Electronically Stored Information: What Matrimonial Lawyers and Computer Forensics Need to Know

By
Gaetano Ferro *
Marcus Lawson **
Sarah Murray ***

Electronically stored information ("ESI") is "information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software."[1] ESI includes emails, voicemails, instant messages, text messages, documents and spreadsheets, file fragments, digital images, and video. There has been a major shift from conventional media to electronic digital media. "It is estimated that ESI has become exponentially greater in volume than that of conventional media."[2]

The use of electronically stored information in matrimonial cases often involves challenging issues. The lawyer involved in such a case needs to become sophisticated as to how computers maintain information. He or she needs to acquire an understanding of both the rudimentary and analytical. At the same

* Matrimonial lawyer in private practice, New Canaan, CT; past president of the American Academy of Matrimonial Lawyers; past Editor-in Chief of the Journal of the American Academy of Matrimonial Lawyers.

** Marcus Lawson, JD, is a former federal agent who specialized in computer crime investigations before founding Global CompuSearch LLC, a computer forensics and electronic discovery firm headquartered in Spokane Washington with offices in Portland, OR and Palm Springs, CA.

*** Matrimonial lawyer in private practice, New Canaan, CT. J.D., University of Connecticut School of Law; B.A., College of the Holy Cross.

1 *See*, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, Kenneth Withers, 4 NW. J. of Tech. & Intell. Prop. 171, *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3. See also, FED. R. CIV. P. (hereafter "FRCP") § 34.

2 Barbara Curchill, Linda Clark, Jonathan Rosenoer, & Fritz von Bulow, *The Impact of Electronically Stored Information on Corporate Legal and Compliance Management: An IBM Point of View,* IBM Corporation, *available at* http://www.cyberlaw.com/images/fss_the_impact_of_eletronically.pdf.

time, the lawyer involved in a case with significant ESI needs to be mindful of criminal and ethical rules. In addition, ESI may prove to be worthless unless the lawyer considers evidentiary problems in advance.

This article will address and give guidance in a number of areas. Part I provides an introduction to electronically stored information. In particular, it addresses why it might be beneficial to pursue electronically stored information in matrimonial cases, how electronically stored information may be found, and the potential pitfalls and ethical violations a matrimonial lawyer should avoid when dealing with informally obtained electronically stored information. Part II delves into the evidentiary issues every lawyer must consider when gathering electronically stored information and using it in his or her case. In Part III, the roles that a computer forensic can play in aiding a matrimonial lawyer to gather and digest electronically stored information are explored. Types of electronically stored information, extending from the more commonly known examples, such as emails and text messages, to the less obvious examples, such as metadata, are outlined in Part IV. Computers are not the only places where these various types of electronically stored information may be found, as is pointed out in Part V. Parts VI and VII of the article examine the role of the computer forensic as an investigator whose findings can become critical evidence in some cases. Lastly, the article closes in Part VIII with a focus on issues arising out of electronic evidence in cases in which there are child pornography or drug abuse allegations.

I. An Introduction to Electronically Stored Information

A. *Why Seek Out Electronically Stored Information*

While seeking out electronically stored information may be time-consuming and expensive, there are good, sometimes compelling, reasons to try to obtain it. It may yield the only evidence on an issue. It may yield information of double importance. In addition to providing proof of adultery, where relevant, or financial misconduct, the same electronically stored information may impeach the credibility of a party, which is often the most impor-

tant consideration to a trial court.[3] The importance of electronically stored information as a source of impeachment information cannot be overstated.

B. *Finding Electronically Stored Information*

There are many ways to obtain ESI. A main source is the client. If the client has the right to access the other spouse's laptop, desktop, iPhone, blackberry or other data storage device, the client should be instructed to make that device available to the computer forensic expert.[4] If the client has already made copies of e-mails, electronic files, and the like, the attorney needs to determine whether the copies will be admissible.[5] If the attorney concludes that the discovery will not be admissible,[6] he or she should consider seeking the same electronic evidence through discovery.

C. *Potential Pitfalls of Informally-Obtained Electronic Evidence*

In a family law case the client can be his or her own best advocate or worst enemy. How he or she handles the gathering of electronically stored data can significantly help or hurt the case. Part of the lawyer's job is to guide the client, and perhaps the client's business associates or employees, through the process of obtaining and handling electronically stored information in a proper manner. Understanding and explaining the potential stumbling blocks of electronic discovery, as defined by federal

---

3 *See* Stone, *Tell-All PCs and Phones Transforming Divorce*, NEW YORK TIMES, September 15, 2007.

4 Before the attorney does so, he or she needs to establish that the client's access to the device is legal. *See infra*, part IV.

5 While the general rule is that illegally-obtained evidence is admissible in a civil action, some federal and state statutes preclude the admission of illegally-obtained electronic evidence. *See infra*, part IV, pp. 5-6. Courts have, however, used consent to reject efforts to suppress electronic information. For example, in *White v. White*, 781 A.2d 85 (N.J. Super. 2001), password-protected e-mails were obtained without a password from the hard drive of the family computer. Because the wife had used the computer with the husband's permission, the court found that she had authorization to access password-protected files. Similarly, in *Bryne v. Bryne*, 650 N.Y.S.2d 499 (N.Y. Supr. Ct. 1996), the court did not suppress password-protected files in a family computer.

6 *See*, FRCP 26(a)(1)(B).

and state law, is a critical aspect of any matrimonial lawyer's role in preparing a client's case.

Federal law, as well as the laws of some states, provides for criminal and civil liability in the event that a person interferes with electronic communications that are en route. The Electronic Communications Privacy Act[7] makes it unlawful for a person to intentionally intercept any wire,[8] oral,[9] or electronic communication,[10] or to use or disclose any wire, oral, or electronic communication that has been intentionally intercepted.[11] The criminal penalty for any such action is a fine or imprisonment of not more than five years, or both.[12] The Act also provides criminal penalties for those who send, manufacture, assemble, possess, sell, or place an advertisement for any devices that are used for the "surreptitious interception of wire, oral, or electronic communications."[13]

---

7 18 U.S.C. § 2510 et seq.

8 A wire communication is:

> [A]ny aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce. 18 U.S.C. § 2510(1).

9 An oral communication is "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(2).

10 Under the statute, an electronic communication is:

> [A]ny 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 that affects interstate or foreign commerce but does not include–(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device. . .; (D) electronic funds transfer information stored by a financial institution. 18 U.S.C. § 2510(12).

11 18 U.S.C. § 2511(1).

12 18 U.S.C. § 2511(4)(a).

13 18 U.S.C. § 2512(1).

The Act also permits civil action against a person or entity who violates it.[14] The person whose electronic communications were unlawfully intercepted may seek relief from the court in the form of "1) such preliminary and other equitable or declaratory relief as may be appropriate; 2) damages. . .and punitive damages in appropriate cases; 3) a reasonable attorney's fee and other litigation costs reasonably incurred."[15] In most cases, "the court may assess as damages whichever is the greater of (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000."[16] The statute of limitations on a civil claim under the Electronic Communications Privacy Act is "two years after the date upon which the claimant first has a reasonable opportunity to discover the violation."[17]

Notwithstanding the prohibition against intercepting wire, oral, or electronic communications, it is permissible for a person not acting under the color of law to intercept a wire, oral, or electronic communication so long as the person is either a party to the communication or one of the parties to the communication gives prior consent to have the communication intercepted.[18] The purpose of the interception, however, cannot be the commission of a criminal or tortious offense that violates the U.S. Constitution or any state or federal laws.[19] While it seems unlikely that a person involved in a contested divorce or custody case would consent to having any wire, oral, or electronic communication intercepted, consent is one way to avoid liability for intercepting communications between a spouse or ex-spouse and a third party.[20]

Attorneys must exercise caution when deciding whether to disclose or use electronic data received from the client. The attorney must inquire into how the client obtained the information in order to determine compliance with the law. The attorney

---

14 *See* 18 U.S.C. § 2520.

15 18 U.S.C. § 2520(b).

16 18 U.S.C. § 2520(c)(2).

17 18 U.S.C. § 2520(e).

18 18 U.S.C. § 2511(2)(d).

19 *Id.*

20 *See supra* note 5.

should not attempt to use data obtained in violation of the Act because anyone who intentionally discloses or uses, or endeavors to disclose or use, wire, oral, or electronic information that has been intercepted, and who knows or has reason to know that the information has been intercepted, is subject to the same penalties as the person who intercepts the information.[21]

Matrimonial lawyers should be aware of the provision of the Electronic Communications Privacy Act stating that:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.[22]

In other words, a lawyer whose client surreptitiously intercepts an electronic communication in violation of this Act must be concerned about the client's exposure to potential criminal and civil liability, and is precluded from entering this evidence, no matter how relevant, before the court.

The Electronic Communications Privacy Act only applies to electronic communications that have been intercepted while being transmitted from the sender to the recipient.[23] The Fifth Circuit has held that "where a transmission has already occurred, merely reading a copy of the message is not an 'interception.'"[24] Reading an email that has already been transmitted to or from the e-mail account does not violate the Act, but doing so may very well violate other law.

Liability for improper access to electronically stored data exists under the Stored Communications Act.[25] Under this federal law, that a person "(1) intentionally accesses without authoriza-

---

21 18 U.S.C. § 2511(1)(c)-(d).

22 18 U.S.C. § 2515.

23 *See* 18 U.S.C. § 2510 et seq. *See also* Stephen Harhai, *Discovery and Admissibility of Electronic Evidence,* Divorce Research Center, http://www.divorcesource.com/research/dl/discovery/01sep157.shtml.

24 *Steve Jackson Games, Inc. v. U.S. Dept. of Justice*, 36 F.3d 457 (5th Cir. 1994).

