality; (2) inventory of the Devices that contain Hard Drives or other Storage Media; (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.
- ***FLORIDA BAR STANDING COMMITTEE ON ADVERTISING ADVISORY OPINION A-00-1 (Revised) April 13, 2010:*** An attorney may not solicit prospective clients through Internet chat rooms, defined as real time communications between computer users. Lawyers may respond to specific questions posed to them in chat rooms. Lawyers should be cautious not to inadvertently form attorney-client relationships with computer users.
- ***PROFESSIONAL ETHICS OF THE FLORIDA BAR Opinion 06-1 April 10, 2006:*** Lawyers may, but are not required to, store files electronically unless: a

statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests. Files stored electronically must be readily reproducible and protected from inadvertent modification, degradation or destruction.

- ***PROFESSIONAL ETHICS OF THE FLORIDA BAR OPINION 06-2 September 15, 2006:*** A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata. 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. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information's receipt. The opinion is not intended to address metadata in the context of discovery documents.
- ***PROFESSIONAL ETHICS OF THE FLORIDA BAR OPINION 07-1September 7, 2007:*** A lawyer whose client has provided the lawyer with documents that were wrongfully obtained by the client may need to consult with a criminal defense lawyer to determine if the client has committed a crime. The lawyer must advise the client that the materials cannot be retained, reviewed or used without informing the opposing party that the inquiring attorney and client have the documents at issue. If the client refuses to consent to disclosure, the inquiring attorney must withdraw from the representation. ***(Note: Consider whether the installation of spyware may lead to "wrongfully obtained evidence" and may subject the lawyer to an ethical violation.)***

VIII. Statutes, Rules

F.S.A. § 934.03: Interception and disclosure of wire, oral, or electronic communications prohibited

In re Amendments to Florida Rules of Civil Procedure--Electronic Discovery, 95 So.3d 76 (2012):

> First, rule 1.200 (Pretrial Procedure) is amended to allow the trial court to consider various issues related to electronic discovery during a pretrial conference, including the possibility of obtaining admissions of fact, the voluntary exchange of documents and electronically stored information, and stipulations regarding the authenticity of documents and electronically stored information; the need for advance rulings on the admissibility of some documents or ESI; and finally, specifically as to electronically stored information, the possibility of an agreement between the parties regarding the extent to which such information should be preserved and the form in which it should be produced. Similarly, rule 1.201 (Complex Litigation) is also amended to require the parties in a complex civil case to address the possibility of an agreement between them addressing the extent to which electronic information should be preserved and the form in which it should be produced.
>
> Next, rule 1.280 (General Provisions Governing Discovery) is amended to expressly authorize discovery of electronically *77 stored information. Rule 1.280 is also amended to add new subdivision (d), which provides some

specific limitations on discovery of ESI; the subsequent subdivisions are relettered accordingly. Under new subdivision (d)(1), a person may object to a discovery request seeking electronically stored information. On a motion to compel discovery, or a motion for a protective order, the person from whom the discovery is sought must show that the information sought or the format requested is not reasonably accessible because of undue burden or cost. If this showing is made, the court may nonetheless order the discovery if the requesting party shows good cause. However, the court may specify certain conditions of discovery, including ordering that some or all of the expenses incurred while complying with the discovery request be paid by the party seeking the discovery. Under subdivision (d)(2) the court, in addressing a motion pertaining to discovery of ESI, must limit the frequency or extent of discovery if it determines that the information sought is: (i) unreasonably cumulative or duplicative, or can be obtained from another source or in another manner that is more convenient, less burdensome, or less expensive; or (ii) the burden or expense of the discovery outweighs its likely benefit.

Rule 1.340 (Interrogatories to Parties) and rule 1.350 (Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes) are both amended to allow for the production of electronically stored information, either as an answer to an interrogatory or in response to a specific request. Both rules provide for a party to produce the ESI in the form in which it is ordinarily maintained or in a reasonably usable form.

Rule 1.380 (Failure to Make Discovery; Sanctions) is amended to provide that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information that was lost as a result of the routine, good-faith operation of an electronic information system.

Finally, rule 1.410 (Subpoena) is amended to authorize a subpoena requesting electronically stored information. A person receiving a subpoena may object to the discovery of the ESI. The person from whom discovery is sought must show that the information or the form requested is not reasonably accessible because of undue costs or burden. If that showing is made, the court may nonetheless order the discovery if the requesting party shows good cause and consistent with the limitations provided in rule 1.280(d)(2) discussed above. The court may also specify conditions of the discovery, including ordering that some or all of the expenses be paid by the party seeking the discovery.

