

What Jefferson Taught Us

Forget the money in the freezer. The real lessons of the FBI search of the congressman's office developed after the government couldn't review what it found.

By KENNETH A. MENDELSON

When the U.S. Court of Appeals for the D.C. Circuit recently ruled that the FBI had to return all legislative material seized during the raid on the Capitol Hill offices of Rep. William Jefferson (D-La.), little attention was paid to the large volume of information stored on the computers in Jefferson's offices that did not have to be returned.

Citing the "speech or debate" clause of the Constitution, the court held that the FBI overreached its authority by seizing legislative data. Nevertheless, the court found that

■ IN-HOUSE COUNSEL ■

the copying of computer hard drives and other electronic media was "constitutionally permissible" because Jefferson will have a chance to show that the electronic information from his congressional office computers is connected to his legislative work and therefore subject to constitutional protection.

The result is that the courts created a conundrum in which the FBI may seize electronic information but is not permitted to review it until Jefferson had the chance to look at it to determine whether or not it is legislative.

PUTTING THE TOOTHPASTE BACK IN

Attorneys with experience dealing with large amounts of electronic data in the discovery phase of litigation may be scratching their heads trying to figure out how Jefferson and his attorneys were able to review the electronic information after it had been seized. In a July 2006 appellate court ruling, the task, seemingly akin to trying to put toothpaste back in the tube, was remanded to U.S. Magistrate Judge John Facciola, a noted expert in the burgeoning field of e-discovery. The result of that process, which was affirmed by the recent decision, may serve as a cost-effective solution for any litigation that requires addressing issues related to how to produce or withhold potentially privileged electronic information.

At some point in most litigation matters, attorneys and their clients must come to terms with the fact that the volume of electronically stored information is going to be larger than anyone imagined, and the cost of reviewing it will probably exceed

any prediction. Add to that the likelihood of intermingled privileged, sensitive, and proprietary information with the electronic information, and the time and effort required to segregate electronic information can give any client sticker shock.

Although most attorneys will likely never have to assert speech or debate privilege, virtually all litigators will have to address attorney-client and other forms of privilege issues that arise during the discovery phase in both civil and criminal litigation, and those issues can become a financial showstopper when large amounts of electronic information are at issue. In litigation, compromise is almost always reluctantly achieved by the parties or required by the court.

However, the procedures used in the Jefferson case were reasonable and effective, and may provide a model for resolution of privilege review of large volumes of electronic information, even when the issues at stake are not rarefied constitutional ones. At the same time, parties can reduce costs, save time, and permit the focus of the litigation to remain on the merits of the case rather than on the distracting ancillary issues that often take up a disproportionate amount of attorney time and client dollars.

THE JEFFERSON PROCESS

In the wake of the July 2006 remand order, the Department of Justice and Jefferson's attorneys agreed to hire Stroz Friedberg, our consulting firm, which specializes in digital forensics and electronic discovery to act as a neutral third party and facilitate the searching and review of the material. The Justice Department would establish the parameters of the search, while preserving Jefferson's ability to review the search results and assert privilege claims before material was released to Justice Department attorneys.

In consultation with the parties, we drafted and submitted a protocol that specified the creation of duplicate forensic images made from the images created by the FBI in the search. We then oversaw the FBI making the duplicate images, and performed the filtering and keyword searching according to the government's specifications. By reviewing statistics of the preliminary searches, the Justice Department could then revise the search parameters by modifying or

removing keywords that caused large numbers of potentially false positive “hits.” We then produced data according to the specifications agreed to by the parties. In this case, the form of production was to be both hard copy (printed documents) and electronic (.pdf versions of the documents).

On a rolling basis, we delivered to Jefferson’s counsel the equivalent of about one banker’s box of Bates-numbered paper documents and a CD-ROM containing the electronic versions of the provided documents. Jefferson’s attorneys had two business days to review the documents and to file a motion with the court to assert privilege over those documents specified by Bates number only.

