DIGITAL OFFENSE AND DEFENSE: OBTAINING ELECTRONIC EVIDENCE LEGALLY, USING IT PROPERLY, AND PROTECTING YOUR CLIENT ALONG THE WAY

Jacqueline M. Valdespino, Esq.
Valdespino & Associates, PA
Fellow, American Academy of Matrimonial Lawyers
Board Certified in Matriminial and Family Law
Miami, Florida

Description:

Family law cases often present the unique situation where the client is sleeping with the enemy. The opposing party has access to and can easily implement a plan to obtain digital information with spyware and/or other hacking efforts in the hopes of gaining an advantage in the proceedings. Join the experts as they provide you with a practical approach to keeping electronic communications and digital information private and secure, even from the enemy close by. With this foundation, the experts will then address how to obtain digital information legally, what to do if the client provides you with information obtained illegally, and perhaps most importantly, how to effectively use electronic evidence in court.

I. HOW PARTIES OBTAIN EVIDENCE ILLEGALLY (AND THE CONSEQUENCES) aka CYBER-MISCONDUCT

A divorce attorney's bad dream: your client comes into your office with a sheaf of papers and proudly announces: Look what I got from my spouse's computer! Or your client plays an audio recording from his/her smartphone, and says, I made this recording when he/she didn't know I was there and I caught him/her talking to his/her paramour! Two words should spring to mind: *"Oh Crap!"*

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).

Here is an interesting case that illustrates this point. In *U.S. v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010)[1], a worker went onto his supervisor's computer and set up an Outlook rule to forward to him, the worker, a copy of any e-mail the supervisor received. The trial court found an "interception" under the wiretap act. The worker appealed, arguing this was a stored communications act case, not a wiretap act case. The appellate court affirmed.

The appellate court found that the Outlook instruction was probably enforced at the server end, so the e-mails were copied *before* supervisor got them; thus, to use a sports analogy, the football was caught in flight, hence an interception (wiretap act), not a fumble (stored communications act). Further, even if the Outlook rule was enforced at the client end (i.e., the supervisor's computer), Outlook sent the copy in the same second that the e-mail arrived. This is a contemporaneous interception even if the football technically arrived .0001 second before it was dropped.

This second point is analogous to the rule that the receiver must actually control the football before a drop is treated as a fumble, e.g., if the football bounces off the receiver's hands and the defender catches it, it's still an interception, not a fumble. If the rule was enforced at the client level, Szymuszkiewicz is like the football bouncing off the receiver's hands.

More recently, the principle was applied in the family law context in *Epstein v. Epstein*, 843 F.3d 1147, 1150 (7th Cir. 2016). There, the court held, "First, the judge misunderstood when an interception occurs. He assumed that the time Paula's email client received the forwarded emails was the moment of interception. Although this

[1] By the way, I have no idea how to pronounce Szymuszkiewicz.

interpretation of “interception” is understandable, we explained in *Szymuszkiewicz* that the interception of an email need not occur at the time the wrongdoer receives the email; in *Szymuszkiewicz* “[t]he copying at the server was the unlawful interception.” 622 F.3d at 704. Because Barry's case was dismissed on the pleadings, we do not know how Paula's auto-forwarding rule worked. For example, we cannot tell if a server immediately copied Barry's emails—at which point the interception would be complete—even though Paula's email client may not have received them until later.”

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:

1. 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.
2. *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.

3. *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.

4. *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.

5. *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."

6. *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 wife's attorney could not access the computer. 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."

7. *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.

8. *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.

9. *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.

10. *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.

11. *McDaniel v. McDaniel*, 2010 WL 2134146 (Tenn. Ct. App., May 27, 2010): In a divorce proceeding, a recording of the wife's telephone conversation with her son from a previous marriage was inadmissible because the recording was in violation of the state's wiretapping statute, which prohibited the intentional interception of telephone conversations. Although the son's father and stepmother had a recording device that recorded all telephone conversations for reasons related to their real estate rental business, and they may not have intended to record this particular conversation, they did intend to record all conversations. Furthermore, the conversation was recorded without the consent of the wife or her son.

12. *State v. Poling*, 160 Ohio Misc.2d 84, 938 N.E.2d 1118 (2010): Stored Communications Act (SCA), not Federal Wiretap Act, applied to actions of mother who obtained and provided to sheriff's office e-mails that defendant had sent to 16-year-old daughter, and thus e-mails

were not required to be suppressed pursuant to Act's exclusionary rule in prosecution of defendant for violation of protection order, where mother obtained the e-mails by copying them from family computer; Act applied to communications that had been intercepted in transit, not stored communications that had been copied. Even so, Mother did not violate Stored Communications Act (SCA) by obtaining and providing to sheriff's office e-mails that defendant had sent to 16-year-old daughter's messages, and thus SCA did not provide any grounds for excluding e-mails in prosecution of defendant for violating protection order, where mother copied the e-mails on the family computer without the use of her daughter's password.

