The Florida Bar Journal
Advertising Rates • Lawyers Marketplace • Submission Guidelines • Archives • Subscribe • *News*
Journal HOME
October, 2008 Volume 82, No. 9

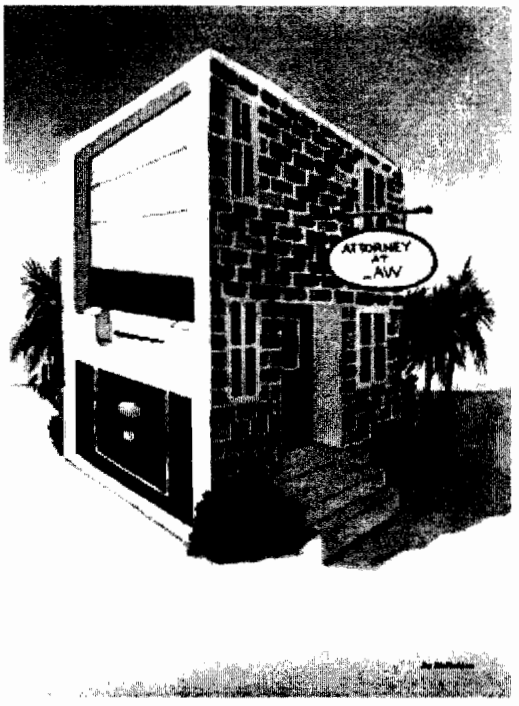
What Every Attorney Needs to Know About Electronic Technology

by D. Patricia Wallace

Page 22

These days an attorney can get away with not knowing what a bit, byte, or gig is, but no longer can a Florida lawyer meet his or her professional obligation of competent representation without knowing the basic characteristics of electronic data. This article provides an introduction to the technology of electronic data in the context of recent court decisions and suggests some easy methods for avoiding common and often costly pitfalls related to electronic technology.

1. All data that passes across an electronic medium is stored there, if only for a short period of time.



Every time we open an electronic file, from whatever source, including the Internet, we save data to our computer. This characteristic of electronic data is one of the most profound for the nonexpert. In layman's terms, opening an electronic file such as an e-mail or a document is tantamount to opening a book. Just like we cannot see the contents of the book without having it in our hands, we cannot read the contents of an electronic document without having the data comprising the document residing in our computer's memory, specifically, our computer's Random Access Memory (RAM). The electronic data differs from the book, however, because, unlike a book that can be reshelved, electronic data stays in our computer's memory even after we have closed the document. Electronic data also differs from the book in that we cannot readily detect most of the electronic data entering our computer's memory; we cannot see that data stays in our computer's memory; and we often cannot or do not control the flow of electronic data into our computer. For example, in order for us to see a Web page, numerous files comprising that Web page must be downloaded to our computer, including those that may be unwanted. These files or parts of them will remain on the computer in some form, likely inaccessible by the regular user.

Litigators must understand this characteristic of electronic data so that they can find information to support their client's claims or defenses. A recent decision from the Central District of California shows the value of being familiar with the staying power or stickiness of

electronic data. In *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419 (S.D. Cal. May 29, 2007), the plaintiff, Columbia Pictures, alleged that the defendant had pirated its copyrighted works.[1] The defendant allegedly sold copies of copyrighted works over the Internet, using a vendor's server located in the Netherlands to process orders.[2] To prosecute its case, Columbia Pictures wanted to find out how many copyrighted works were sold illegally and who made the illegal purchases. During discovery, its attorneys requested the IP addresses of users of the defendants' Web site, the users' requests for files (that is, the films purchased), and the dates and times of such requests.[3] The defendants contended that this information was not within their possession because it was routed to the RAM of their Dutch vendor.[4] According to the defendants, the information routed to their vendor's RAM was not "in any medium from which the data [could] be retrieved or examined, or fixed in any tangible form such as a hard drive."[5] This response may have been acceptable in the world of paper discovery, but Columbia Pictures' attorneys knew that any information that went across a server had to stay there if only for a short period of time. The attorneys confirmed through discovery that a customer's order remained in RAM for about six hours on the server in the Netherlands.[6] Columbia Pictures convinced the court that such information was in the custody and control of the defendants.[7] The court ordered the defendants to cause their vendors' automatic overwriting process to cease so that the requested information would be preserved during the course of litigation.[8]