25 18 U.S.C.A. § 2701 et seq. The Stored Communications Act also deals with governmental use of electronically stored information, which is beyond the scope of this article. *Id.*

tion a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system, "[26] is a punishable offense. This statute pertains to improper access of Internet- based email services, such as Gmail, Yahoo, and Hotmail,[27] and is meant to protect the information found in such services. Since these Internet-based email services have become increasingly popular as people's primary Internet service providers, they have become the subject of controversy in matrimonial cases.

Punishment under this statute varies depending upon the purpose for which the electronic storage facility has been improperly accessed.[28] If the electronic storage facility has been accessed "for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State,"[29] then the person who committed the offense can, for a first offense, be fined or imprisoned for not more than 5 years, or both.[30] For any subsequent offense, the penalty is a fine or imprisonment for not more than 10 years, or both.[31] If, however, an electronic storage facility was improperly accessed for purposes other than those listed above, the punishment is a fine or imprisonment for not more than 1 year, or both, for the first offense.[32] Subsequent offenses are punishable by a fine, imprisonment for not more than 5 years, or both.[33] Exceptions to the statute exist, including exceptions for any person or entity providing a wire or electronic communications service or for users of a wire or electronic service "with respect to a communication of or intended for that user."[34]

The Stored Communications Act prohibits "a person or entity providing an electronic communication service to the public"

26 18 U.S.C.A. § 2701(a).
27 *See* Harhai, *supra* note 23.
28 *See* 18 U.S.C.A. § 2701(b).
29 18 U.S.C.A. § 2701(b)(1).
30 18 U.S.C.A. § 2701(b)(1)(A).
31 18 U.S.C.A. § 2701(b)(1)(B).
32 18 U.S.C.A. § 2701(b)(2)(A).
33 18 U.S.C.A. § 2701(b)(2)(B).
34 18 U.S.C.A. § 2701(c)(1)-(2).

from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[35] The statute also provides that:

> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service–
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
>
> (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.[36]

Thus, not only does the Act protect electronic information that has been accessed without authorization, but also it protects information stored with a third party provider from being revealed by that third party provider.

The statute distinguishes between an "electronic communications service" and a "remote computing service." An electronic communications service, as defined in the Electronic Communications Privacy Act and as used in the Stored Communications Act, is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[37] A remote computing service, on the other hand, is legally defined as the "provision to the public of computer storage or processing services by means of an electronic communications system."[38] A provider of a remote computing service is permitted to release the contents of a communication to the addressee or intended recipient (or the recipient's agent).[39] The remote computing service provider may also release the contents of a communication

---

35 18 U.S.C.A. § 2702(a)(1).

36 18 U.S.C.A. § 2702(a)(2)-(3).

37 18 U.S.C.A. § 2510(15).

38 18 U.S.C.A. § 2711(2).

39 18 U.S.C.A. § 2702(b)(1).

to a third party with the lawful consent of either the originator, the addressee, the intended recipient, or the *subscriber* of the service.[40] The statute treats differently the provider of an electronic communications service in that such a provider may not disclose communications to the subscriber of the service.[41]

The Stored Communications Act only provides protection for electronically stored information that has been accessed by a person or entity not authorized to access the information, or by a person or entity that has exceeded authorization in order to access the information. The statute, however, does not provide that all emails and other electronically stored information found in Internet-based services are not discoverable.

Formal discovery is often the only way to obtain ESI. Given the way the Federal Rules of Civil Procedure are structured, a lawyer representing a client in a divorce or dissolution of marriage action in a jurisdiction with rules similar to the Federal Rules should consider formally requesting ESI.

Federal Rule 16(b) was amended in 2006 and provides that "disclosure or discovery of electronically stored information" may be addressed as part of the scheduling order. Rule 26(a)(1)(B) provides that ". . . a party must . . . provide to other parties . . . a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment." Rule 26 was also amended in 2006 to replace reference to "data compilations" with "electronically stored information."[42] Rules 33, 34, 37, and 45 were amended in 2006 to make express reference to electronically stored information.

Thus, any issue about whether discovery extends to electronically stored information has been affirmatively decided by the 2006 rules. The real issue about electronic evidence is not

---

40 18 U.S.C.A. § 2702(b)(3). Issues will arise in cases where the subscriber to a service is an employer.

41 *See* 18 U.S.C.A. § 2702(b)(3).

42 *See* R. Mayer, *Electronically Stored Information and the Amended Federal Rules of Civil Procedure*, ABA Section of Litigation, TRIAL PRACTICE JOURNAL, Vol. 21, No. 3, p.2.

whether it is discoverable. The issue may be whether it is affordable. Federal Rule 26(b)(2)(B) provides:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.[43]

Two recent decisions indicate that courts will not necessarily order discovery of electronically stored information, *carte blanche*. In *Kay Beer Distributing v. Energy Brands*,[44] a suit arising out of a dealership agreement, the court restricted the plaintiff's discovery where the defendant's electronic search generated five DVDs with 17 gigabytes of data, comprising 56,547 documents and hundreds of thousands of pages. The court ordered that only documents which included "Kay Beer" or variants of that name be produced because "[t]he mere possibility of locating some needle in the haystack" did not warrant the expense to be incurred in reviewing the DVDs.

In *Kilpatrick v. Breg*,[45] a products liability claim against the manufacturer of a medical device, shortly before trial it was contended that the defendant knew facts of which he had previously denied knowledge. Instead of allowing full-scale discovery on the eve of trial, the court allowed the plaintiff to employ an expert to use a limited methodology, i.e., limited search terms ap-

---

43 FRCP 26 (b)(2)(c) provides that the court may limit discovery if it determines that:

> (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
>
> (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
>
> (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

44 2009 U.S.Dist.Lexis 1773 (E.D.Wisc. Feb. 20, 2009).

45 2009 U.S. Dist. Lexis 3092 (S.D.Fl. Jan. 9, 2009).

plied to a designated number of backup tapes, to determine whether documents had been withheld.

To decide whether to pursue electronic discovery, the lawyer should do a cost-benefit analysis. As the amount of money in dispute in the case increases, the analysis will tilt in favor of electronic discovery. Where the issue cannot be quantified in money, e.g., child custody, it is not as easily subject to a cost-benefit analysis. The lawyer should also consider that pursuing electronic discovery may add to the emotional overlay of the case.[46]

The cost of electronic discovery, while hard to quantify, should not be understated. While forensic analysis of a computer used only for personal matters would be inexpensive, such a computer is a rara avis. Moreover, requests for electronic discovery are usually met with objections and reciprocal requests, which will escalate the costs involved. One computer expert begets an opposing computer expert.[47]

For one who is willing and able to pay for it, the potential objects of electronic discovery can be voluminous. If electronic evidence is to be pursued, there must be a game plan which takes into account a number of considerations:

1. Will the other side ask for similar information in response and, if so, which litigant is likely to suffer more damage from the electronic discovery?
2. Will the other side seek and receive an award of fees and will the electronic discovery increase the likelihood or amount of that award?

---

46 The American Academy of Matrimonial Lawyers' Bounds of Advocacy suggests that reducing the emotional level of a family dispute is an appropriate goal for the lawyer. *See* Goal 1.3 ("An attorney should refuse to assist in vindictive conduct and should strive to lower the emotional level of a family dispute by treating all other participants with respect.") *See also* Goal 7.1 ("An attorney should strive to lower the emotional level of marital disputes by treating counsel and the parties with respect.")

47 Two legal magazine posts have recently suggested that the rising costs of electronic discovery have stemmed what would otherwise have been a wave of litigation. K. Sloan, *For Litigators, a Different Kind of Recession*, The National Law Journal, August 18, 2009; D. Weiss, *E-Discovery Fears May Explain Why Recession Didn't Spur Litigation*, ABA Journal Law News Now, August 18, 2009.

3. Should the electronic discovery wait until after the other side has been deposed so that the value of the electronic evidence as impeachment is enhanced?[48]
4. Should the party be asked for the electronically stored information before it is subpoenaed from third parties?

Deferring electronic discovery is risky. Once a formal request for electronically stored information is made, the other side will have to preserve it or risk sanctions for spoliation.[49] However, Federal Rule 37(f) provides that "[A]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

It has been suggested that a preservation letter be sent out early in the case.[50] Doing so may be "belt and suspenders" because the duty to preserve evidence arises when a party has notice that evidence is relevant to litigation or should know it is relevant to future litigation.[51] Nonetheless, a preservation letter will put the opposing party on notice that electronic evidence may be relevant and will make a claim of lack of notice more difficult to maintain.

Of course, once a preservation letter is sent, time can be taken to carefully craft, with the assistance of the computer forensic expert, a request for production which does not ask for too much information and results in neither an unwieldy mass of data nor a reciprocal onerous request.

---

48 The general rule appears to be that a party has a duty to preserve evidence known to be relevant to present or future litigation. *See*, *e.g.*, *Cilvestri v. General Motors Corp*., 271 F.3d 583, 591 (4th Cir. 2001). Serving a document request will make it harder to contend that the requested evidence was not known to be relevant. "Once a court has concluded that a party was under an obligation to preserve the evidence that it destroyed, it must then consider whether the evidence was intentionally destroyed, and the likely contents of that evidence. The determination of an appropriate sanction for spoliation, if any, is assessed on a case-by-case basis." *Fujitsu Ltd. v. Federal Express Corp*., 247 F.3d 423, 435 (2d Cir. 2001) (internal citation omitted).

49 *See* discussion *infra* pp. 13-16.

50 C. Ball, *Meeting the Challenge: E-Mail in Civil Discovery*, Five on Forensics, *available at* www.craigball.com/cf.pdf.

51 *Zubalake v. UBS Warburg*, 220 FRD 212 (S.D.N.Y. 2003).

