by Donald A. Wochna, Esq.

Request for Production of Documents Can be a ***Technology Trap***

*T*raditionally, litigators obtain relevant documents from their opponent by issuing a *Request for Production of Documents*. Although the Rules of Civil Procedure mandate the disclosure of relevant, non-privileged documents1, it is a rare case in which an opponent copies all relevant documents and provides them in response to the first request. Usually, counsel must make several phone calls, write letters, monitor the partial responses provided and constantly work to obtain as complete a production of documents as possible.

Invisible Documents

The use of computers to create, process and store data has placed additional burdens on attorneys. Attorneys now must understand some basic computer concepts in order to determine whether they are receiving a proper production of documents. For example, most attorneys know "deleting" a document does not remove the document from the computer's hard drive. The document remains stored on the computer, but is merely rendered "invisible" to the operating system. Because deleted documents are "invisible" to a computer's operating system, a party cannot produce deleted documents in response to a request for production of documents. In the past, therefore, deleted documents have usually been ignored and left behind; notwithstanding the fact they were discoverable.

Deleted documents are not the only data that can be rendered invisible to a computer's operating system and thereby left out of a standard production response. It is very common to have documents created on a computer using a program that, at the time of the document request, can no longer read the documents. Accounting programs, for example, are updated each year. Some updates are not "legacy," meaning the updated program cannot read and interpret old files. In some cases the program used to create relevant files has been removed from the computer and the computer simply cannot open or read those files. All this data is invisible to the operating system, insofar as this data will not be retrieved when searching the system for documents responsive to a document request.

Data with an inaccurate file extension is also "invisible" to the operating system. Simply changing the extension associated with a file (for example changing ".doc" to ".jpeg") will render the contents of the ".doc" file unintelligible to the operating system. This technique is a favorite amongst users trying to hide data. In some cases these users also save the file (with an inaccurate extension) in a folder used by the operating system, where one would normally never look for documents and data. This data will not be produced in response to a document request.

Data that was never "saved" as a file by a user is also "invisible" to the operating system. Many attorneys are surprised to learn that a computer's operating system automatically saves data by writing it to the hard drive without any input from the computer's user. Almost all users, however, have seen this feature work, such as when a user recovers from a transient power loss that occurred while creating a brief or memo. When power is restored and the computer is re-booted, the operating system will automatically ask whether the user wishes to open the document that was being created when the power failed. This "retrieved" document will be available, even though the user had not saved the work. The "retrieved" document was created by the operating system, which automatically saved the work. If the user elects to ignore this "retrieved" document, the document remains on the hard drive, but is thereafter ignored by the operating system.

A computer's operating system also renders invisible large amounts of data used by the operating system to perform functions. For example, when printing documents, the operating system copies the data into a "spool file" – a file the system will use to print, and afterwards ignore. After printing the documents, a copy of them will remain in the spool file. Similarly, the operating system creates (and subsequently ignores) thousands of temporary, cache, buffer files and other types of data used by the system to perform various functions. This data is generally referred to as "artifacts" and can be analyzed to determine the manner in

which a computer was used. For example, operating system artifacts can prove a user improperly copied customer lists to a floppy drive prior to leaving a company. Artifacts could also prove that a user had removed a hard drive from a system at a time when the user knew of pending litigation.

None of the data discussed above will be produced in response to a request for production of documents where counsel has requested "documents" that can be retrieved from only the active files on a computer system. If counsel's definition of documents only relates to information visible to the computer operating system, then counsel has not requested any of the other discoverable data available on the hard drives of relevant computers. While all this information (visible and invisible) is all discoverable, it is usually simply left behind on the hard drives of the relevant computers. Additionally, "invisible" information is being overwritten through the normal use of the computer system. "As a computer is used in the normal course of business, the operating system overwrites all forms of data, including data relevant to the Plaintiff's claims or the Defendant's defenses." *Antioch v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D.Minn. 2002).

How important is this invisible data? Experienced litigators know the way in which an opponent has used computer systems often provides a road map that proves essential elements of tortuous conduct. Discovering the substance of deleted documents, instant messages, emails, etc. often provides a treasure-trove of statements that support or contradict essential legal theories or strategies in a case.