It cannot be emphasized enough: All data that crosses over an electronic medium is stored there. The attorneys for Columbia Pictures used this knowledge as part of their litigation strategy. Conversely, defending attorneys need to anticipate requests such as those made by Columbia Pictures, work with their clients to develop a strategy before receiving such requests, and lay the groundwork for convincing the court of the appropriateness of their client's position and actions.

2. Deletion does not mean destruction.

By now, most attorneys know the basic rule that deletion of an electronic document does not eradicate it, but few contemplate all the dangers and opportunities arising from this characteristic of electronic data. "Deletion" of electronic files simply means that the space occupied by those files is now available to store other files. Techies commonly use the analogy that deletion of files is like removing a library's card catalog: The books are still in the library, but without another card catalog, the library patron cannot find them. In the electronic storage system, until new files occupy the old spaces, that data survives even if it is locatable only through the application of forensic software.

Attorneys must incorporate an understanding of this technology into every aspect of handling their clients' and their own electronic media. It is not enough just to be cautious about the fates of files, electronic media, and discarded computers. Attorneys must think how they can use this sticky property of electronic data to their client's advantage. For example, attorneys may want to consider whether to retain a computer forensics expert to recover "deleted" files. A fictional adaptation of circumstances in recent Florida litigation illustrates this point: An attorney representing a husband in divorce was surprised to learn after months of talking with his client that the wife had used the computer that now belonged to the husband. The husband assumed the wife's use was not important because she had copied all her files to CDs and then deleted the files from the husband's hard drive. The attorney knew better and engaged the services of a certified computer examiner. The husband was astonished by what the computer

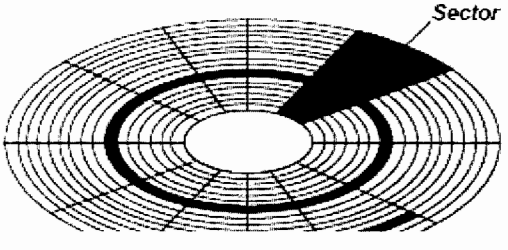
examiner was able to restore. So was the wife.

Understanding this basic characteristic of electronic data also applies defensively by helping attorneys avoid disclosure of confidential information. Without application of this knowledge, attorneys risk inadvertently producing materials and destroying the protection of attorney-client privilege not only with respect to the produced documents but also with respect to the entire subject matter of the documents inadvertently produced.[9] Courts are not always sympathetic to the plight of the lawyer who accidently turns over confidential documents to opposing counsel. In *Amersham Biosciences Corp. v. Perkinelmer, Inc.*, No. 03-4901(JLL), 2007 WL 329290 (D.N.J. Jan. 31, 2007), for example, the plaintiff's counsel carefully reviewed Lotus Notes e-mails saved on a DVD, segregated into a separate file those e-mails deemed "privileged," and deleted the file of privileged documents before submitting the DVD to the firm's vendor with instructions to prepare the documents in a readable format for production to opposing counsel. The vendor converted the files from Lotus Notes to single page image files.[10] Unknown to counsel, however, his vendor's software captured the "deleted" files and also converted them into single page images.[11] Without examining the processed DVD copy, counsel produced it to the opposing party.[12] Months later, producing counsel saw his error and asked for the return of the inadvertently produced privileged documents.[13] The parties took the issue to the magistrate judge who found the inadvertently produced Lotus Notes documents were privileged and ordered their return on the ground that plaintiffs knew or should have known that the information retrieved from this metadata was privileged and had not been intended to be disclosed.[14] The district court, however, disagreed. The court concluded that the producing party's counsel should have detected his error, and, therefore, the production of the documents waived the privilege.[15]

3. The typical hard drive of a computer is comprised of several disks, each of which contains fixed-size spaces for storing electronic data.

