

YOU GET WHAT YOU ASK FOR: USING DOCUMENT\ PRODUCTION REQUESTS IN THE COMPUTER AGE

The widespread use of computers has caused some attorneys to recognize a problem with the traditional Request for Production of Documents. The problem relates to the manner in which computers operate and store data. Basically, because computers cannot “see” data that has been deleted, hidden, or rendered invisible by several means, the scope of the definition of documents in a traditional Request for Production of Documents does not include this valuable, discoverable data. The problem is significant because a client may not understand why relevant data was not discovered by its attorney simply because the data had been “deleted” or otherwise rendered invisible; especially in light of case law that supports the safeguarding and discovery of all data, visible and invisible, resident on computer systems.

An instructive comparison of two cases highlights the problem: a request for production of documents can usually be satisfied by the respondent producing only the data “visible” to its computer system, resulting in a lost opportunity to discover all relevant data. Bethea v. Comcast et al. 218 F.R.D. 328, 2003 U.S. Dist. LEXIS 21595, 57 Fed. R. Serv.3d (Callaghan) 428 (D.D.C., December 3, 2003) and Antioch vs. Scrapbook Borders, Inc., 210 F.R.D. 645, 2002 U.S. Dist. LEXIS 20811 (D.Minn. 2002).

BETHEA. Request for Documents at end of discovery

In an employment discrimination case, the United States District Court for the District of Columbia, Magistrate John M. Facciola, denied Plaintiff Valerie Bethea’s motion to compel defendant Comcast Inc, her former employer, to permit plaintiff to enter defendant’s premises, inspect its computer systems and related programs, and copy relevant information. The Motion to Compel was filed after plaintiff had served a traditional Request for Production of Documents and Defendant had responded. Bethea at p.330. Plaintiff did not contest Defendant’s response, nor did Plaintiff claim that Defendant had wrongfully withheld documents. Rather, plaintiff was concerned that only so few documents were located.

We [Plaintiff] would like to inspect the computer and make another request for some additional documents just to see if the defendants are going to say that there are no documents that exist which we are requesting... We just can’t believe that an organization of that magnitude could go through a reorganization and would not create one single document.

Id. At 329.

Magistrate John M. Facciola analyzed the Plaintiff’s motion as follows:

When a party seeks to compel discovery, it first has the burden of demonstrating the relevance of the information to the lawsuit. Alexander v. FBI, 194 F.R.D.

305, 311 (D.D.C. 2000). In the context of computer systems and computer records, inspection or seizure is not permitted unless the moving party can ‘demonstrate that the documents they seek to compel do, in fact, exist and are being unlawfully withheld.’ Id. As indicated by this court and other courts, a party’s suspicion that another party has failed to respond to document requests fully and completely does not justify compelled inspection of its computer systems. See Id.; see also Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc., 2003 U.S. Dist. LEXIS 5606, No. 01 C 9148, 2003 WL 1809465, at *2 (N.D.Ill Apr. 4, 2003).

Bethea at 329-330.

Magistrate Facciola denied plaintiff’s motion to compel on the ground that plaintiff had not demonstrated any relevance for the information still contained on defendant’s hard drives, and failed to show that the additional documents actually exist or that defendants have unlawfully failed to produce them. Id.

ANTIOCH: Request to Interrogate Hard Drive

In contrast to the results in Bethea, the United States District Court for the District of Minnesota, Magistrate Judge Raymond Erickson, granted Plaintiff’s Motions for Expedited Discovery and to Appoint a Neutral Computer Forensic expert filed in the case at a time prior to the commencement of discovery under the federal rules. Early in this copyright infringement case, prior to any Scheduling Order, and prior to the commencement of formal discovery pursuant to Rule 26, Federal Rules of Civil Procedure, plaintiff filed its motion seeking an order compelling the defendants to produce computer equipment for the purposes of investigation, copying, imaging, and interrogation, by a Court-appointed computer forensic expert. Antioch at 16.

Magistrate Erickson granted plaintiff’s motion on the ground that defendants used computers to create and read email, and that the plaintiff’s expert testified by affidavit that **“data which is deleted from a computer is retained on the hard drive, but is constantly being overwritten by new data, through the normal use of the computer equipment”**. Antioch at 651.