Although attorneys agree it would be very desirable to discover this data, most litigators have never tried to do so. This was because until very recently case law related to production of documents did not seem to easily apply to data created, processed, and stored on computers. There was no set of procedures and protocol an attorney could follow similar to the procedures related to requesting production of documents. Additionally, it appeared to many attorneys that it was unrealistic to request access to an opponent's computers because to do so would be disruptive, burdensome, over broad, costly and in violation of privilege. Attorneys did not want to incur substantial research, time and effort in motion practice to compel access where such motion did not seem likely to be granted. Most attorneys agreed if they could economically obtain all the data related to a case (visible and invisible to the computer), without spending significant time and effort in motion practice or getting lost in the technical world of "computer-speak," they would pursue the production of all such data.

Discovery of All Data - Visible and Invisible

Within the last few years, federal and state courts have recognized technology and protocol that permits discovery of all relevant data, including the data rendered invisible to a computer's operating system.

- *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002). "[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable."
- *Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 427-431 (S.D.N.Y. 2002). Stating, "[E]lectronic documents are no less subject to disclosure than paper records," and only questioning which party should bear the cost of such discovery, especially for backup tapes or deleted e-mails.
- *McPeek v. Ashcroft,* 202 F.R.D. 31, 34 (D.D.C. 2001). Stating, "[D]uring discovery, the producing party has an obligation to search available electronic systems for information demanded," and ordering a limited backup restoration of e-mails.
- *Kleiner v. Burns*, 48 Fed. R. Serv. 3d 644, 2000 WL 1909470 (D. Kan. Dec. 15, 2000). Noting that Rule 26(a)(1)(B) requires description and categorization of computerized data, including deleted e-mails, and stating that "[T]he disclosing party shall take reasonable steps to ensure that it discloses any backup copies of files or archival tapes that will provide information about any 'deleted' electronic data."
- *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000). "First, computer records, including records that have been 'deleted,' are documents discoverable under Fed. R. Civ. P. 34." Citing *Crown Life Insurance Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993); *Illinois Tool Works, Inc. v. Metro Mark Products Ltd,* 43 F.Supp.2d 951 (N.D. Ill. 1999).
- *Playboy Enter. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999). "Plaintiff needs to access the hard drive of Defendant's computer only because Defendant's actions in deleting those e-mails made it currently impossible to produce the information as a 'document.'" *Anti-Monopoly, Inc. v. Hasbro, Inc.* WL 649934 (S.D.N.Y., Nov. 3, 1995); *Seattle Audubon Society v. Lyons*, 871 F. Supp. 1291 (W.D. Wash. 1994); *Linnen v. A.H.Robins, Co.* WL 462015 (Mass. Super., June 16, 1999); *Crown Life Insurance Co., v. Craig* 995 F.2d 1376 (7th Cir. 1993).

Simply stated, attorneys can now obtain all relevant data in one simple, economical process, that is non-disruptive, properly limited to relevant data and protecting privilege. Fortunately, the process is very similar to that used by attorneys to request production of documents. *Simon Property Group v. mySimon, Inc.* 194 F.R.D. 639, 2000 U.S.Dist.LEXIS 8950 (S.D.Ind. 2000); *Playboy Enter. v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999).

The process begins by either (1) substituting for a traditional document production request, a request to produce the hard drives of relevant computers or (2) serving a traditional request for production of documents drafted to define document as any medium upon which intelligence or information is recorded or from which intelligence or information can be recorded, retrieved or perceived, with or without the use of detection devices, including detection devices other than the operating system and programs installed on any of defendant's computers. Note that the definition of document focuses upon the substance carrying the data. Paper, for example, is a medium on which data – intelligence or information – is recorded and from which the data can be perceived by reading. Similarly, a hard drive in a computer is a medium on which is recorded data in the form of polarized, magnetic particles, that can be perceived (i.e. understood) using a computer as a detection device. This definition includes data that cannot be recognized using the producing party's computers. Courts have recognized, however, this data can be perceived using programs and software tools available to a computer forensic expert. . "Judges are getting the message. It makes more sense to look to one neutral expert, with the appropriate protocols, rather than relying on the parties to do it and duplicate their expense and effort." *Playboy Enterprises, Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D. Cal. 1999). *Simon Property Group v. mySimon, Inc.* 194 F.R.D. 639 (S.D.Ind. 2000).