At first blush, this fact may strike the attorney as overly techie, but it is a simple concept that, if understood, can save much heartache. In simple terms, electronic file structure is like that of a metal file drawer where each file folder and each file drawer are of fixed sizes that do not expand or contract with the addition or deletion of material.[16] To apply the comparison to electronic data, two further conditions must be imposed: All of the folders and drawers are always full, and nothing can be removed from the file folders or drawers unless something else is stuck in its place. Electronic data storage media are comprised of clusters (the file drawers), which are, in turn, comprised of sectors (the file folders). Diagram A illustrates the basic storage structure of one side of a single disk of a hard drive.[17] When we save a file (for example, a Microsoft Word document) to a hard drive, the data of that file fills in cluster after cluster, writing over data that had been "deleted," until all the data of the file is stored. Any space left over in the last sector remains as "file slack." File slack remains filled with the "deleted" data.[18] Diagram B illustrates this storage structure and file slack.

Diagram A



The FBI and other law enforcement agencies here and abroad have examined electronic media's file slack and located incriminating evidence such as downloads from the Internet or e-mails.[19] Examination of file slack will play an increasingly important role in civil litigation as attorneys become more aware of the possible uses of computer forensics as a discovery tool. Although the

process of recovering data from slack and unallocated space (the space on a hard drive not occupied by a partition; it is not formatted) is labor intensive and expensive, recovering this data may be essential to prosecuting certain kinds of cases, and attorneys must understand the basics of this technology or associate with someone who does in order to provide competent representation.[20] No longer should a sentence such as "A bit-stream mirror image copy of the media item(s) will be captured and will include all file slack and unallocated space" sound foreign to attorneys. That is not techno-language; it is part of a magistrate judge's discovery order.[21] In some instances, companies are conducting their own internal computer forensics examinations when theft of proprietary information is a concern.[22] Attorneys need to know when this type of investigation is appropriate, and they need to be able to advise their clients of possible repercussions of such investigations. Such investigations may be discoverable. In *Lockheed Martin Corp. v. L-3 Communications Corp.*, No. 6:05-cv-1580-Orl-31KRS, 2007 WL 2209250 (M.D. Fla. July 29, 2007), the magistrate judge concluded that documents recovered through computer forensics examination are "facts" and are, therefore, "not protected by the attorney-client privilege."[23]

Understanding the structure of clusters and slack, attorneys can better protect themselves and their clients from inadvertent disclosure of confidential information. From a strategic perspective, a rudimentary understanding of electronic file structure may help attorneys discover opportunities to obtain relevant evidence they otherwise would have missed.

4. Information on work stations is not necessarily stored on network servers.
Ignoring this fact may result in sanctions for not adequately searching for responsive documents, especially where a request for production asks for all versions and variations of a single document. It is not uncommon, for example, for an employee to prepare a memorandum on his or her work station, save it to the server, revise the document, and save the revised version over the original version on the server. Depending on the network set-up, the original document may be inaccessible from the server, but it may remain on the employee's work station, thus, leading to a client's having two or more versions of the same responsive document. This problem is exacerbated as versions of documents are e-mailed and opened on different work stations.

