Electronic Evidence and Discovery

Increasingly family law practitioners face the challenge of retrieving, authenticating, admitting and preserving electronic evidence. Since surfing the web always leaves a footprint searching a computer to find out where on the information highway a litigant has traveled may lead to the discovery of valuable financial records and/or hidden assets. Business records, e-mail, personal and business financial records, photographs, internet transactions, address books, videos and phone and text messages are often archived digitally and subject to discovery. In today's world most evidence can be converted into an electronic format even when it did not originate as a digital file. Electronic evidence is now a cornerstone of every family law case.

Retrieving the information is complicated by the fact that the digital data is stored in a myriad of places: desktops; laptops; servers; removable/external hard drives; data ports and other portable media systems); back up systems (in house and remote); PDA's; cellular phones; and online journals or blogs such as MySpace.com or FaceBook.com. Another problem for the practitioner is that electronic data can be manipulated, changed or altered.

Information stored on a computer is always in a constant state of fluctuation; every time a user accesses a file or installs a program, the

Jacqueline M. Valdespino, Esquire
Valdespino & Associates, PA
2641 Abaco Avenue
Miami, FL 33133

information changes. It is important to make sure that the evidence you may need, or want, is preserved. The first step is to send a preservation or anti-spoliation letter. This letter places everyone on notice that you will be requesting electronic data as part of your discovery. Once a preservation letter[1] is received, the other side cannot claim innocence if the electronic data sought is later unavailable. Send the letter early in the proceedings and be specific as to the place the data is located as well as the specific data you want preserved. Your letter should contain:

1. An introductory paragraph explaining that electronically stored data will be the source of a discovery request.
2. A paragraph detailing exactly where and what must be preserved.
3. A cautionary paragraph warning the recipient against destruction, either intentionally or inadvertently, of the evidence.

You may also consider seeking an *ex parte* temporary restraining order which would require the other party to preserve the evidence. In most jurisdictions you will need to allege that the issuance of the injunction is necessary because irreparable harm will result; if the electronic evidence is destroyed, altered or deleted, your client will not be able to obtain the data from any other source.

If you receive a preservation letter, or is a restraining order is entered against your client, be sure to immediately advise the client that all reasonable

[1] For a sample preservation letter, see, ABA Section of Family Law Advocate, Winter, 2007, Volume 29, No. 3, page 19.

steps to preserve the electronic data must be taken because failure to do so will result in sever penalties. Even continued use of the computer will result in the "destruction" of evidence. Once you receive a preservation letter consider filing a Motion for Protective Order, in particular if the request seeks to have your client produce confidential business records or privileged information. A protective order will provide clear directives regarding:

1. who the information can be disclosed to;
2. the manner and limitation on disclosure of evidence;
3. the use of the information, including if the data is to be returned and or destroyed at the conclusion of the case; and,
4. the process for maintaining the confidentiality of the information, including limitations on reproduction and disclosure of the information.

Often the parties and counsel can enter into reasonable stipulations regarding the preservation of the confidential business information. Before producing documents enter into a confidentiality agreement with the opposing party.

The new Federal Rules of Evidence require a "meet and confer" dialogue regarding electronic evidence and specifically recommend that the parties enter into agreements regarding: the form in which the data is to be produced; the protection of confidential or privileged data; and the preservation of discoverable evidence.

Before you actually send a request for evidence, get to know the "systems" you are seeking to obtain evidence from. You may request to review computerized and electronic records at the normal operating site under normal conditions. Your expert can attend with you and the staff responsible for the computer operations (use, maintenance, installation) should be made available as well. This is your opportunity to learn how the systems work, what type of information is available and where it is stored. Specifically it is imperative that you learn, at a minimum:

1. all places (on and off site) were information is stored;
2. number and type of computers (storage devises) used both on and off site;
3. storage capacity of each computer or hard drive;
4. number of servers and network connections to server;
5. the use of digital copiers hooked up to the network;
6. type of network used;
7. level and type of security, including the use of a firewall;
8. names, contact information and function of all people using, maintaining, upgrading etc., the computer systems, including any network administrator;
9. types of software used, (including any remote access software, operating systems, data management programs, encryption

software, presentation software, calendar and messaging software, etc.) including the version of each software used;

10. the use of passwords and the names and contact information for all people using passwords and/or having access to other's passwords;
11. type of back-up systems and frequency of use;
12. email use, both internal and external;
13. any written policies regarding computer use, including the use of email and world wide web;
14. the use of document management software that logs email communications;
15. the manner and system use to store data electronically (remember to ask if any electronic data is printed and if so where is it kept).