Upon receipt of a copy of the motion, we redacted the identified documents from a second box of identical documents and created a new CD-ROM without the specified electronic versions. Each redacted set would be delivered to the Justice Department attorneys for review. This process continued until all nonprivileged documents meeting the search criteria were produced to Justice.

The procedure used in the Jefferson case was straightforward, confirmed in a consent order, and kept the discovery process moving forward. A trustworthy consultant that provides assurance to all parties and the court, and the expertise to both construct and implement a workable, fair protocol, goes a long way to making this procedure a viable option in virtually any litigation in which large volumes of electronic information must be reviewed for privilege.

So how does this apply to other cases? At the earliest stages of litigation, the parties should agree on the data to be preserved, the storage media it will come from, and the method of preservation. Usually by this time, a “litigation hold” will have been issued, directing individuals with potentially relevant information to preserve data. At the same time, the organization must consider a systematic approach to collecting, reviewing, and producing preserved data that will withstand scrutiny as to its completeness.

Forensic preservation of electronic information is the “gold standard” that may not be necessary in every case. Forensic preservation means the verifiable “bit-for-bit” copying of electronic information, including metadata, deleted files, slack space, or unallocated space, and avoids the inadvertent modification or destruction of data that may occur simply by copying files from one place to another. Preserving electronic information forensically is a stake in the ground to which a party can tie claims of good faith, since taking this step reduces the viability of allegations that data was not handled properly, or that spoliation occurred due to bad faith or a lack of diligence.

Forensic preservation of electronic information and the extraction of relevant data according to an agreed-upon procedural protocol also goes a long way toward minimizing claims of discovery abuse. This approach assures that the results are the product of the neutral application of search criteria, unaffected by any bias of the party or reviewer.

WHAT TO DO

A procedural protocol that lays out what will be done to what data includes:

- What electronic information will be forensically preserved (such as server data, e-mail, laptops, PDAs), with a general description of the method to be used.
- General specifications for how the data will be handled, searched, refined, and delivered, including data types, date ranges, keywords, and other filters. This will also describe how to handle unsearchable documents, such as images and audio files, and whether unallocated space and slack space (areas of the hard drive not typically accessible by the computer user, but which may contain relevant data) will be searched.
- Time frames or schedules for review of the data by the owning party, and how it will be turned over to the other side.
- Creation and submission of a privilege log, and how nonprivileged items will be redacted and delivered.

The consultant will also prepare a second, more detailed protocol that is essentially a step-by-step procedure to be used by forensic examiners and technicians in their work. The detailed protocol will describe with specificity the tools to be used, how they will be employed, and the process to be used in the creation of any material. These are not “click-by-click” instructions, but are sufficiently detailed to permit another examiner to achieve identical results using the same raw data, tools, and search specifications.

While the cost of forensic consultants and e-discovery can be significant in the short term, an agreement to use this process early in the litigation may drastically reduce the overall cost of the litigation. Reducing the volume of electronic information through targeted filtering will significantly lower the cost for both sides. By stipulation or by court order, the focus of the litigation can remain on the merits of the case, rather than on the elements of discovery.

Perhaps less obvious, but no less significant from a cost reduction standpoint, is the fact that file types known to be irrelevant (media files, images, .mp3 music files) can be filtered out before production, eliminating a time consuming diversion from the initial review process. Since the data has been preserved, any of these files can be identified and produced later, if analysis of the data indicates that a redacted file may be relevant.

Finally, data can be produced on a rolling basis according to priorities agreed upon by the parties before production begins. Early focus on “low-hanging fruit” often obviates the need for more expensive processes (such as backup tape restoration) later in the case.

With the cooperation of the parties, the guidance of the court, and the expertise of a digital forensics firm, the Jefferson matter produced an expeditious and effective solution for dealing with privilege issues involving electronic information. While the constitutional privilege issues raised may be unique, the legacy of this case regarding the discovery of electronic information has broader application.

Kenneth A. Mendelson is managing director of the Washington, D.C., office of Stroz Friedberg, an electronic discovery services firm.