13. *Forward v. Foschi*, 27 Misc.3d 1224(A), 911 N.Y.S.2d 692 (Table) (N.Y. Sup. 2010): E-mails that are protected by the attorney-client privilege did not lose protection because the husband had system passwords for administrative purposes.

14. *Lewton v. Divingnzzo*, 772 F. Supp.2d 1046 (D. Neb. 2011): Father of minor child and others brought action against mother, maternal grandfather, and others alleging violations of the Wiretap Act, and state law claims, in connection with secret recordings of plaintiffs' private conversations made with device hidden in minor child's toy for use in custody case. The parties cross-moved for summary judgment. Held: (1) mother and grandfather violated civil liability provision of Wiretap Act; (2) mother's attorney in custody case violated Wiretap Act; (3)

mother and grandfather were liable to each plaintiff for statutory damages in the amount of $10,000; (4) mother's attorney was not liable to pay statutory damages.

15. *Jennings v. Jennings*, 401 S.C. 1, 736 S.E.2d 242 (2012): Husband brought action against wife, wife's daughter-in-law, and private investigator hired by wife for violations of Stored Communications Act (SCA), stemming from accessing of husband's e-mails to his girlfriend by wife's daughter-in-law. Two justices held that an email cannot be in backup storage unless another copy of that email exists somewhere else. So, if an e-mail is on the server but it has not been downloaded to another computer, such that the server copy is the only copy existing, it is not a backup. (I find this a very strained reading of the statute.) Three concurring justices held that backup storage applies only to backup storage by the service provider. This reading effectively guts any protection offered by the SCA to e-mail stored by private citizens; the Ninth Circuit has expressly rejected this reading.

16. *Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. 2012): Even assuming that a cell phone was a facility for purposes of the Stored Communications Act (SCA), which prohibits accessing without authorization a facility through which an electronic communication service is provided and thereby obtaining access to an electronic communication while it is in electronic storage, the storage of text

messages and pictures on a cell phone did not fit within the SCA's definition of “electronic storage”; the text messages and pictures did not constitute information stored by an electronic communication service provider, and instead was information stored on the cell phone by its user. (This means that a husband or wife can get text messages off a spouse’s phone without running afoul of the SCA.)

17. *Rutter v. Rutter*, 316 Ga. App. 894, 730 S.E.2d 626 (2012): In divorce proceeding, husband moved to exclude any evidence that wife might have derived from several video surveillance devices that she had surreptitiously installed in the marital residence. The trial court denied the motion to exclude, and the husband appealed. Held: Wife was a resident of the marital home when she captured video footage of husband using video surveillance devices that she had surreptitiously installed in the marital residence, for purposes of determining whether subparagraph of wiretap statute, which expressly permitted one to conduct video surveillance of persons within the curtilage of one's own residence for certain purposes, authorized wife's clandestine videotaping as to render video footage admissible at trial, in divorce case; during the time that wife used the video surveillance devices, she kept clothes and other personal items at the marital residence, she paid a portion of the mortgage for that residence, she received some mail at that residence, and she spent some portion of every other day at the residence.

18. *People v. Janisch*, 966 N.E.2d 1034 (Ill. Ct. App. 5 Dist., 2012): Barbara Janisch and Michael Brumitt were in the midst of an ongoing dispute over child support. They had been divorced for over a decade. Barbara accessed Michael's personal data by entering his e-mail account by using his password without permission. On that basis, Barbara was convicted of computer tampering under Illinois' Computer Crime Prevention Law.

19. *Morgan v. Preston*, 2013 WL 5963563 (U.S. Dist. Ct., M.D. Tenn., Nov. 7, 2013): The husband brought an action against the wife under the Computer Fraud and Abuse Act. The court held he insufficiently alleged damages. He also sought relief under the Stored Communications Act. This failed, because "the overwhelming body of law supports the following conclusions: an individual's personal computer is not a "facility through which an electronic communication service is provided," an individual's personal computer does not provide "electronic storage" within the meaning of the SCA, and the SCA does not cover personal/family computers."

20. *Bruce v. McDonald*, 2014 WL 931522 (U.S. Dist. Ct., M.D. Ala., March 10, 2014): At issue in this case is Mr. McDonald's access to three electronic accounts: first, Mrs. Bruce's individual email account hosted by Yahoo.com; second, the joint email account the Bruces shared; and third, a joint account the Bruces shared on a website called "Adult Friend Finder" (or "AFF"). The Court held there was no

interception, BUT, "This is not to say that mere access, without some duplication device, could never amount to interception. If the Bruces could establish that Mr. McDonald had actually acquired even one message contemporaneously with its transmission, they might be able to show interception. That question is not before the court because there is simply no such evidence in this case. Rather, the evidence indicates that [Mr. McDonald] periodically accessed [the] accounts and printed e-mails [and other documents] after they had been delivered."