The scope of discovery will be defined in part by the information learned during this on site inspection. It is important to reduce the breadth of the request because unless you know how to limit the amount of information, you may receive more than you can adequately analyze and/or use.

Now that you have assured the preservation of the evidence, developed a discovery plan by having and on-site inspection and identifying exactly what it is you need for your case, and addressed the confidentiality and privilege issues, it is time to submit discovery requests. You should serve: a request for production of documents; interrogatories directed to the responding party's IT person; a

request for admissions (after you receive and analyze the documents produced); and a subpoena for deposition directed to the IT personnel (if after you receive a response to the interrogatories, a deposition is necessary). Any discovery requests should be specific, rather than broad. A request that is general should be met with an objection; following the on site meeting, requests should be precise and detailed and directed at obtaining only discoverable evidence.

You should hire a forensic expert to acquire/clone, the data. Acquiring and/or cloning a hard drive is different than copying a hard drive: a major difference is that in the cloning process no changes are made to the file directories or tables. The forensic expert can then compare the data received to the data on the cloned hard drive. The forensic expert can recover hidden files with renamed file extensions and deleted files (when you hit the delete button on your computer, it does not necessarily erase the data, it simply makes the space where the data once resided available). The forensic expert will conduct a technological, systematic inspection of the computer system and its contents for evidence using specialized software and technology. The expert will not only be able to locate the file, he will also be able to retrieve the data which may be the missing link necessary to help your client win the case.

Once you have the evidence, when you seek to introduce it at trial, you must authenticate it first. To authenticate e-mails, web site material, instant messaging or chat room evidence use the same standard and procedure used

for any other type of documentary evidence.[2] Under Federal Rule of Evidence, documents must be properly authenticated as a condition precedent to their admissibility "by evidence sufficient to support a finding that the matter in question is what its proponent claims."[3] This includes, "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[4] [5]

"E-mail communications may be authenticated as being from the purported author based on the affidavit of the recipient; the e-mail address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the e-mail communication that is being authenticated."[6] In *Fenje v. Feld*, the

---

[2] Gregory Joseph, *Internet and E-mail Evidence*, Practical Litigator, March 2002

[3] Fed.R.Evid. 901(a)

[4] Fed.R.Evid. 901(b)(4)

[5] E-mail is self-authenticating when the documents produced during discovery contain e-mail from the party's files that on its face purport to have been sent by the party. This is no different than the testimony to authenticate a photograph, replica or other demonstrative evidence; the admission of photographs lies within the discretion of the trial court. HTML codes may also present visual depictions of evidence sufficient to authenticate a document. "HTML codes are similar enough to photographs to apply the criteria for admission of photographs to the admission of HTML codes."

[6] Fenje v. Feld, 2003 WL 22922162 at 22 (N.D.III 2003)

defendant wanted to admit two e-mails into evidence.[7] The printed e-mails showed a source e-mail address that matched the plaintiff's letterhead; the content of the e-mails were consistent with other evidence; and a witness identified the e-mail communication as that between herself and the plaintiff.[8] Thus, the court found the e-mails to be properly authenticated and admitted them into evidence.[9]

The party objecting to the admission of the electronic evidence will object on hearsay grounds. Hearsay is "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[10] E-mail may become admissible under the party's own statement exception to the hearsay rule. Federal Rule of Evidence, Rule 803 (1) states that an exception to the hearsay rule is a "statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter."[11]

An e-mail may also be admissible as a statement against interest. A

---

[7] Id. at 23

[8] Id.

[9] Id.

[10] Fed. R.Evi. 801(c)

[11] All states have local rules of evidence that control the admission of evidence. Check your local rules and determine how they treat admissions by a party opponent.

statement against interest, under the Federal Rules, is:

> A statement which was at the time of its making so far contrary to the declarant's pecuniary or proprietary interest, or so far tended to subject the declarant to civil or criminal liability, or to render invalid a claim by the declarant against another, that a reasonable person in the declarant's position would not have made the statement unless believing it to be true.[12]

A proper hearsay objection by the opponent does not guarantee that electronic evidence will be excluded. In *Van Westrienen v. Americontinental Collection Corp.*, 94 F.Supp.2d 1087, 1109 (D. Or. 2000), "contents of the web site are not hearsay for purposes of this summary judgment motion" because the plaintiff "personally viewed the website and submitted an affidavit detailing specifically what he viewed." In contrast, in *U.S. v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000), cert denied 531 U.S. 973 (2000), web postings were found to be hearsay because they "were not statements made by declarants at trial, and they were being offered to prove the truth of the matter." The defendant tried to offer the web posting as a hearsay exception as a business record under Federal Rule of Evidence 803 (6). *Id.*