D. *Ethical Violations*

Lawyers must avoid either inadvertent or purposeful spoliation of electronic data in order to remain within the boundaries of professional ethics. Besides reviewing the ethical guidelines of the state in which the matrimonial lawyer practices, the family lawyer should also consult the Bounds of Advocacy put forth by the American Academy of Matrimonial Lawyers for standards of practice for dealing with electronic discovery.[52] The Bounds of Advocacy are not binding upon family law attorneys, but provide aspirational guidelines for the practice of matrimonial law.[53]

The Academy recommends that "[a]n attorney should not condone, assist, or encourage a client to transfer, hide, dissipate, or move assets to improperly defeat a spouse's claim."[54] The comments explain that a matrimonial lawyer's duty to discourage fraud encompasses a duty to protect data relating to assets: "The client must also be advised not to conceal data about property or fail to furnish relevant documents."[55]

The lawyer who assists or condones a client who spoils electronic data not only violates ethical rules, but also exposes his or her client to sanctions in the event that this spoliation of data is discovered.[56] A lawyer's duty to preserve electronically stored

---

52 *See* American Academy of Matrimonial Lawyers, Bounds of Advocacy: Professional Cooperation and the Administration of Justice, http://www.aaml.org/go/library/publications /bounds-of-advocacy/.

53 AAML Bounds of Advocacy Preliminary Statement.

54 AAML Bounds of Advocacy 5.1.

55 *Id*., comment.

56 *See Kucala Enters., Ltd. v. Auto Wax Co., Inc.* 56 Fed. R. Serv. 3d 487 (N.D. Ill. 2003) (plaintiff purchased and used disk-wiping software called "Evidence Eliminator" the night before his computer was to be turned over to the defendant for inspection). *See also Carlucci v. Piper Aircraft Corp.* 102 F.R.D. 472 (S.D. Fla. 1984) (entry of default judgment against a party that willfully destroyed electronic discovery); *Century ML-Cable Corp. v. Carrillo* 43 F.Supp.2d 176 (D.P.R. 1998) (default judgment entered against a party who willfully destroyed business records and a laptop computer in violation of a temporary restraining order); *Wm. T. Thompson Co. v. Gen. Nutrition Corp., Inc.* 593 F. Supp. 1443 (C.D. Cal. 1984) (defendant given money sanctions and a default judgment after defendant violated a protective order by destroying documents). FED. R. CIV. P.37(a)(3) specifically authorizes federal judges to impose sanctions on a party for failing to disclose information required by Rule 26(a). Though this rule states that a judge may not impose sanctions, absent exceptional circumstances, for "failing to provide electronically stored informa-

information for discovery purposes means that the lawyer cannot advise a client to wipe data or condone a client's spoliation of electronic information prior to and throughout divorce and custody litigation.

Situations may arise in which a client has not preserved electronic data, such as emails, and, as a result, the electronically stored information is no longer available, despite efforts by forensic experts to retrieve it.[57] In these instances, the offending party still may be sanctioned, even if there is no finding of bad faith or intentional destruction of data.[58] Therefore, it is important for the matrimonial lawyer to assess the need for electronic discovery early on in a case in order to advise the client properly about preserving electronic data.

Complex cases in which electronic discovery issues are raised often involve an immense amount of discovery, which in turn creates the possibility that privileged documents may inadvertently be provided to the other side. When hard drives are copied, for example, there is no differentiation between data that is privileged, data that is irrelevant or not responsive to discovery requests, and data that is relevant and discoverable. Allowing the other side access to all of the information found on a hard drive without prior review is almost a guarantee that there will be an inadvertent disclosure. Lawyers need to take steps to review the electronic discovery before it is turned over in order to prevent privileged communications from being disclosed.

---

tion lost as a result of the routine, good faith operation of an electronic information system," a person who destroys evidence in bad faith will most likely be sanctioned. FED. R. CIV. P.37(e). Matrimonial lawyers should be aware of state laws that track this federal rule.

57 *See* discussion regarding the method for retrieving data *infra* pp. 24-26; 34-39.

58 *See MasterCard International, Inc. v. Moulton* 2004 WL 1393992 (S.D.N.Y. 2004) (no emails preserved until 5 months after the lawsuit was filed; court found there was no bad faith but the defendant's actions were grossly negligent, and so civil sanctions were granted). *See also MPCT Solutions Corp. v. Methe* 1999 WL 495115 (N.D. Ill., July 2, 1999) (no finding of intentional violation of court's preservation of evidence order in order for sanctions to be issued). Though these are not family law cases, judges in many jurisdictions have the discretion to impose similar sanctions for discovery violations in family cases.

Most jurisdictions have laws, court rules, or ethical guidelines governing what a lawyer should do in the event that he or she receives an inadvertent disclosure. The American Academy of Matrimonial Lawyers counsels that "[a]n attorney who receives materials that appear to be confidential should refrain from reviewing the materials and return them to the sender, as soon as it becomes clear they were inadvertently sent to the receiving lawyer."[59] Some jurisdictions adhere to this approach, whereas others take the opposite approach and deem the inadvertent disclosure of privileged or confidential materials to be a waiver of privilege or confidentiality.[60] Matrimonial lawyers have a duty, as all lawyers do, to comply with the guidelines of the jurisdiction in which they practice when dealing with inadvertent disclosures of electronic data.

II. Evidentiary Considerations

An expert is needed when an intelligent evaluation of facts is difficult or impossible without the application of scientific, technical, or other specialized knowledge.[61] Even the most basic electronic evidence may require an expert to explain it.

> Whether ESI [electronically-stored information] is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI *relevant* as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401 is it *authentic* as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it *hearsay* as defined by Rule 801, and if so, is it covered by an applicable exception (Rules

---

59 AAML Bounds of Advocacy 7.6.

60 *See, e.g., Hopson v. Mayor and City Council of Baltimore* 232 F.R.D. 228 (D. Md. 2005) (court encouraged parties to enter into a claw back agreement and framed it as a court order, but "such an order would not relieve the parties of the duty to perform a reasonably thorough privilege review, as time and resources allow, nor would it act as an iron clad protection against a 'privilege waiver' claim being raised in another jurisdiction, particularly one that takes a strict view of waiver.")

61 *See* FED. R. EVID. 701.

> 803, 804, and 807); (4) is the form of the ESI that is being offered as evidence an *original* or *duplicate* under the original writing rule or, if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001 - 1008); and (5) is the probative value of the ESI substantially outweighed by the danger of *unfair prejudice* or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.[62]

Whether evidence is relevant, hearsay, or whether it carries the danger of unfair prejudice poses no considerations unique to electronically-stored information. Authentication and best evidence, however, warrant special analysis.

Authentication is a basic requirement for the admissibility of evidence.[63] Where the evidence is produced by a computer, "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result,"[64] should suffice to authenticate computer evidence. A mere printout will not suffice.[65]

That a computer contains a particular piece of information in and of itself may not be probative of anything. If an expert is able to testify as to who caused that information to be placed upon the computer and when the information was placed on the computer, it may be probative of something. Similarly, while admitting an e-mail into evidence is often routine, a challenge to its authenticity may cause one to wish that an expert had been hired. It is "a fairly simple matter for a hacker to spoof (falsify) the identification of all but the final delivery server [on an e-mail.] Accordingly, where the origin or origination date of an e-

---

62 *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 538 (D.Md. 2007) (Grimm, C.M.J) (footnote omitted) (emphasis in original).

63 *See* FED. R. EVID. 901(b).

64 FED. R. EVID. 901(b)(9).

65 *See, e.g., Toytrackerz LLC v. Koehler*, 2009 WL 2591329 (D. Kan.) (website printout not admitted into evidence because it was not authenticated. "In order to satisfy the requirement of Fed.R.Evid. 901 . . . they must provide a statement or affidavit from someone with personal knowledge of the contents of the website 'sufficient to support a finding that the matter in question is what its proponent claims. . . . While Plaintiffs' Application does refer to and identify the exhibit as the website maintained by Defendant Koehler, it fails to identify who retrieved the website printout, when and how the pages were printed, or on what basis the printouts accurately reflect the contents of the website on a certain date."). *See*, *generally*, ELECTRONIC EVIDENCE AND DISCOVERY: WHAT EVERY LAWYER SHOULD KNOW NOW, pp. 143-44 (A.B.A. 2d Ed. 2009).

mail is suspect, the actual route of the message may need to be validated at each server along its path."[66] The header on an e-mail with the "From" e-mail address does not prove the existence of the sender any more than a return address on an envelope proves who sent it.[67]

Nonetheless, e-mails have been authenticated through circumstantial evidence about their contents, substance, internal patterns or other distinctive characteristics.[68] Similarly, instant messages have been authenticated through circumstantial evidence.[69] One can only surmise that the courts which allowed such authentication were unaware of how easy it is to change the sender's e-mail address to make it appear that it was sent by someone other than the actual sender.[70]

That evidence is authenticated is not sufficient to have it admitted. The best evidence rule applies. Rule 1002 of the Federal Rules of Evidence provides that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."[71] An "electronic recording" is a writing or a recording.[72] Rule 1003 provides that a duplicate is admissible unless there is a "genuine question as to the authen-

---

66 Ball, *supra* note 50.

67 Harhai, *supra* note 23, at 2.

68 *U.S. v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000), *aff'd* 533 U.S. 940, 121 S.Ct. 2573 (2001) (trial court did not err in admitting e-mail into evidence where it had been authenticated by containing defendant's e-mail address as sender, the content of the e-mail indicated that the author knew the details of the defendant's conduct, and the e-mail referred to the defendant by his nickname); *United States v. Safavian*, 435 F.Supp.2d 36 (D.D.C. 2006) (e-mails authenticated because of distinctive characteristics including e-mail addresses, the defendant's name, and the contents which contain discussions relating to the defendant's work).