21. *Treon v. Treon*, 2015 WL 6964663 (U.S. Dist. Ct., S.D. Ala., Nov. 10, 2015): Husband who, without the Wife's knowledge or consent, secretly and surreptitiously recorded Wife's oral communications with third parties and intentionally intercepted, disclosed, or used the communications to bolster his position in the divorce proceedings, was guilty of wiretapping.

22. *Wildstein v. Davis*, 2016 WL 6591681 (Md. Ct. App., Nov. 4, 2016): The mother did not violate Section 7–302 of the Criminal Law Article by copying a family computer (a) to which she had unlimited access during the marriage, (b) on which she had her own administrator profile and (c) in the absence of any notice that her authority had been restricted.

23. *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016): Internet user's complaint, stating that the communications between him and a married woman were not stored on the married woman's computer hard drive, that

device for surreptitiously monitoring computer activity, installed by married woman's husband, intercepted his communications and routed them to its manufacturer's server facility, and that marketing materials for the device referenced its ability to monitor communications in "near real-time," sufficiently alleged that his communications were acquired contemporaneously with their transmission, as required to as required to state cause of action under Wiretap Act against manufacturer.

24. *Vista Marketing, LLC v. Burkett*, 812 F.3d 954 (11th Cir. 2016): Emails in ex-husband's corporate account that were opened by ex-wife, in an effort to prove to divorce court that ex-husband was lying about and hiding assets, but had not yet been opened by ex-husband were maintained in "electronic storage" by an online host operating as an electronic communication service (ECS), as required for Stored Communications Act (SCA) violation; host provided company's employees with ability to send and receive electronic communications, including emails, and before emails that ex-husband's corporate account received were opened, they were in electronic storage with host for purposes of providing backup protection of ex-husband's emails, at least until such time as he received and opened them on his computer.

25. *Papillon v. Jones*, 892 N.W.2d 763 (Iowa 2017): Evidence supported a finding that father knew he was violating the Interception of Communications Act, as required for an award of punitive damages

to mother, where he continued to use his illegal secret recordings of mother's conversations with others that he obtained through the use of a sound-activated device in their home in child custody litigation after mother's lawsuit put him on notice of the Act's prohibitions.

II. HOW TO OBTAIN ELECTRONIC EVIDENCE LEGALLY (AND THE CONSEQUENCES, i.e., MAKE IT ADMISSIBLE)

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 rule 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. In order to invoke Rule 26 be certain to send you spoliation letter early on.

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."

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, external storage drives, USB, 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.[2]

A. Formal Discovery Requests

1. 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, in an unpublished trial court opinion, the husband had given his old computer to the parties' daughter. The wife turned the computer over to Computer Forensics, Inc., and was able

[2] You may also wish to introduce into evidence electronic evidence that is readily available on social media: Facebook, Instagram, Snapchat, Twitter, etc. There are many fine resources on how to introduce this type of evidence that the attorney may garner him/herself from social media. *See,* Marcia Canavan and Eva Kolstad, *Does the Use of Social Media Evidence Matter in Family Law Litigation?* 15 Whittier J. Child & Fam. Advoc. 49 (2016); Family Advocate, Spring 2015 issue (devoted to social media evidence) https://www.americanbar.org/publications/youraba/2016/november-2016/how-to-get-social-media-evidence-admitted-to-court.html

to discover more assets than the husband had admitted. The assets were discoverable. Therefore, as part of your interrogatories you may want to ask if a party has gifted any old computers to anyone else, of if there even are older, unused computers to access.

2. 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.

3. When

Set time parameters for the creation of files. Generally, the request should not exceed the term of the marriage; for longer marriages a term of five (5) years should be sufficient. Send a spoliation letter to give advance notice so that data is not destroyed early on in the case.

4. 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.

5. 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.

6. 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.

* 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.

B. Obtaining Discovery From Social Networking Cites

Unfortunately, or rather fortunately, we are not the NSA: we can't just request information from Internet servers on the patters and practices, and content, of its users. Rather, formal discovery requests have to be made to Google for gmail, to Facebook, to hotmail.

Some case law on discovery of social networking information:

1. *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. (Note: Asking for information from MySpace is probably moot.)
2. *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."

3. *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."
4. *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."

C. When Formal Discovery Leaves You Wanting More: Computer Forensics, or How to Find the Stuff You Just *Know* They're Hiding[3]

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 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

[3] 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

computer yourself (or have your client do it), because the mere act of booting up changes the registry on about 400-600 Windows files.