Failure to understand or to heed this network basic can lead to sanctions, as it did in the trademark infringement case, *Cache la Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614 (D. Colo. 2007). In what appeared to be honorable efforts to preserve relevant material, Land O'Lakes' counsel, within days of filing of the suit, imposed a litigation hold and instructed employees to search for responsive materials, including paper documents, e-mails, and compact disks.[24] Counsel expanded its inquiry as discovery proceeded and included additional employees in the discovery process.[25] Despite these good faith efforts, counsel made a costly mistake in assuming that data stored on employees' hard drives was saved on Land O'Lakes' numerous servers. Because of this mistaken assumption, both in-house and outside counsel allowed Land O'Lakes to continue with its standard operating procedure of wiping clean the hard drives of the work stations of departed employees.[26] The magistrate judge, finding that Land O'Lakes' counsel had failed to monitor adequately the discovery process by not stopping Land O'Lakes' standard procedures for dealing with the computers of departing employees, held that counsel had "interfered with the judicial process." The judge imposed a $5,000 fine and ordered Land O'Lakes to pay the court reporter fees and transcript costs of the plaintiff's deposition of Land O'Lakes' in-house counsel.[27]

The *Cache la Poudre* order does not mean that clients must shut down all standard operating procedures when litigation appears imminent. Consistent with the holding in *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004), the order emphasizes that clients and counsel must take reasonable steps to preserve data and monitor compliance with a litigation hold. Sometimes a lockdown on hard drives may be expensive and disruptive. A good alternative is to hire a certified computer examiner to make mirror copies of all hard drives that may contain relevant information and to maintain a chain of custody record. This procedure provides a forensically sound copy of the relevant electronic media, which the computer examiner should keep in a safe, and the clients may continue to use their computers without fear of deleting or changing relevant information. If the client chooses this option, it *must* use a computer examiner working with appropriate software: Having employees or worse, attorneys, duplicate the files without the appropriate software actually changes the data on the hard drive, risks spoliation of evidence and consequential sanctions, and often requires the person who made the copies to serve as a witness.

5. Clients' information may be stored on the servers of third parties.
This basic is not so much technological as it is common sense, but as we have seen with the Columbia Pictures case, the nature of electronic data requires attorneys to cast a wider net to identify possible sources of relevant materials and to do so as soon as it appears that litigation is imminent. The first step for quickly identifying sources of relevant material, as almost every electronic discovery how-to pamphlet or book will advise, is to examine a data map of the client's information systems. An accurate and complete data map and inventory shows where information comes into the client's systems, where it is processed, where it leaves the client, where information is stored, where it is backed up, how client employees communicate within the organization, and how all the client's systems interact. A good inventory should show all laptops, home computers, and other devices for storing electronic data that are used for any company purpose, whether within the bricks and mortar of the client's operations, on the road, or in employees' homes. Often omitted from either the data map or the inventory, however, are identifications of vendors, attorneys, or other service providers who may have relevant data — perhaps the only remnants of that data. As happened in *Columbia Pictures*, a court may order a party to see that its vendor retains electronic information, even information as transient as that downloaded to RAM for the sole purpose of fulfilling purchase orders.

Attorneys who have continuing relationships with corporate clients should discuss data maps with them before litigation appears evident. Attorneys, however, should be aware that this is an extremely sensitive topic. The many companies that find themselves without a day's rest from litigation should be careful not to expose themselves in continuing litigation by admitting that their current procedures for handling electronic data are not sufficient. To avoid or mitigate this problem, companies may be able to show that their current procedures were reasonable given the circumstances at the time they were developed and that they proceeded with the improvements because of better technology and development of case law that clarified their responsibilities. Attorneys with continuing relationships with corporate clients need to work with them to ensure that the data maps and inventories are constantly updated and that the procedures for storing and deleting data comports with the changing law surrounding e-discovery.

Electronic discovery is a (if not THE) major litigation problem for most companies.[28] Of all the

reasons to learn something of electronic technology, this may be the most important. Electronic discovery is posing a huge and expensive problem to corporations.[29] Granted, most large enterprises have sophisticated IT departments and deep legal departments, but often there is a vast gap between the "geeks" and in-house counsel. A good outside attorney will serve as a translator between these two departments; the client and the court; and the client and its opponent. To be an effective translator, the outside attorney needs to understand the rudiments of electronic data creation, transmission, and storage, and he or she needs to be able to examine a client's data map and computer system inventory and understand it quickly. Litigators' intelligence when it comes to systems and electronic data is absolutely crucial in the context of federal litigation, where one must serve initial disclosures within at most three months of service and be prepared to tell opposing counsel within that time period what his or her client is willing and able to produce and in what format.