What happens when the electronic data is retrieved by a snooping spouse? In, *White v. White*, 781 A.2d 85, 87 (N.J. Super. Ct. Ch. Div. 2001), the wife hired an investigator to copy her husband's stored saved e-mails off the hard drive of the family computer, which revealed e-mails sent between the husband and the husband's girlfriend. *Id.* The husband's password was not used and a written

[12] Fed. R. Evi. 804 (b)(3)

report of the infidelity findings was issued. *Id.* The husband sought to suppress the evidence on grounds that by his wife accessing his e-mails without a password, she violated his common law right of privacy. *Id.* The court reasoned that the wife did not use the husband's password without authorization because although she did not often use the family computer, she had authority to do. *Id.* She accessed the files by searching through different directories. *Id.* Consequently, "where a party 'consents to another's access to its computer network, it cannot claim that such access was unauthorized.'" *Id.* Relying on *Del Presto v. Del Presto*[13], the court found that the husband's right of privacy was not invaded because when the wife searched through the files on the computer hard drive, it was no different then her searching through files in an unlocked filing cabinet. *Id.*

In *Bryne v. Byrne*, 650 N.Y.S.2d 499, 500 (N.Y. Sup. Ct. 1996) the issue was not who possessed the computer, but who had access to the computer's memory. In *Bryne*, the wife removed her husband's notebook computer from the marital residence and gave it to her attorney because she believed the memory in it contained important financial information. The husband used the laptop as part of his employment and for personal purposes since he allowed his children

[13] In *Del Presto v. Del Presto*, 235 A.2d 240, 245 (N.J. Super. Ct. 1967), the husband sought to suppress evidence of his infidelity, which the wife found in an office filing cabinet, which she had complete access to. The court held that the wife had a legitimate reason to be looking in the files and had a right to seize evidence she thought evidenced her husband's infidelity. *See, Strafford v. Strafford, supra.*

to do homework on it. Thus, the wife did not act illegally by removing the family computer from the residence. The court reasoned that "[t]he computer memory is akin to a file cabinet." The wife could have access to a file in a filing cabinet that was located in the marital residence. Consequently, she is able to have access to the family computer. The wife's expert was entitled to download the entire memory files contained in the computer, including those files that were password protected (the court noted that the process would be expedited if the husband provided the passwords, analogizing the process to an inventory of a safety deposit box). Once the documents were downloaded, the husband was to review the files and file a motion for a protective order as to anything that was subject to the attorney-client privilege. However, if the motion was not timely filed, all of the downloaded material was to be turned over to the wife's attorney. Once the downloading was complete, the notebook was then to be given back to the husband's employer.

In, *State v. Appleby*, 2002 Del Super. LEXIS 152 at 8, the court also reasoned that a hard drive is "an electronic file cabinet. It has an electronic lock opened by password acting like a key. It is organized by partitions, which are akin to drawers. Inside each partition are directories, which are somewhat analogous to folders stored inside an office filing cabinet." In *Appleby*, the defendant's ex-wife gave police a hard drive containing incriminating evidence against him. The hard drive was initially in the defendant's computer, then it was transferred to the ex-wife's computer. The hard drive stopped working and was left lying around in

the marital residence. During the marriage, each party had complete access to the other's computer and both had user profiles on the hard drive in question. The defendant left the marital home and weeks before she was served divorce papers, the wife turned the hard drive over to the authorities, which contained incriminating evidence against the defendant. The court held that the ex-wife had complete access to the hard drive because "after the husband and wife co-mingled their computer hardware, using it freely as each saw fit, its ownership and possession were joint." Assuming that the hard drive was the defendant's before the marriage, the hard drive would not become his again until the Family Court declared so. At the moment the wife turned the hard drive over to authorities, she controlled it no less then the defendant, "[i]n fact, she had more control over it than he because she possessed it." When the police opened the hard drive they did not look at anything that the ex-wife was not entitled to see herself. The court reasoned that the hard drive was like an unlocked filing cabinet because both the defendant and his ex-wife had passwords for the hard drive but they did not use them.

The electronic age presents special challenges for the practitioner in the collection, retention, presentation and admission of evidence. It is important that both the litigator and the client be educated on the issues. While the evidence sought to be admitted may seem different, all the traditional rules apply in determining whether or not it may properly be admitted. Since electronic data can rarely be completely deleted, it is almost always accessible. It is important

that the practitioner and the client determine the information that is potentially available, create a road map for obtaining the information and a plan for successfully admitting it into evidence.

Jacqueline M. Valdespino, Esquire
Valdespino & Associates, PA
2641 Abaco Avenue
Miami, FL 33133