69 *People v. Pierre*, 41 A.D.3d 289, 838 N.Y.S.2d 546 (N.Y.A.D. 2007) (instant message properly authenticated although witness did not save or print it and no technical evidence, where witness testified to defendant's screen name, another witness testified she sent instant message to same screen name and received a reply which made no sense unless sent by defendant.)

70 The common law prohibition against examining about the contents of a document not in evidence was not discussed in the cases cited in footnotes 64 and 65.

71 FED. R. EVID 1002.

72 "'Writings' and 'recordings' consist or letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating,

ticity of the original."[73] The litigator attempting to offer a document printed from a computer need not, however, go round in circles.[74] "If data are stored in a computer or similar device, any printout or other output readable by sight, *shown to reflect the data accurately*, is an 'original.'"[75] While a lay person may often be able to give such testimony, in many cases only a computer forensic expert may opine that a printout reflects the data in a computer accurately. Nonetheless, a commentator has stated that the best evidence rule will rarely present a problem for the admissibility of electronically-stored information.[76]

> In determining who may offer opinion testimony, courts usually defer to anyone who knows more than the average person about the area of knowledge at issue.[77] Thus, if scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the fact of the case.[78]

"Nothing . . . is intended [by the 2000 Amendments to Rule 702] to suggest that experience alone - or experience in conjunction with other knowledge, skill, training or education - may not

---

photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation." FED. R. EVID 1001(1).

73 FED. R. EVID 1003.

74 *See* B. Preston, *Will It Go Round In Circles*, from Music Is My Life (A & M Records, 1972).

75 FED. R. EVID 1001(3) (emphasis supplied).

76 Jablon, *God Mail: Authentication and Admissibility of Electronic Mail in Federal Courts*, 34 AM. CRIM. L. R. 1387, 1401 (1997).

77 That courts do so is consistent with areas in which lay persons are permitted to give expert opinions. For example, an owner of a business may testify to its value without being qualified as an accountant or an appraiser. *See, e.g., Lightning Lube, Inc. v. Witco Corp.* 5 F.3d 1153 (3d Cir. 1993). Similarly, courts have let lay witnesses testify that a substance appeared to be a narcotic. *See, e.g., United States v. Westbrook*, 896 F.2d 330 (8th Cir. 1990). The rationale for both is knowledge: the owner of a business has knowledge of the business and its day to day affairs; the lay witnesses, being heavy amphetamine users, had familiarity with the substance.

78 FED. R. EVID 702.

provide a sufficient foundation for expert testimony."[79] Nonetheless, as with all experts, the better the expert, the more persuasive the testimony.

Finding a computer forensic expert is no different than finding any other expert and similar approaches should be used. Other practitioners should be consulted. Professional associations may be of use.[80] While the best computer forensics are not necessarily the best authors, many can be found from their writings.[81]

Many experienced computer forensic experts come from law enforcement backgrounds, including the Department of Defense, the Internal Revenue Service, the Federal Bureau of Investigation, and state and municipal police departments.

Certifications may illuminate a computer forensic expert's qualifications. Those which stem from examination and experience, study or training are meaningful.[82] Send-the-check certifications are suspect.

The potential forensic expert should be questioned about evidence acquisition, handling, and storage procedures, and documentation of those procedures. If the attorney is computer-sophisticated, the potential expert should be asked about the forensic software to be employed. The expert's previous experience in matters involving similar issues, previous court experience and references should also be the subject of inquiry.

---

79 FED. R. EVID 702 advisory committee's note 2000. Of course, if the witness is relying solely upon experience, the witness should "explain how the experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts." *Id.*

80 Organizations include: The International Society of Forensic Computer Examiners which provides the Certified Computer Examiner (CCE) certification (requirements: training, experience, or self-study as a prerequisite to a four-part testing process); and the International High Technology Crime Investigation Association (requirements: peace officer, investigator or prosecuting attorney engaged in investigation or prosecution of computer criminal activity or management level/senior staff security professionals; no testing).

81 *See e.g.*, *The Digital Forensics Bibliography*, *www.e-evidence.info/biblio.html*.

82 *See* Jablon, *supra* note 76. Meaningful certifications are offered by some software manufacturers. For example, EnCase (EnCE) certification requires successful completion of written and a practical examinations and training or experience.

A large number of so-called computer forensic experts are familiar with forensic software but do not understand how that software works. While that understanding may not be necessary to adequately performing the task at hand, it may be necessary for expert testimony to be effective. If the expert is unable to explain how the software works and how it generated the result obtained, the expert may not be allowed to testify.[83] Even if the expert is allowed to testify, an inability to explain the process will likely mean an inability to persuade the trier of fact that the expert's result is accurate.

It is exceedingly important that the expert be able to explain the complexities of the forensics process in plain English with as little "computereze" as is possible. The expert should assume that the judge knows little, if anything, about how computers work, how data is stored, what deleting data means, and how data is retrieved. The lawyer should do a test run with the expert. He should be asked to explain the processes he employed to obtain the results he reached. Until and unless the lawyer is able to follow the expert's explanation, neither the lawyer nor the expert is prepared for the expert's testimony.[84]

Some computer forensics may have the wrong mindset. Some with a law enforcement background may jealously guard the secrets of their trade. As a result, they are not good witnesses because their defensiveness causes them to withhold meaningful explanations.

The computer expert needs to be mindful that lack of knowledge often breeds skepticism. While the following was written thirty-five years ago, the concerns expressed undoubtedly still exist among those born before the onset of Generation X:

> Although the computer has tremendous potential for improving our system of justice by generating more meaningful evidence than was

---

[83] *See, e.g., American Oil Co. v. Valenti*, 179 Conn. 349, 359 (1979) ("testimony by a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer" is required for the admission of computer-generated evidence.). *See also* FED. R. EVID 702, codifying *Daubert v. Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579 (1993). One district judge has opined that Rule 702 is applicable to computer-generated evidence. *Rivera-Cruz v. Latimer, Biaggi, Rachid, & Godreau, LLP, et al.*, D.N. 3:04-cv-02377-ADC (D. Puerto Rico, June 16, 2008).

[84] Dave Lang, *Dos and Don'ts for Digital Evidence*, Security Management Online, http://www.securitymanagement.com/library/001744.html.

> previously available, it presents a real danger of being the vehicle of introducing erroneous, misleading, or unreliable evidence. The possibility of an undetected error in computer-generated evidence is a function of many factors: the underlying data may be hearsay; errors may be introduced in any one of several stages of processing; the computer might be erroneously programmed, programmed to permit an error to go undetected, or programmed to introduce error into the data; and the computer may inaccurately display the data or display it in a biased manner. Because of the complexities of examining the creation of computer-generated evidence and the deceptively neat package in which the computer can display its work product, courts and practitioners must exercise more care with computer-generated evidence than with evidence generated by more traditional means.[85]

The expert must be able to persuasively explain to the skeptic why, if sound procedures are employed, there is no "possibility of an undetected error."[86]

In selecting a computer forensic expert, the lawyer also needs to be mindful of the expert's dual role: witness and consultant.[87] As a consultant, the expert should assist in the cross-examination of opposing experts.[88] He or she should be present for all testimony, whether lay or expert, about any aspect of the digital evidence in the case. The consultant should assist in voir dire by pointing out notable omissions, inconsistencies, and impossibilities in the opposing expert's qualifications.[89] He or she should assist the lawyer by suggesting well-constructed, relevant questions to ask on cross-examination. The technical aspects and jargon associated with computer technology in general leave abundant room for an expert to confuse the trier of fact and to offer opinions not based in a realistic evaluation of the data. The consultant should assist in understanding and cutting through the jargon.

Of course, it is imperative that the lawyer and the forensic be aware of a critical difference between a consultant and an ex-

---

85 Jerome J. Roberts, *A Practitioner's Primer on Computer-Generated Evidence*, 41 U.CHI.L.REV. 254, 255-56 (1974).

86 For a discussion of hearsay problems with computer-generated evidence, *see generally*, Harhai, *supra* note 23.

87 *See* text at footnotes 97 and 98, *infra.*

88 In doing so, the expert needs to be mindful of appearance. He needs not to appear to be an advocate.

89 M. LaBancz, *Expert vs. Expertise: Computer Forensics and the Alternative OS,* http://www.linuxsecurity.com/content/view/117371/49/sic.

pert witness. As long as the consultant remains a consultant, his or her work and communications with the attorney will usually be protected by the work product doctrine.[90] Once the consultant is disclosed as an expert witness, the work product protection ceases.[91]

III. The Roles of the Computer Forensic

The lawyer needs to define the computer forensic's tasks. The first task may be to give the lawyer assistance in deciding what to request. This can be as simple as helping the lawyer draft interrogatories and a request to produce. First, interrogatories should be designed to find out what electronic evidence may exist. Then, a request to produce should be tailored to the electronic evidence in existence.

The second task for the forensic may be to obtain information from the devices produced in response to the request to produce. The major goal of computer forensics is to recover electronically stored information and explain it in the context of the metadata[92] that exists on a computer or other digital media. The explanation can be as straightforward as a statement of what information is present on a storage device. The explanation can be as complex as explaining the sequence of events responsible for the presence or absence of certain important data. Stated in a different way, on occasion, how, when, and by whom information was placed on or removed from a device may be of greater importance than the information itself. Thus, while the forensic strives to retrieve as much data as is possible, he or she should know that data alone is not the only goal of the forensic process.

The quality of the forensic investigation should not be limited by the tools employed by the forensic. State of the art software is essential.[93] Using such software makes possible

---

90 *Hickman v. Taylor*, 329 U.S. 495 (1947). There are, of course, limitations on what is work product and qualifications on what is protected. *See*, generally, E. Epstein, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE (ABA Section of Litigation, 3rd Ed. 1997).