6. The history of clients' hardware, including hard drives may be critical.
Often we assume that clients' hardware was never used before the client obtained it, but that is not always the case, especially in our current world of numerous small start-ups where equipment changes hands in a relatively short period of time. An attorney who does not know the history of his or her client's work stations and servers may risk missing out on identifying relevant evidence. For example, in *Phoenix Four, Inc. v. Strategic Resources Corp.,* No. 05 Civ. 4837(HB) 2006 WL 1409413 (S.D.N.Y. May 23, 2006), the court held that outside counsel had failed to meet its discovery obligations because they did not identify and produce responsive information that was stored on a portion of their clients' server that had been partitioned from what employees could access from their work stations. The defendant, Strategic Resources Corp. (SRC), had provided various services for the plaintiff, Phoenix Four.[30] After the business relationship between the parties ended, SRC wound down, but its principle, Paul Schack, opened a new company, and there he installed a server and several work stations from SRC.[31] Once litigation started, Schack told outside counsel the new company did not have any responsive documents other than what it had already provided Phoenix Four during the course of their relationship.[32] Counsel relied on this representation and did not investigate what happened to the SRC computers once that business wound down.[33] The court did not view this omission as an innocent oversight and found that counsel "failed in its obligation to locate and timely produce the evidence stored in the server that the SRC defendants took with them from [their previous office]."[34] The court held that it was not enough that counsel *asked* its client for "all electronic and hard copy *documents*."[35] The court advised that counsel was obliged "to search for *sources* of information," and, in this instance, because counsel did not investigate the server of Schack's new company, counsel failed to meet their obligations.[36]

Between the data map and a short history of hardware (and in some cases whole systems), the attorney has, in fairly short order, an enormous head start in preparing a list of all places where relevant information may be found. Examining and understanding the data map and history also gives the attorney the enormous advantage of understanding better what the client does, how the client does it, where the client started, and where the client is going. Armed with this information, the attorney can more effectively and efficiently help his or her client through discovery in case after case.

7. Client assurances will not insulate attorneys from sanctions.
As discussed in connection with the *Land O'Lakes* and *Phoenix Four* decisions, courts are not allowing attorneys to rely on the assurances of their clients to excuse passive approaches to

discovery. In an unsettling decision from the Southern District of California, one judge contemplated reporting to the state bar attorneys who purported to rely on client assurances. In a patent enforcement action, *Qualcomm Inc. v. Broadcom Corp.*, No. 3:05cv1958-B (BLM) (S.D. Cal. Aug. 6, 2007), Doc. No. 593 at 32, the district court concluded the patents were unenforceable in part because it found that "by clear and convincing evidence . . . Qualcomm ['s] counsel participated in an organized program of litigation misconduct and concealment throughout discovery, trial, and post-trial before new counsel took over lead role in the case on April 27, 2007." After the district court ruled on the unenforceability of the patents, Magistrate Judge Barbara L. Major considered Broadcom's motion for sanctions for discovery violations. Judge Major ordered to appear before her "all attorneys who signed discovery responses, signed pleadings and pre-trial motions, and/or appeared on behalf of Qualcomm," to show cause why sanctions should not be imposed against them.[37] Among the sanctions the magistrate judge stated she would consider imposing on the attorneys were "monetary sanctions, continuing legal education, referral to the California State Bar for appropriate investigation and possible sanctions, and counsel's formal disclosure of this court's findings to all current clients and any courts in which counsel is admitted or has litigation currently pending."[38]