Using specialized forensic software tools, a forensic expert first makes a "clone" of those computers used by a party to create, process, store, archive or otherwise manipulate data related to a particular case. These are the "relevant computers" in a case, and identifying them at the onset of litigation is the common objective of all parties and their attorneys. At the moment when a party knows or should know that litigation is anticipated, that party has a duty to preserve electronic evidence and prevent its spoliation. Continuing to use computers on which resides visible and invisible data relevant to a matter overwrites the data and causes spoliation. Thus, in order to prevent the spoliation of evidence, the parties must identify the relevant computers and thereafter take action to preserve the evidence on the relevant computers. (*Antioch*, supra.) Preventing spoliation can be accomplished by refraining from using relevant computers or by creating a forensic image of each of these computers. Because it is rarely acceptable to refrain from using relevant computers, litigants most often resort to forensic imaging.

A ***forensic image*** contains all the data—visible and invisible—that is resident on the relevant computers' hard drives. Once a forensic image of each relevant hard drive is created, the computer can be returned to service because all the data has

Continued on page 37

Continued from page 27

cutting edge

been "frozen" on the forensic image. The forensic image is an electronic "snapshot" of each of the relevant computers.

Making a forensic image requires a computer forensic expert be granted access to the subject computer's hard drive for four to six hours. Access can be provided on-site, at a lawyer's office, home or any location convenient for the producing party. To avoid disruption, access is usually granted at night, over a weekend or during non-business hours. The forensic expert will attach to the subject computer a "write-blocking" device which prevents any data from being written to or changed on the subject drive, while an exact, bit by bit image is copied onto a drive supplied by the forensic expert. If several relevant computers are involved in a matter, they can all be imaged simultaneously – so making a forensic image of many computers can be accomplished in less than eight hours. The producing party and its counsel can observe the creation of the forensic image.

The last step in creating a forensic image is to verify the image. Verification is the process that embeds into the image a "digital DNA marker," termed an "MD5 Hash Value." This value can be used to prove the forensic image has not been altered in any fashion whatsoever from the time of its creation. *State v. Cook* 149 Ohio App.3d 422 (2nd Dist. Mont. County, 2002).

After forensic clones are made of each of the relevant computers, they are then simultaneously connected to a forensic lab computer to be electronically searched. Electronic searching is conducted by the forensic expert using powerful searching software that identifies and extracts only relevant data. No "fishing expedition" is conducted by randomly opening files or folders hoping to stumble across something relevant. Because relevant data is identified electronically, no person will ever view any data that is not related to the litigation.

Once relevant data has been extracted it can be compiled, parsed and arranged so that the data intelligently reflects the issues in a case. At this point, the relevant data is usually placed into a report that can be read using a word processor. The report will contain exact copies of all relevant data including all deleted email, letters, memos, instant messages, etc. The report is then presented to counsel for the producing party so that counsel can redact the data for privileged matter. After redacting the data and creating any applicable privilege logs or reports as required by the court, the producing party provides the data to the requesting party.

The requesting party will receive all relevant data, including all data hidden, deleted or otherwise rendered invisible to the computers of the producing party. The requesting party will receive, therefore, all the documents that would have been produced in the traditional manner, plus all documents and data that could not have been copied from the computers of the producing party. See, for example, the decisions of *Simon Properties, Playboy vs. Welles, Antioch vs. Scrapbook*, cited herein.

This process is very quick. Imaging is usually accomplished in a matter of hours. Using software to electronically search and extract relevant data is completed within seven working days, including about 25-30 man hours to analyze, parse and compile the search results (this takes more time for cases where artifacts must be analyzed to determine the manner in which te computer was used). An initial report can be delivered electronically to counsel for the producing party, and is usually redacted in 10 days. In almost all cases litigators can have all the relevant facts within three to four weeks from the date of access to the computers.

The process is very economical. Usually the time spent on discovery disputes is reduced, while costing about 10 percent of the total legal fee incurred in a case.

Donald A. Wochna, Esq., is co-founder of Vestige, Ltd., a provider of computer forensics and electronic discovery services to the legal community. For more information go to ***www.vestigeltd.com.***