91 FED. R. CIV. P. 26(a)(2)(B) and commentary.

92 *See* IV. F., *infra*.

93 As the state of the art of computer forensics changes, so too do the state of the art tools. As this article is being written state of the art tools include Software's EnCase®, http://www.guidancesoftware.com/computer-

combing through vast amounts of data, both active and deleted. Original media is never analyzed because using original media will necessarily alter it. Instead, the subject of the analysis is a forensic copy (referred to as a mirror, clone, or ghost).

The forensic acquisition of electronically stored information can be fairly straightforward in the case of desktop and laptop computers but can become extremely technical when performed on such sources as email servers and cellular telephones. Commercially available copying software that is often used is not recommended for this task. The media needs to be acquired in a forensic manner such that the files themselves are not touched, slack file space[94] is acquired, and a hash value is obtained.

A hash value is a mathematical algorithm, in essence a digital fingerprint, of the original media that needs to be exactly the same as the forensic copy to ensure that a true "mirror" copy or exact duplicate is created. This hash value will again be important if a forensic expert is employed by the opposition to do their own forensic examination. The hash value assures that all parties are looking at the same evidence.

Forensic investigations may require the use of software tools that are used to analyze specific types of information. NetAnalysis®,[95] for instance, is used for recovery and analysis of deleted Internet histories. Super Yahoo Messenger Archive Decoder®[96] allows the forensic to read Yahoo chat conversations without a password.

Software tools are not enough. Computer forensics requires specialized expertise, the capacity to think outside the box, the ability to investigate, and knowledge of how findings affect and interact with legal proceedings.

---

forensics-ediscovery-software-digital-evidence.html, and AccessData's Forensic Toolkit®, http://www.accessdata.com/forensictoolkit.html.

94 "Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called 'file slack.'" NTI, Information, http://www.forensics-intl.com/def6.html.

95 Digital Detective, Netanalysis, http://www.digital-detective.co.uk/netanalysis.asp.

96 Paravi Software Solutions Home Page, http://www.piravi.com.

In short, a computer forensic should be able to provide consulting from the onset of litigation. He or she should be able to assist in fashioning discovery requests, testify in support of obtaining court orders for electronic discovery, examine media, engage in trial consulting about trial tactics, assist with evidentiary issues, and, ultimately, testify as an expert witness.

IV. Types of Electronically Stored Information

A. *Emails*

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication. E-mail messages are usually encoded in ASCII text.[97] However, non-text files, such as graphic images and sound files, may be sent as attachments in binary streams. E-mail was one of the first uses of the Internet and is still the most popular use. A large percentage of the total traffic over the Internet is e-mail.[98]

B. *Voicemail*

Voicemail is a computerized telephone answering system that digitizes incoming voice messages and stores them on disk or flash memory. It usually provides auto-attendant capability, which uses prerecorded messages to route the caller to the appropriate person, department, or mailbox. Voice mail systems may also offer directory lookup by name.[99]

---

97 Because computers only use binary numbers, words must be translated into numbers. ASCII, an acronym for the American Standard Code for Information Interchange, is a code for representing English letters as numbers, with each letter assigned a number from 0 to 127. Internet.com, Webopedia, http://www.webopedia.com/TERM/A/ASCII.html.

98 E-mail can also be exchanged between online service provider users and in networks other than the Internet, both public and private. E-mail is one of the protocols included with the Transport Control Protocol/Internet Protocol (TCP/IP) suite of protocols. A popular protocol for sending e-mail is Simple Mail Transfer Protocol and a popular protocol for receiving it is POP3. SearchMobileComputing.com, http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci212051,00.html.

99 Answers.com, http://www.answers.com/topic/voicemail.

C. *Instant messaging*

Instant messaging (IM) is a type of communications service that enables one to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communications. Typically, instant messaging systems alert the user whenever somebody on the user's private list is online. The user can then initiate a chat session with that particular individual.[100]

D. *Text messages ("texts")*

Text messages or texts are the exchange of brief written messages between mobile phones over cellular networks. While the term often refers to messages sent using the Short Message Service (SMS),[101] it can also include messages containing image, video, and sound content, such as MMS[102] messages. Individual

---

100 Internet.com, Webopedia, http://www.webopedia.com/TERM/I/instant_messaging.html.

101 SMS stands for "Short Message Service." SMS is used to send text messages to mobile phones. The messages can typically be up to 160 characters in length, though some services use 5-bit mode, which supports 224 characters. SMS was originally created for phones that use GSM (Global System for Mobile) communication, but now all the major cell phone systems support it. SMS is most commonly used for text messaging between friends or co-workers. Subscription SMS services transmit weather, news, sports updates, and stock quotes to users' phones. SMS can also notify employees of sales inquiries, service stops, and other information pertinent to their business. Doctors can receive SMS messages regarding patient emergencies. Text messages sent via SMS do not require the recipient's phone to be on in order for the message to be successfully transmitted. The SMS service will hold the message until the recipient turns on his or her phone, at which point the message will be sent to the recipient's phone. TechTerms.com, *SMS (Short Message Service),* http://www.techterms.com/definition/sms.

102 MMS stands for "Multimedia Messaging Service." MMS, sometimes called Multimedia Messaging System, is a communications technology developed by 3GPP (Third Generation Partnership Project) that allows users to exchange multimedia communications between capable mobile phones and other devices. An extension to the SMS protocol, MMS defines a way to send and receive, almost instantaneously, wireless messages that include images, audio, and video clips in addition to text. When the technology has been fully developed, it will support the transmission of streaming video. A common current application of MMS messaging is picture messaging (the use of camera phones to take photos for immediate delivery to a mobile recipient). Other possibilities

messages are referred to as "text messages" or "texts" and can be retrieved forensically.[103] Text messages can be stored on a particular device for a short period of time, but also may be accessed from the phone service provider for a specified period of time as well.[104]

E. *Documents and Spreadsheets*

Like conventional hard copy counterparts, documents and spreadsheets can be found electronically in the form of various computer or digital files stored on a hard drive or other media device. These documents can represent a variety of information including on-line purchases, financial statements, financial records, reports, letters, and statements.[105]

F. *Metadata*

Metadata is information about a particular item of data. A common way to access metadata is to right click on a given file in Windows and then click on "properties." This should reveal metadata about the file including its creation date, when it was last accessed, and if and when it was ever modified. In similar fashion, a digital image taken with a digital camera will typically include information inside the data making up the digital picture about the camera with which it was taken and the date and time at which the camera was set. This too is metadata. In a forensic examination, metadata is critical when determining time lines of user activity because files in a computer can be sorted by their time/date stamps (their metadata) in an effort to help determine

---

include animations and graphic presentations of stock quotes, sports news, and weather reports. SearchMobileComputing.com, *Multimedia Messaging Service*, http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci 943702,00.html.

103 Wikipedia, *Text Messaging*, http://en.wikipedia.org/wiki/Text_messaging.

104 *See* Holson, *Text Messages: Digital Lipstick on the Collar*, NEW YORK TIMES, December 8, 2009.

105 Documents and spreadsheets may have untraditional file extensions based on the application used to create them. Documents and spreadsheets can be "hidden" by changing their file names and extensions. Forensic software, such as Encase by Guidance Software or Forensic Tool Kit by Access Data, can be used to detect hidden documents and spreadsheets.

who was at the machine at a given point in time, as well as what the activity was.

G. *Digital images*

Digitization is the process of transforming images, text, or sound from analog media[106] into electronic data that can be saved, organized, and retrieved. The electronic data can be restored into perceptible surrogates of the original works. Of the vast number of digital images that are being created, still images, texts, motion pictures, and sound recordings predominate. A digital image is one that has been created through the process of digitization.[107]

H. *Video*

"Video is the technology of electronically capturing, recording, processing, storing, transmitting, and reconstructing a sequence of images representing scenes in motion."[108] Digital forms of video can be found on a variety of media sources such as DVD, CD-ROM, hard drives and thumb drives. Video can be formatted in a variety of ways including QuickTime, MPEG, AVI, and MOV files.

V. Devices Which May Contain Electronically Stored Information

ESI is all around us. The most common locations are desktop and laptop computers. Other media where ESI can be found include cell phones, external storage drives, digital cameras and loose media such as DVD's and thumb drives. Home

106 Analog media includes, generally, formats or objects that can be seen or heard.

107 Bowdoin, http://www.bowdoin.edu/it/dam/def-of-digital-image.shtml.

108 "Streaming video is a computer concept wherein video is served over a data network, traditionally the Internet, and rather than being saved for later playback, the data is played back immediately and then discarded. Websites typically use technologies like Adobe Flash to stream video, though some websites rely on older technologies like RealNetworks' RealPlayer and Microsoft's Active Streaming format. Streaming video's biggest advantage is a quick load time and content providers maintaining control over the content, but compatibility with diverse systems remains a concern for users." Obsessable, *Streaming Video*, http://www.obsessable.com/glossary/streaming-video.

and business networks, including company email servers, may also provide ESI.

When seeking ESI, it is important to consider uncommon places, including iPhones, Blackberry(s), Mp3 players, video game consoles, and G.P.S. devices. Many automobiles store in their on-board G.P.S. devices information about where, when, and sometimes at what speed, a particular route was taken.[109] This information can be extracted and, in the right circumstances, be very important information in a case.

On-line sources of data and backup storage should also be considered. Companies such as Carbonite[110] and Mozy[111] offer complete backup of data. When a computer has been "lost" or the ESI contained in it is inaccessible, ESI may be obtained from the provider of an on-line backup service.