D. 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.

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.

---

she find a pivotal piece of electronic evidence that will bring someone down. It's the smoking gun of the future.

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

1. *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.
2. *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."
3. *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.
4. *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.

5. *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.

6. *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.

7. *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. He was also potentially liable under the CFAA, but material issues of fact still existed regarding the $5,000 damages threshold. Under the wiretap act, the 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 <u>not</u> a violation of the FWA. Defendant's Motion for Summary Judgment is therefore granted as to Plaintiff's claims under the FWA.

8. *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.

9. *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]).

10. *Hui Lin Wei v. Cai Feng Chen*, 2014 WL 3843158 (N.J. Super., App. Div., Aug. 6, 2014): Audiotapes made by one spouse were not properly authenticated, N.J.R.E. 901, and the transcript was unreliable. Lin, the allegedly thieving employee who made the recordings, did not testify. Plaintiff's testimony about what Lin told her, concerning the creation of the recordings, was inadmissible hearsay.

11. *Ewing v. Ewing*, 333 Ga. App. 766, 777 S.E.2d 56 (2015): Wife was entitled, in a divorce action, to engage in discovery which might lead to admissible evidence of husband's alleged adultery, and, thus, the trial court did not abuse its discretion in denying husband's motion for a protective order to prohibit or limit wife's discovery requests with regard to private e-mails on husband's smartphone and to quash wife's subpoenas for the production of his smartphone phone records, regardless of the admissibility or inadmissibility of the content of husband's e-mails, including photographs and videos of another woman.

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.

What's important to remember is that federal law not only provides civil remedies, most states' law provide for criminal prosecution of these same acts. This is from a news report in 2010:

An Internet law designed to protect the stealing of trade secrets and identities is being used to levy a felony charge against a Michigan man after he logged onto his then-wife's Gmail account and found out she was cheating.

Leon Walker, 33, of Rochester Hills, Mich., is being charged with felony computer misuse, and faces up to five years in prison after logging into the email account of now ex-wife Clara Walker on a shared laptop using her password, the Detroit Free Press reports. He is facing a Feb. 7 trial. Leon and Clara Walker's divorce was finalized earlier this month, the Free Press reports.

Clara, who was married twice previously, was having an affair with her second husband, as Walker found in her email, according to the Free Press. The second husband had been arrested earlier for beating her in front of her young son from her first husband. Walker was worried about more domestic violence from husband No. 2, so he handed the e-mails over to the child's father, the Free Press reports. He promptly filed an emergency motion to obtain custody.

Leon Walker, a computer technician with Oakland County, was arrested in February 2009, after Clara Walker learned he had provided the emails to her first husband. "I was doing what I had to do," Leon Walker told the Free Press in a recent interview. He has been out on bond since shortly after his arrest. "We're talking about putting a child in danger."

Oakland County Prosecutor Jessica Cooper defended her decision to charge Walker, calling him a skilled "hacker" who downloaded the material in "a contentious way."

Electronic Privacy expert Frederick Lane told the Free Press that the case hinges in a legal grey area, and the fact that the laptop was shared may help Walker's cause.

About 45 percent of divorce cases involve some snooping -- and gathering -- of email, Facebook and other online material, Lane said. But he added that those are generally used by the warring parties for civil reasons -- not for criminal prosecution, the Free Press reports.

Some Law Review Articles on Electronic Evidence and Discovery

Christophe Brett Jaeger & Gregory D. Smith, *Computer and Electronic Snooping: Opportunities to Violate State and Federal Law*, 34 Am. J. Trial Advoc. 473 (2011)

Gaetano Ferro, Marcus Lawson, Sarah Murray, *Electronically Stored Information: What Matrimonial Lawyers and Computer Forensics Need to Know*, 23 J. Am. Acad. Matrim. Law. 1 (2010)

Laura W. Morgan, *The Individual's Right of Privacy in a Marriage*, 23 J. Am. Acad. Matrim. Law. 111 (2010)

Jennifer Mitchell, *Sex, Lies, and Spyware: Balancing the Right to Privacy Against the Right to Know in the Marital Relationship*, 9 J. L. & Fam. Stud. 171 (2007)

Laura W. Morgan, *Marital Cybertorts: The Limits of Privacy in the Family Computer*, 20 J. Am. Acad. Matrim. Law. 231 (2007)

Camille Calman, Note, *Spy vs. Spouse: Regulating Surveillance Software on Shared Marital Computers,* 105 Colum. L. Rev. 2097 (2005)

Richard C. Turkington, *Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort*, 82 Neb. L. Rev. 693 (2004)

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

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>

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

Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home,* 2 J. High Tech. L. 87 (2003)

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

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
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