How had Qualcomm's attorneys violated the discovery orders? For one, they claimed they had not been able to find over 200,000 pages of relevant e-mails and other documents even though they were able to identify other company records. They also claimed that Qualcomm had "'kept [them] in the dark'" about these and other documents. Neither the district court nor the magistrate judge accepted these assertions. On October 29, 2007, Magistrate Judge Major recommended sanctions against Qualcomm and its attorneys.[39] On December 11, 2007, the district court adopted Judge Major's recommendation that Broadcom be awarded $8,568,633.24 in attorneys' fees, additional litigation costs, and expert fees as well as pre- and post-judgment interest.[40] On March 5, 2008, however, the district court vacated the sanctions order as to the attorneys, but not as to Qualcomm.[41] Qualcomm's appeal is pending before the U.S. Court of Appeals for the federal circuit.

8. Rule 26(f) may set a trap for the unwary.
As discussed in *Amersham* and *Qualcomm*, attorneys' ignorance of electronic discovery has led to inadvertent disclosure of client confidential information and inadvertent (or perhaps purposeful) failure to disclose responsive documents. Even with an understanding of electronic technology, however, attorneys risk disclosing confidential information because of the sheer volume of data to be reviewed and the fact electronic data is often hidden.

The Federal Civil Rules Committee recognized this problem, and the 2006 amendments to the Federal Rules of Civil Procedure tried to provide two mechanisms to help attorneys and clients avoid being penalized for inadvertent disclosure of confidential information: the so-called "clawback" and "sneak peek" agreements. These mechanisms, however, do not provide a panacea, and a brief analysis of the clawback provision shows attorneys cannot rely on them to solve problems stemming from attorneys' ignorance of technology.

Rule 26(b)(5) allows a party who has produced material it believes is subject to privilege to "notify any party that received the information of the claim [of privilege] and the basis for it." Once so notified, the receiving party "must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is

resolved." The comments to this 2006 amendment state: "Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production." Rule 26(f)(4) requires parties to consider these issues during the initial conference, and the notes recognize that a number of parties enter the now familiar "clawback agreements," which provide "that production without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances."

Clawback agreements sound like a good idea, but like so many good ideas, such agreements pose problems. First, the parties in litigation must keep in mind that clawback agreements are procedural arrangements, a child of the federal rules. Privilege issues are evidentiary and are governed by rules promulgated by Congress. A clawback arrangement alone does not protect privilege. Second, clawback arrangements are limited to the parties who entered them, and it is questionable whether they can be enforced against third parties.[42] Third, as with any waiver of privilege situation, once a document is produced, the privilege may be waived not only as to that document, but also as to all documents or communications of the same subject matter, even where privilege had been asserted.[43] Proposed Federal Rule of Evidence 502[44] attempts to resolve these problems by providing that inadvertent disclosure where the holder of the privilege took reasonable steps to prevent disclosure and where the holder of the privilege took reasonable steps to rectify the error will, as a matter of law, not act as a waiver. Unless and until this legislation is enacted, production of privileged documents is risky. Neither attorneys nor clients should enter clawback agreements (or sneak peek agreements) lightly, and how clients approach privilege issues including such arrangements should be carefully considered and ultimately incorporated into company-wide litigation preparedness plans.

Conclusion

Electronic discovery is slowly catching on in Florida, and savvy attorneys are learning to use it to their clients' advantage. Within a few years, there will be no escaping electronic discovery as litigators, rulemakers, and courts address the hard fact that the vast majority of contemporary information is created, manipulated, transmitted, or stored as electronic data. Attorneys do not need to be able to convert decimals into hexadecimals or understand hash values (yet), but we must have a basic knowledge of how data is stored on electronic media so that we can ask questions that will identify all sources of relevant information, develop viable discovery plans, and protect our clients.