Valdespino & Associates, PA
2641 Abaco Ave, Miami, FL 33133
(305) 442-1200
Jacquie@valdespinopa.com

Some Law Review Articles on Electronic Evidence and Discovery

Linda Volonino, *Electronic Evidence and Computer Forensics*, 12 Communications of the Association for Information Systems, Article 27 (October 2003)
http://cais.isworld.org/articles/12-27/article.pdf

Jason Krause, *Unlocking Electronic Evidence: ABA Task Force Offers Draft E-Discovery Standards*, 3 No. 5 ABA J. E-Report 5 (Feb. 6, 2004)
<http://www.abanet.org/journal/ereport/f6litigate.html>

Andrew T. Wampler, *Digital Discovery: Electronic Options Make the Search for Evidence a New Adventure*, 40 Tenn. B.J. 14 (Feb. 2004)

Comment, Shane Givens, *The Admissibility of Electronic Evidence at Trial: Courtroom Admissibility Standards*, 34 Cumb. L. Rev. 95 (2003-2004)

David Narkiewicz, *Electronic Discovery and Evidence*, 25 Pa. Law. 57 (Dec. 2003)

Thomas J. Casamassima, Edmund V. Caplicki III, *Electronic Evidence at Trial: The Admissibility of Project Records, E- Mail, and Internet Websites* 23 Construction Law. 13 (Summer 2003)

Wade Davis, *Computer Forensics: How to Obtain and Analyze Electronic Evidence*, 27 Champion 30 (June 2003)

Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation*, 29 Rutgers Computer & Tech. L.J. 219 (2003)

Christopher D. Payne, *Discovery of Electronic Evidence*, 1 Comm. Computer and Law Office Tech. (2001)

Kimberly D. Richard, *Electronic Evidence: To Produce or Not to Produce, That Is the Question*, 21 Whittier L. Rev. 463 (1999)

Kevin Eng, *Spoliation of Electronic Evidence*, 5 B.U. J. Sci. & Tech. L. 13 (1999)

Christine Sgarlata Chung, *The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence*, 4 B.U. J. Sci. & Tech. L. 5 (1998)

Some Other Useful Resources

George J. Socha, Jr., *Discovering and Using Electronic Evidence* (ABA Section of Litigation Feb. 2001) (35 pp., $12.50) (contains Notice to Preserve and Retain Electronic Data; Notice of Avoid Destruction of Electronic Data; Short Form Request for Production of Electronic Media; Sample Deposition Questions for Custodians of Electronic Records; Sample Request for Production of Documents)

Michael Arkfield, *Electronic Discovery and Evidence* (Law Partner Publishing LLC, 2004-2005 ed.) ($199.95)

Adam I. Cohen & David J. Lender, *Electronic Discovery: Law and Practice* (Aspen 2003) ($195.00)

Some Internet Resources

Law.Com: Electronic Data Discovery
http://www.law.com/special/supplement/e_discovery/preparation_is_key.shtml

Steven Ungar and Katherine Foldes, *Electronic Evidence: Issues Arising in Domestic Relations Cases*
http://www.lanepowell.com/pubs/pdf/ungars_001.pdf

Electronic Evidence Information Center
http://www.e-evidence.info/legal.html
(A pretty amazing cite, with links to hundreds of other cites and articles on e-discovery)

LexisNexis Applied Discovery Center on Electronic Discovery
http://www.lexisnexis.com/applieddiscovery/clientResources/eDiscoveryInDepth.asp

ABA Law Practice Management: Systematic Discovery and Organization of Electronic Evidence (Feb. 2003)
http://www.abanet.org/lpm/lpt/articles/tch0214031.html

Electronic Discovery (California focus, but lot's of cases nationwide and general principles)
http://californiadiscovery.findlaw.com/electronic_discovery_general.htm

Rehman Technology Services: Case Law on Admissibility of Electronic Evidence
http://www.surveil.com/case_law.htm

Unlocking, Discovering and Using Digital Evidence (Annual Meeting 2003)
http://www.abanet.org/scitech/annual/5.pdf
(contains sample preservation letters, requests, interrogatories, etc.)
SETEC Investigations, Legal Tools

Valdespino & Associates, PA
2641 Abaco Ave, Miami, FL 33133
(305) 442-1200
Jacquie@valdespinopa.com

Sample interrogatories, requests for production of documents, etc.
http://www.setecinvestigations.com/lawlibrary/legaltools.php

Discovery Resources
Sample electronic discovery interrogatories and requests for production
http://www.discoveryresources.org/docs/eddrequest.doc

Computer Forensics, Inc.
Sample interrogatories, etc.
http://www.forensics.com/html/resource_sampledocs.html