Data retrieval companies including Advanced Data Recovery[112] and Drive Savers' Data Recovery[113] may recover data even after efforts have been made to destroy a computer or cause physical damage to media. ESI can be obtained on-line from free Internet mail services such as Yahoo![114] and Hotmail.[115] Websites for social network services[116] such as FaceBook,[117]

---

109 Craig Ball, "*GPS Evidence Might Drive Your Case Home,*" LAW TECHNOLOGY NEWS, October 29, 2008, *available a*t http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202425606808; *see also*, Forensics Wiki, *Global Positioning System*, http://www.forensicwiki.org/wiki/Global_Positioning_System.

110 http://www.carbonite.com.

111 http://mozy.com.

112 http://www.adrecovery.com.

113 http://www.drivesaversdatarecovery.com.

114 http://yahoo.com.

115 http://www.hotmail.com.

116 A social network service focuses on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Wikipedia, *Social Network Services*, http://en.wikipedia.org/wiki/Social_network_services. Online social networking services are increasing in popularity daily and while many exist for dating, hobby-related hookups, and party announcements, some are being used as a method of building business connections. X. Jardin, "Online social networks go to work," http://www.msnbc.msn.com/id/5488683. *See also*, Social Network Sites: Definition, History, and Scholarship, Danah M. Boyd, School of Information, University of California-Berkeley and Nicole B. Ellison, Department of Telecommunication, Information Studies, and Media, Michigan State University. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

MySpace[118] and Twitter[119] may provide useful ESI. Personals sites such as Adult FriendFinder[120] may also be a source of important ESI, especially in jurisdictions where fault is relevant.[121]

On-line ESI sources may not be known until a forensic examination of electronic media reveals their existence. Emails from on-line free Internet mail services, online email services, and memberships in social network services and personals sites are often revealed by forensic examination. On other occasions, the most valuable information gleaned is the existence of the membership itself which can then be more thoroughly explored by deposition and subpoena.

VI. Beyond Data Recovery

The examination and review of computer digital evidence is unlike any other type of evidence examination. It almost always involves the review of enormous amounts of data and often requires the use of multiple forensics tools to do so. Because computer evidence is by its nature digital, and digital evidence is fragile, such evidence requires special forensics software tools for examination as well as the knowledge of how to use them correctly. Hence, computer evidence is virtually always examined in a controlled laboratory environment by trained personal using specialized investigative software.

Computer forensics is more appropriately called a computer or digital investigation. In other words the media is investigated to determine what occurred, when it occurred, how it occurred and who was responsible for its occurrence. To answer these questions requires not just a working knowledge of data recov-

---

117 http://www.facebook.com.

118 http://www.myspace.com.

119 http://www.twitter.com. It has been reported that Twitter is the most popular English word of the year, 2009, a distinction not previously achieved in their first year by previous internet companies such as MySpace, Facebook, and YouTube. J. A. Vargas, *Why Twitter is the Most Popular Word of 2009*, HUFFINGTON POST, *available at* http//huffingtonpost.com/jose-antonio-vargas/why-twitter-isthe-most-p_b_374140.html.

120 http://www.adultfriendfinder.com.

121 Adult FriendFinder's home page brazenly states: "Meet real sex partners tonight!" "Adult FriendFinder is your ultimate source for free sex personals, adult dating, amateurs & swingers. . . . Turn your wildest fantasies into reality. Join Adult FriendFinder today and make love tonight." *Id.*

ery, but a working knowledge of the Internet, it is applications, how offenses are committed with these applications, what types of behaviors are associated with which applications and a myriad of related issues.[122]

Much of what passes as computer forensics is only forensic to a minimal extent. It only answers the question: "What information is here?" It is data recovery. It may not even address what may be the most important data in a case, deleted files and deleted history.

The typical data recovery or "e-discovery" company is provided with the media, usually a computer. A technician extracts active (undeleted) data and places it in a standard format (such as TIF files[123]) for the attorney to cull through. The technician does not address or analyze the sequence of events responsible for the existence of the data presented.

Computer forensics can and should be more than a mere compilation. It should be an investigation.[124] The media examined should be analyzed in the context of the litigation. The role of the computer forensic includes informing the attorney about anything and everything potentially relevant to the case. Individual pieces of data are often meaningless unless the context of the data is analyzed and explained.

The first consideration in a forensic acquisition is to ensure that data on the drive being duplicated is not altered. If the data being acquired is damaged in the process, authentication for purposes of having it admitted into evidence will be made difficult or impossible.[125] The method of acquiring data without altering it is not mysterious. The hard drive is duplicated in a forensically-sound fashion and secured. The duplicate must contain a copy of every bit, byte, and sector of the hard drive, including unallo-

---

122 "The overall computer forensics process is sometimes viewed as comprising four stages: Acquire: Identifying and Preserving; Analyze: Technical Analysis; Evaluate: What the lawyers do; Present: Present digital evidence in a manner that is legally acceptable in any legal proceeding." http://computer-forensics.safemode.org/index.php?page=four_Step_Process.

123 TIF ("Tagged Image File") is a "high-quality graphics format often used for storing images with many colors, such as digital photos." FileInfo.com, *TIF File Extension*, http://www.fileinfo.com/extension/tif.

124 M. LaBancz, *Expert vs. Expertise: Computer Forensics and the Alternative OS*, http://www.linuxsecurity.com/content/view/117371/49/sic.

125 *See* text at notes 80-85, *supra.*

cated space and slack space. The process is described as making a "clone," an "image," a mirror," or a "ghost." There is not one process for making a duplicate. A number of tools are available. Some create a drive image, that is a file which can be restored to match the source drive.[126] Others create a clone drive which duplicates the source data without the need for data restoration.[127]

Being able to establish that the data has not been altered and is complete is just as important as not altering the data. That confirmation is provided by a digital thumb print in the form of hash values or check sums. These 128bit to 256bit strings of characters represent the media as a whole. Hash values, sometimes called check sums, are created for the original drive to be copied and for the copy itself. If the two numbers are identical, nothing has been altered and an exact duplicate has been made.[128] For the hash values to be identical, forensic software and/or hardware must be used.[129] Commercial copying software typically used by office IT professionals may "touch" the files as it copies, irrevocably altering dates associated with their access and resulting in different hash values.

VII. Critical Areas of Forensic Examination

In a typical laptop or desktop computer there are many critical areas that should be examined for relevant ESI. They include user profiles, installed programs, My Documents, deleted data and unallocated file space, cache files, and browser history.

A user profile is a collection of personal data associated to a specific user, usually the owner of the computer. User profiles

---

126 One such device is ICS Image Masster Solo-3 (www.icsforensic.com).

127 Hardware cloning devices are available from Intelligent Computer Systems (www.ics-iq.com) and Logicube, Inc. (www.logicube.com).

128 A hash function is a transformation that takes an input and returns a fixed-size string which is called the hash value. RSA Laboratories, *What is a Hash Function*?, http://www.rsa.com/rsalabs/node.asp?id=2176. Said another way, "[a] hash function accepts a value of any size as its input, performs a complex calculation on that input and returns a value of fixed length as its output." Craig Ball, *Computer Forensics for Lawyers Who Can't Set a Digital Clock*, *available at* http://www.craigball.com/CF_0807-Digital%20Clock%20article%20only.pdf.

129 *See* notes 101 and 102, *supra*.

can be found on operating systems, such as Microsoft Windows and Mac OS, and are used to store information and items associated to a particular user.[130] Online forums can also have user profiles where the user may write a short résumé and add a photo. Statistical information about the user, such as date of birth, height, and weight, may also be displayed.

User profiles are very elaborate in online social networking services such as Facebook, Google profile or LinkedIn. In those services, a user may describe his or her identity. The information present in these profiles is often inaccurate and can be fodder for cross-examination.

A forensic user profile is distinct from a user profile on an operating system, forum or networking service. The forensic examiner will often attempt to determine if patterns of use of the computer can be established. If patterns are established, they may be extremely helpful in determining who was at the keyboard at critical times.[131]

The existence of installed programs can be determined with forensic software. The forensic examiner will create an inventory of the machine's applications and programs to ascertain if any exist which are relevant to the examination. Applications and programs may reveal information about the user and the types of use the machine sees. In a rudimentary sense, analysis of the computer's applications and programs may lead to a forensic user profile. Moreover, such an examination may lead to files of significance. For example, file sharing applications such as Limewire and Kazza that allow a user to search for and collect digital images can be analyzed to determine the types of images searched for by the user as well as those that were saved. Child pornography and pictures of deviant sexual behavior may have relevance to the case.

The default Windows location, My Documents, is usually used to save documents, music, pictures, downloads, and other files. My Documents also includes the accompanying metadata indicating each file's creation, modified and last accessed dates.

---

130 Indiana University, Information Technology Services, http://kb.iu.edu/data/aidk.html.

131 Tamas Abraham, *Event Sequence Mining to Develop Profiles for Computer Forensic Investigation Purposes*, Information Networks Division, *available at* http://crpit.com/confpapers/CRPITV54Abraham.pdf.

A review of that metadata may be useful in creating a time line of critical computer events which, in turn, may assist in determining who was responsible for those events.

Deleted data and unallocated file space can be of tremendous importance because when a file is deleted in Windows it is not necessarily gone forever. Even formatting a disk will not necessarily destroy information.

To understand why deleting a file does not really erase it, one needs to understand how Windows maintains files. Files are created at various locations on the hard drive. Windows keeps track of them in a master file table. When a file is deleted,[132] Windows does not actually locate the file and remove it. Instead, it tells the operating system that the disk space containing the data, called unallocated space, is available for storage of new data. The deleted data remains until it is overwritten by new data. If a computer has been in use for some time, it will likely have substantial data in unallocated file space. How long the deleted data will remain before being overwritten will depend on many factors. But the chances are good that unless the user has used software to erase or wipe the hard drive, significant amounts of deleted data or bits and pieces of deleted data will remain.