[1] For the most part, this article discusses unpublished decisions of U.S. district courts in a number of jurisdictions. Few appellate courts have had an opportunity to review electronic technology decisions because these decisions are largely confined to discovery issues, which seldom reach appeal. The paucity of appellate opinions and even published trial court orders from Florida courts does not mean that litigators can await such decisions, the promulgation of state rules governing electronic discovery, or reported state court decisions. Florida's discovery rules are broad enough to include inspection of an opponent's computer system. *See Strasser v. Yalamanchi*, 669 So. 2d 1142 (Fla. 4th D.C.A. 1996). The infamous jury verdict of $1.4 billion against Morgan Stanley in *Coleman Holdings, Inc. v. Morgan Stanley & Co.*, No. 679071, 2005 WL 679071 (Fla. 15th Cir. Ct. Mar. 1, 2005), resulted in part from the court's giving the jury an adverse inference instruction in light of Morgan Stanley's failure to preserve e-mails after it knew that litigation was imminent. The Fourth District Court of Appeal reversed the

award on grounds unrelated to the alleged spoliation issue. *See Morgan Stanley & Co. v. Coleman (Parent) Holdings Inc.*, 955 So. 2d 1124 (Fla. 4th D.C.A. 2007).

[2] *See Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419 (C.D. Cal. May 29, 2007).

[3] *See id.* at *1.

[4] *See id.* at *5.

[5] *Id.*

[6] *See id.* at *3

[7] *See id.*

[8] *See id.*

[9] *See, e.g., Martin Marietta*, 856 F.2d 619, 621-23 (4th Cir. 1988) ("any disclosure of a confidential communication outside a privileged relationship will waive the privilege as to all information related to the same subject matter").

[10] *Amersham Biosciences Corp. v. Perkinelmer, Inc.*, No. 03-4901(JLL), 2007 WL 329290, at *1 (D.N.J. Jan. 31, 2007).

[11] *See id.*

[12] *See id.*

[13] *See id.*

[14] *See id.* at *2.

[15] *See id.* at *5-6.

[16] *See, e.g.,* Craig Ball, *Can Your Old Files — Don't Be So Sure Your Deleted Files Are Gone*, L. Tech. News 18 (Jan. 2004), *available at* www.americanbusinessmedia.com/images/abm/pdfs/events/neal_library/Law%20Technology%20News%201.pdf.

[17] Most hard drives now are designed so that the amount of space on an interior sector is the same as on an exterior sector, but this diagram depicts the structure of older hard drive platters. The concepts of sectors, clusters, and slack are, however, the same. Technology, especially with respect to storage devices, is advancing rapidly. For this reason, it behooves attorneys to retain the services of a computer forensics examiner as soon as practicable.

[18] Clusters may contain data other than "deleted" data. Electronic media, even when new, contain data. Data downloaded from the Internet, even inadvertently, may end up stored indefinitely in the "slack" or unallocated space.

[19] *See, e.g.,* Deborah Radcliffe, *Handling Crime in the 21st Century*, CNN.com (Dec. 15, 1998), www.cnn.com/TECH/computing/9812/15/cybersleuth.idg/; John Ashcroft, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, U.S. Dep't of Justice, Office of Justice Programs, Inst. of Justice (Apr. 2004); Gov't's Opposition to Standby Counsel's Reply to the Government's Response to Court's Order Computer and E-Mail Evidence, *United States v. Zacariah Moussaoui*, No. 01-CR-455-A (E.D. Va. Dec. 30, 2002).

[20] Rule of Professional Conduct 4-1.1, requires that lawyers "provide competent representation," which "requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." One of the comments to this rule states: "Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge."

[21] *See XPEL Technologies Corp. v. Amer. Filter Film Distributors*, No. SA-08-CV-0175 XR, 2008 WL 744837 (W.D. Tex. Mar. 17, 2008). Under the terms of the order, the plaintiff's computer forensics expert was allowed to make mirror images of the defendants' computers and other electronic storage devices.

[22] *See, e.g., Lockheed Martin Corp. v. L-3 Communications Corp.*, No. 6:05-cv-1580-Orl-31KRS, 2007 WL 2209250 (M.D. Fla. July 29, 2007) (evaluating the burdensomeness of recovering information from the unallocated space on former employees' hard drives).