Accordingly we conclude that the Defendants may have relevant information, on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the Plaintiff’s claims, or the Defendants’ defenses. **This information may be in the form of stored or deleted computer files, programs, or e-mails, on the Defendants’ computer equipment. (emphasis added).**

Antioch at 652.

The Magistrate ordered the creation of a forensic image of the Defendants’ computer hard drives and an analysis following the protocol set forth in Simon Property Group L.P.

v. mySimon Inc., 194 F.R.D. 639, 640 (N.D.Ill. 2000). He based his decision on the “well accepted proposition that deleted computer files, whether they be emails or otherwise, are discoverable. See, Rowe Entertainment, Inc. v. The William Morse Agency, Inc., 205 F.R.D. 421, 427, 431 (S.D.N.Y. 2002); McPeck v. Ashcroft, 202 F.R.D. 31, 31, 34 (D.D.C. 2001); Kleiner v Burns, 2000 U.S. Dist. LEXIS 21850, 2000 WL 1909470 (D.Kan. December 15, 2000); Simon Property Group L.P. v. mySimon, Inc. 194 F.R.D. 639, 640 (N.D.Ill. 2000); Playboy Enterprises v. Welles, 60 F. Supp.2d 1050, 1053 (S.D.Cal. 1999).

ANALYSIS:

These two cases can be reconciled if one remembers that a computer hard drive is comprised of two separate and distinct types of data: data that can be read by the operating system (visible), and data that cannot be read by the operating system (invisible). Computer forensic analysis is required where you want to access both types of data. (For a discussion of the significance of “invisible” data, see).

It is beyond serious debate that rendering data invisible does not remove the data from the scope of discovery. Thus, deleting emails, for example, renders the email “invisible” to the operating system, but does not remove the email from the scope of discoverable data on a computer hard drive. This result satisfies our common sense that evidence cannot be rendered non-discoverable by the mere expedient of a quick finger on the “delete” key. Similarly, hiding data by changing its file extension, or rendering data “invisible” by updating, modifying, or uninstalling the program needed to read the data, does not place the data outside the scope of discovery. Additionally, the normal use of the computer system overwrites “invisible” data, threatening the ongoing destruction and spoliation of evidence.

None of these computer-related facts, however, are relevant in those cases in which counsel for the requesting party only requests visible data, i.e. data that can be accessed and printed or copied by the responding party’s computer systems. Although the producing party will not access nor recover any invisible data, such as deleted, orphaned, hidden, or residual data, it is not required to do so by the terms of the Request for Production of Documents. This is the result in cases similar to Bethea. In these types of cases, absent proof that the responding party withheld visible data from production, the requesting party is not entitled to access the responding party’s computers.

In cases such as Antioch, however, in which the requesting party has sought to protect and interrogate **visible and invisible** data, the producing party cannot respond by accessing only the data that is “visible” to the operating system. In fact, as properly stated in Antioch, the continued use of the producing party’s computers is a threat to the integrity of the invisible data. In these types of cases, discovery of relevant data and prevention of spoliation of evidence requires that a forensic “snapshot” be created of relevant hard drives. This forensic snapshot can then be searched and analyzed in accordance with protocols that protect privilege and confidentiality.

The lesson of Bethea and Antioch seems clear: you only get what you ask for. If counsel only asks for active, visible documents, then that is all the producing party must provide. This is especially true today, as the costs of extracting invisible data by forensic analysis has significantly decreased and federal and state courts have recognized the universal application of forensics.

The rules (of Civil Procedure) talk about the production of relevant information, so we seem to create the burden to seek e-data...**I can't imagine how counsel who is responsible cannot seek relevant electronic information.**

Judge Loretta Preska, U.S. District Court, S.D.N.Y; "How a Judge Expects You To Handle Electronic Records in Discovery", July,2003.

Lawyers who forsake electronic discovery on behalf of a client due to costs, come close to professional negligence.

Comments of Magistrate Judge John M. Facciola, U.S. District Court, D.Col., author of McPeck vs. Ashcroft, 212 F.R.D.33 (D.D.C., January 9, 2003) at seminar "How a Judge Expects You To Handle Electronic Records in Discovery", July 2003.

The challenge for litigators is to explain to clients that it is necessary in litigation to discover all the facts that relate to claims and defenses, including data that has been deleted, hidden, or otherwise rendered invisible. Usually informed clients readily agree that this type of data will be needed in a case. In all cases, counsel ought to document that the client was advised about the need to discover this data.