Forensic software allows one to view and retrieve deleted files, even if they have been partially overwritten. A consequence of deleting a file is that the operating system no longer "sees" the file. As a result, deleted data retrieved from unallocated file space will not have corresponding metadata regarding creation, modification, and last accessed dates. Nonetheless, the existence of the data itself is often of critical importance. It can include virtually everything including internet histories, letters, e-mails, and images.[133]

Internet web browsers keep files called cache files that automatically index the user's browser sessions in detail. Dates and

---

132 To delete files, access the internet and click on "Tools," then click on "Internet options." At "Browsing history" click on "delete." This will bring up a "Delete Browsing History" menu upon which will appear buttons to delete files, cookies, history, forms, or passwords. Clicking on those buttons will delete information, but the information will not be eradicated.

133 A. K. Dart, *Deleted Files Can Be Recovered*, http://www.akdart.com/priv9.html.

times of web sites searched and visited, as well as images and videos, are all stored in cache files. In Windows, these files are called Temporary Internet Files (TIF's). Windows also keeps running textual logs of browser use called Index.dat files.[134] Index.dat files contain all web sites visited, including every URL,[135] every web page, and all e-mails sent and received.[136] Browser history can be sorted by time and date with forensic software. The computer forensic expert can create a moment-by-moment time-line of computer activity. While it is usually impossible to know to a certainty who was at the keyboard at a certain time, the information can, in some cases, make that knowledge easily inferable or exclude a particular person as having been engaged in that activity.

Browser history can help determine activity in social groups.[137] It can provide useful information about online prescription drug purchases, pornography viewing habits, online banking and transactions.

A. *Conduct of the Examination*

The forensics expert should use an investigative approach. The inquiry should be systematic. The expert should view the data as leads and should pursue those leads to otherwise unknown information. For example, an examination of a browser history may reveal the existence of a previously unknown bank account. The account number should be provided to the attorney. The inquiry, however, should not end there. The expert should search, whether in unallocated file space or elsewhere, for information about the account. Any transactional information should be culled. Each forensic examination should include file signature analysis, keyword searching, hash set analysis, gallery viewing, and unallocated space searching.

File signature analysis involves searching for mis-labeled or un-labeled computer files. Operating systems provide signature

---

134 Wikipedia, *Index.dat*, http://en.wikipedia.org/wiki/Index.dat.

135 A URL, i.e., a Uniform Resource Locator, is the global address of documents and other resources on the web. Webopedia, *URL*, http://www.webopedia.com/term/u/url.html.

136 Acesoft, *Index.dat File*, http://www.acesoft.net/delete_index.dat_files.htm.

137 Social groups include Facebook, MySpace, and LinkedIn.

verification tools which allow one to verify that the file actually contains the data indicated by its filename extension.[138] A filename extension is a suffix to the name of the computer file which indicates the file format of its contents. For example, "doc" indicates a written document and "jpg" indicates an image. The signature analysis tool alerts the expert that an extension, such as doc, does not match the actual data content of the file, an image.[139] That the extension does not match the format of a file's content indicates that a user may have attempted to hide the file's content.

Forensic software also allows for keyword searching through both allocated (live) files and unallocated (deleted) file space and will reveal every instance where the keyword appears. For instance, if a nickname, used for chatting and email with Yahoo!, is known or discovered during the examination, that nickname can be searched and may uncover previously deleted emails and chats. In similar fashion, searching keyword combinations relevant to the use of web search engines such as Google and Yahoo may uncover deleted Internet searches. Information which would otherwise be hidden about what the user searched for and, potentially, the results of that search may come to light.[140]

Keyword searching is generally the most efficient method of combing through vast amounts of textual data on a given hard drive. It is impossible to manually review all data on even an average-sized laptop. Keyword searching allows for selective, efficient searching. Both active and deleted files can be searched. A name that appears in e-mail or a chat can be keyword searched and other e-mails and chats containing that name will be revealed. Keywords can be searched in combination in conjunction with search engines like Google or Yahoo! to find deleted searches and, often, the results of those searches.

Hash values[141] can be used to identify files. Just as the content of a drive can be hashed,[142] so too can individual files be

---

138 FILExt is a website which can be used to find out what a file extension means and the type of data it represents.

139 *See FILExt The File Extension Source*, http://filext.com.

140 See *Keyword Searching*, Project Bamboo, https://wiki.projectbamboo.org/display/BPUB/Keyword+Searching.

141 *See* text at pages 20 - 21, *supra.*

142 *See* text at footnote 79 - 80, *supra.*

hashed creating unique fingerprints for them. Once a hash value for a given file is known, the forensic expert may search for that hash value with the forensic software throughout other computers and other pieces of media. This can be useful in determining if personal files have been taken from one user's machine and placed on another machine with or without the user's knowledge.[143]

Images, both allocated and unallocated, can be retrieved by forensic software and placed in a thumbnail gallery view. This gallery can then be sorted by file creation date creating a time line of images that can be scrolled through relatively rapidly.

Often the data that is most relevant to the case will have been previously deleted and can only be found in unallocated file space. Forensic software provides various tools for finding this data. Although data recovered from unallocated file space will no longer have associated metadata revealing date of creation, last access and the like, sometimes a date will become evident. A recovered letter, for example, may have a date with the signature line. A deleted web page may have an embedded date that was part of the page itself when it was viewed by the user. Many commercial pornography portal sites offer gateways to explicit images and videos by offering visitors links organized by sexual subject matter. Many of these portal sites have an embedded date and time reflecting when the portal was last updated. When that page is cached to the user's computer, that embedded information will be included. Even if that cached page is deleted, it may be recovered with forensic software. The date and time that the user was there will be recovered.

B. *Assembly and Presentation of Findings*

The examiner needs to be able to present his or her findings in an articulate, understandable way.[144] Advocacy should be

---

143 *See generally*, SearchSQLServer.com, *Definitions hashing*, http://searchsqlserver.techtarget.com/sDefinition/0,,sid87_gci212230,00.html.

144 *See generally*, Forensic Focus Computer Forensic News, Information and Community, *Computer Forensics Reports - Sample Reports, Articles & Links*, , http://www.forensic focus.com/report-writing.

avoided. A well-constructed report should persuade the court that its findings are sound.[145]

The report should begin with an explanation of how the investigation began and how a forensically sound copy of the data was made. It should detail the methodology employed throughout the examination. It should explain the workings of any software employed and should set forth any data of interest and where it was found and anything relevant about the data.

For example, if a user's web browsing is of importance to the case because it is claimed that the user is addicted to internet pornography and the examiner found deleted web pages that are relevant, the report should identify those pages and the information on them. The report should also discuss how web pages in general are cached by the operating system, how they were deleted, and how they were retrieved by the forensic software. Explanations need to be focused on relevant findings, but too much maybe confusing and may appear to be self-aggrandizing.

The report should include screen captures or screen shots[146] taken during the forensic process. During the narrative of the report, reference can be made to individual screen captures to assist the reader's understanding.

VIII. Special Issues in Family Law Cases

A. *Child Pornography and Child Sexual Abuse Allegations*

Few issues are likely to stir as much controversy, or emotion, as allegations of child pornography or child sexual abuse by one parent against another. Mere allegations alone can be enough to cause tremendous damage to reputation, and can cause irrevocable damage to family relationships. The Internet has made the viewing of depictions of virtually every conceivable sexual act a mouse click away. While possession of child pornography is illegal,[147] finding child pornography on the Internet is not particu-

---

145 *See generally*, *Rivera-Cruz v. Latimer, Biaggi, Rachid, & Godreau, LLP, et al.,* D.N. 3:04-cv-02377-ADC (D.P.R., June 16, 2008).

146 A screenshot or screen capture copies what is currently displayed on a computer screen to a file or printer. Internet.com, Webopedia, www.webopedia.com/TERM/S/screen_capture.html.

147 *See e.g.* Child Pornography Prevention Act of 1996, 18 U.S.C. §§ 2251 - 2260.

larly difficult. In cases involving child pornography or child sexual abuse allegations, electronically stored information may be very telling. Trying to disprove or prove allegations that a party has viewed child pornography will usually necessitate forensic analysis of personal and business computers.

A fundamental understanding of what a "child" is and what constitutes "child pornography" is necessary both for the matrimonial attorney and the forensic expert. A "child" or "minor" is defined by law as anyone under the age of eighteen.[148] The definition of "child pornography" is not as simple to interpret or to determine in practice. Federal law defines child pornography as:

> any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where–
>
> (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
>
> (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
>
> (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.[149]

The issue in forensic analysis becomes how a forensic expert can identify child pornography when reviewing and removing data from an electronic device.

Though it is the job of the matrimonial lawyer to create an argument as to why an image is or is not child pornography, the lawyer will only succeed in making such an argument with the proper evidence and, many times, with the aid of expert testimony. Computer forensic experts are critical in discovering evidence of child pornography and in offering expert testimony as to how the child pornography was placed on the electronic device, when it was placed on the device, and when the pornography was accessed. The fundamental issue for a family lawyer using a forensic expert to obtain data either in support of or in defense of child pornography or child sexual abuse allegations is ensuring that the expert has an understanding of what constitutes "child pornography."

---

148 18 U.S.C. § 2256(1).

149 18 U.S.C. § 2256(8).

For example, if a person has pornography on a personal computer that portrays a mature-looking seventeen-year-old engaging in sexually explicit conduct, is that "child pornography"? Furthermore, determining the age of someone in an image is difficult, at best, if the person appears to be a teenager. There are thousands of teen pornography web sites on the Internet, many with models who appear to be quite young. Federal law requires that all producers of pornography keep records of identification on file as to the names and ages of actors and models portrayed.[150] Many United States-based, and some foreign-based, pornographic web pages have a compliance notice displayed on their opening pages.[151] True child pornography web sites do not include a compliance notice and most brazenly announce that they contain real child pornography.