[23] *Id.* at *6. The magistrate judge ordered Lockheed Martin to produce documents recovered from the unallocated space of hard drives. *See id.* at *11.

[24] *See Cache la Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 624 (D. Colo. 2007).

[25] *See id.*

[26] Wiping clean the hard drives of departing employees is an effort to accommodate the fact that information remains on work station hard drives even if each employee consciously saved data only to the server. Discarding or passing along work station hard drives without writing over the data numerous times, that is, "wiping" the hard drives, risks disclosure of confidential information.

[27] *Cache la Poudre*, 244 F.R.D. at 636.

[28] For a discussion of why electronic discovery is such a problem for most companies, *see Top Ten Reasons e-Discovery is a Major Headache for Most Companies and Lawyers*, http://ralphlosey.wordpress.com/2007/06/07/top-ten-reasons-e-discovery-is-a-major-headache-for-most-companies-and-lawyers/.

[29] *See, e.g., Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228, 239 (D. Md. 2005) ("'The cost of responding to a discovery request can be in the millions of dollars if several years' worth of archived e-mail and files must be located, restored, sorted through and cleansed to remove non-relevant confidential material.'") (quoting Linda Volonino, *Electronic Evidence and Computer Forensics*, 12 Comm. of the Ass'n for Info. Sys. 14 (Oct. 2003),

available at http://cais.isworld.org/articles/12-27/article.pdf)).

[30] *See Phoenix Four, Inc. v. Strategic Resources Corp.*, No. 05 Civ. 4837(HB) 2006 WL 1409413 (S.D.N.Y. May 23, 2006).

[31] *See id.*

[32] *See id.*

[33] *See id.*

[34] *Id.* at *5.

[35] *Id.* at *6-7 (emphasis added).

[36] *Id.* at *14 (emphasis added).

[37] *Qualcomm Inc. v. Broadcom Corp.*, No. 3:05cv1958-B (BLM) (S.D. Cal. Aug. 6, 2007) Doc. No. 593, at 3.

[38] *Id.* at 2-3.

[39] *See Qualcomm Inc. v. Broadcom Corp.*, No. 3:05cv1958-B (BLM) (S.D. Cal. Oct. 29, 2007) Doc. No. 715).

[40] *See Qualcomm Inc. v. Broadcom Corp.*, No. 3:05cv1958-B (BLM) 2007 WL 43451017 (S.D. Cal. Dec. 11, 2007).

[41] *See Qualcomm Inc. v. Broadcom Corp.*, No. 3:05cv1958-B (BLM) 2008 WL 638108 (S.D. Cal. Mar. 5, 2008).

[42] *See, e.g., Hopson*, 232 F.R.D. at 235. (stating that even if nonwaiver agreements are enforceable as to the parties entering them, "it is questionable whether they are effective against third-parties") (citing *Westinghouse Elec. Corp. v. Rep. of the Philippines*, 951 F.2d 1414, 1426-27 (3d Cir. 1991) (agreement between litigant and DOJ that documents produced in response to investigation would not waive privilege does not preserve privilege against different entity in unrelated civil proceeding); *Bowne v. AmBase Corp.*, 150 F.R.D. 465, 478-79 (S.D.N.Y. 1993) (nonwaiver agreement between producing party in one case not applicable to third party in another civil case)).

[43] *See, e.g., Martin Marietta*, 856 F.2d 619, 621-23 (4th Cir. 1988).

[44] S. 2450, 110th Cong. (2007) ("A bill to amend the Federal Rules of Evidence to address the waiver of the attorney-client privilege and the work product doctrine," was introduced to the Senate Committee on the Judiciary on December 11, 2007).

D. Patricia Wallace *is an attorney with the Fort Lauderdale firm Walter J. Mathews, P.A. Her practice focuses on federal litigation and state and federal appeals.*

Journal HOME

[Revised: 08-19-2010]