Whether a court will accept the testimony of a computer forensic as being expert on the issue of child pornography and child sexual abuse is not easily predictable. Many states follow the federal threshold standard for the admissibility of expert testimony set forth in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*[152] In *Daubert*, the Supreme Court rejected the *Frye* stan-

---

150 18 U.S.C. §§ 2257.

151 A typical compliance notice reads:

> 18 U.S.C. Section 2257 compliance notice:
>
> All models, actors, actresses and other persons that appear in any visual depiction of actual sexually explicit conduct appearing or otherwise contained in this Website were over the age of eighteen years at the time of the creation of such depictions.
>
> All other visual depictions displayed on this Website are exempt from the provision of 18 U.S.C. section 2257 and 28 C.F.R. 75 because said visual depictions do not consist of depictions of conduct as specifically listed in 18 U.S.C section 2256 (2) (A) through (D), but are merely depictions of non-sexually explicit nudity, or are depictions of simulated sexual conduct, or are otherwise exempt because the visual depictions were created prior to July 3, 1995.
>
> With respect to all visual depictions displayed on this website, whether of actual sexually explicit conduct, simulated sexual content or otherwise, all persons in said visual depictions were at least 18 years of age when said visual depictions were created.
>
> The original records required pursuant to 18 U.S.C. section 2257 and 28 C.F.R. 75 for all materials contained in the website are kept by the following Custodian of Records:

152 509 U.S. 579 (1993) [hereinafter *Daubert*].

dard of admissibility.[153] The Court stated: "[f]aced with a proffer of expert scientific testimony, then, the trial judge must determine at the outset, pursuant to Rule 104(a), whether the expert is proposing to testify to (1) scientific knowledge that (2) will assist the trier of fact to understand or determine a fact in issue."[154] To make this assessment, the Supreme Court set forth a multi-factor analysis, including whether or not the scientific or technical knowledge posited by the expert can be, or has been, tested, whether it has been subjected to peer review and publication, the known or potential rate of error, and the general acceptance of the proposed theory or technique.[155]

Despite the prevalent, and almost overwhelming, use of electronic media and electronically stored information in both people's business and personal lives, "[c]omputer forensics is in the early stages of development and as a result, problems are emerging that bring into question the validity of computer forensics usage in the United States (U.S.) federal and state court systems."[156] Beyond the practicalities of the expert being able to identify what images are "child pornography," there are legal issues as to the weight of expert evidence by computer forensics, a relatively novel field. In applying the multi-factor analysis set forth in *Daubert* to the use of computer forensic experts in child custody cases involving allegations of child pornography use and child sexual abuse, questions are raised as to, among other things, the field's ability to be subject to testing, the availability of peer review and publication, the rate of error, and the general acceptance of the testimony being offered. Since computer forensics is a developing field and "there are no standards in the field or peer reviews of methods,"[157] very little information exists for attorneys and judges to use to determine whether one forensic method is superior to another.[158] It seems that, in many cases,

---

153 *See Frye v. United States*, 293 F.1013 (D.C. Cir. 1923). *Frye* held that expert testimony must be based upon a well-recognized principle, sufficiently established to have general acceptance in the relevant scientific community.

154 *Daubert*, *supra*, note 152, at 592.

155 *Id*. at 593-94. This list is not exhaustive.

156 Meyers and Rogers, *Computer Forensics: The Need for Standardization and Certification*, 1 INT'L JOURNAL OF DIGITAL EVIDENCE, Fall 2004, Vol. 3, Issue 2.

157 *Id.* at 5.

158 *See* discussion, *supra* pp. 19-23.

the attorney planning to present expert testimony or to cross-examine an expert must begin to familiarize himself or herself with forensic methods and critically analyze the validity of the information put forth.

Federal law makes it a punishable offense to knowingly transport, receive, distribute, sell, or reproduce visual depictions of a minor child engaging in sexually explicit conduct that have been transported or shipped in interstate or foreign commerce using a computer or the mails.[159] It is also illegal when a person "knowingly possesses one or more books, magazines, periodicals, films, videotapes, or other matter which contain any visual depiction that has been mailed or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer."[160] It is a crime to knowingly transport, receive, distribute, sell, or reproduce visual depictions of a minor child engaging in sexually explicit conduct that have been transported or shipped in interstate or foreign commerce using a computer or the mails "for purposes of inducing or persuading a minor to participate in any activity that is illegal."[161]

It is also illegal for a person to knowingly possess, produce, distribute, receive, or possess with intent to distribute a "visual depiction of any kind" that "depicts a minor engaging in sexually explicit conduct; and is obscene" or "depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; and lacks serious literary, artistic, political, or scientific value."[162] Under the statute, a "visual depiction" can include "data stored on a computer disk or by electronic means which is capable of conversion into a visual image. . .[a] digital image or picture, computer image or picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means."[163] If an attor-

159 18 U.S.C. § 2252(a).
160 18 U.S.C. § 2252(a)(4).
161 18 U.S.C. § 2252A(a).
162 18 U.S.C. § 1466A(a)-(b).
163 18 U.S.C. § 1466A(f)(1).

ney represents a client who suspects the other party has sexually abused children or views or distributes child pornography, the attorney should consult the statutory definition of what constitutes a visual depiction so as to fully instruct a forensic expert regarding the depth and breadth of his analysis.

When allegations are made of internet child pornography viewing by a divorcing spouse many questions need to be asked and answered, including: What was allegedly seen? When was the image or video seen? Was it seen on multiple occasions? If custody of minor children is at issue, were the children exposed to the child pornography? Were law enforcement officials called? Were child protection authorities contacted? Was there an investigation?

If three or more items of child pornography exists on any electronic device during the course of a forensic investigation, the device and any printouts containing the items should be immediately surrendered to law enforcement.[164]

There is an affirmative defense to the allegation that a client has possession of child pornography.[165] It is, however, no defense that the person possessing the pornography is an attorney or a computer forensic expert.

The affirmative defense is that the defendant:

> (1) possessed less than three matters containing any visual depiction proscribed by that paragraph [(a)(4)]; and
> (2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction or copy thereof–
>
> (A) took reasonable steps to destroy each such visual depiction; or
>
> (B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.[166]

In short, the attorney or computer forensic who comes into possession of fewer than three items of child pornography must proceed with caution. The statute permits the destruction of fewer than three visual depictions of child pornography or a report to law enforcement as a defense to an allegation of posses-

---

164 *See* § 18 U.S.C. §2252(c)(1) which makes it a defense to prosecution that the defendant "possessed less that three matters containing any visual depiction [of child pornography]."

165 18 U.S.C. § 2252(c).

166 18 U.S.C. § 2252(c)(1)-(2).

sion of child pornography. The latter, however, may implicate a client. Some computer forensics have a policy of always providing child pornographic images to law enforcement. The attorney and the computer forensic need to agree upon a course of action before child pornography is discovered.

B. *Drug Abuse Allegations*

A persistent occurrence that is seen more and more frequently as use of the Internet has grown is the online purchase of prescription drugs. Sometimes legally purchased, sometimes not, the addictive use of medication purchased over the Internet is often revealed for the first time by way of forensic examination of a computer.

The Internet holds literally thousands of web-sites devoted to the questionable sale of prescription narcotics such as Oxycontin and Percocet.[167] Many of these sites require little or nothing in the way of valid prescriptions or will offer an online evaluation by a "doctor" who creates the prescription. Many of these sites advertise themselves by way of spam email.

Just as money transfers and asset management occur using a web browser and visiting web pages, so too do most prescription medication sales sites. Hence, when these sites are visited, the pages are cached with date/time stamps as well as indexed in the history files. A forensic examination may thus reveal how many and how frequently these sites were visited, what was purchased, and the quantity purchased. Knowledge of a prescription drug addiction can obviously be very relevant for issues such as child custody.

IX. Conclusion

To say that electronically stored information poses challenges is an understatement. Nonetheless, it should never be overlooked. Electronically stored information may be the only evidence on an important issue. In may serve two purposes: ob-

---

167 The proliferation of drug websites offering narcotics for sale is exceeded only by the apparent interest in narcotics. For example, on August 31, 2009, Google reported 2,990,000 hits for the word "Percocet," http://www.google.com/search?hl=en&source=hp&q=percocet&btnG=google+Search&aq=F&oq=&aqi=.

taining information and impeaching the credibility of the opposing party. The lawyer, aware of the potential significance of electronically stored information, should find out whether the client possesses or may lawfully possess that information.

The impact of federal and state laws which may result in civil or criminal liability requires analysis. Ethical rules which may apply to the possession and use of electronically stored information warrant careful attention. Because the ultimate objective of obtaining that information is its use at trial, the lawyer needs to be careful to make sure that it is obtained in a manner which will not present an insurmountable evidentiary hurdle.

The lawyer needs to exercise great care in selecting a computer forensic. The expert's qualifications are important. So too is the expert's familiarity with the type of evidence being sought. The lawyer and the expert should discuss whether the expert will be a testifying expert, a consulting expert or both. The pitfalls of a dual role should be addressed early in the engagement.

The expert needs a clear understanding of his or her role. If testimony is a potential, the scope of the engagement should be defined. Will the expert merely be searching for and compiling data? Or will it be an in-depth forensic exercise?

The expert and the lawyer need frequent contact so that decisions about the scope of the examination are reviewed and revised from time to time. If information carrying potential criminal liability is discovered, the decision about what to do with it should be made in concert.

In a given case, electronically stored information may prove to be of critical importance.