

INVESTIGATIONS & COMPUTER FORENSICS

ALM

HTTP://WWW.NYLJ.COM

TUESDAY, MAY 30, 2006

Think of the **Corporate** Office As a Potential **Crime** Scene?

*That's how prosecutors and regulators see it.
Pay attention to chain of custody, and
preservation of identical documents.*

**BY RONALD L. MARMER
AND ANDREW WEISSMANN**

SINCE THE DEMISE of Enron in the winter of 2001, prosecutors around the country have devoted much attention to white collar investigations and prosecutions. And with the advent of these sophisticated white collar investigations, as well as the rapid demise of Arthur Andersen LLP, much attention also has been paid by companies and their counsel to document retention policies—what should be saved, how it should be saved, and when it should be saved.

Less attention has been devoted to the production of documents in such cases. A gap often exists between the expectations of the government and corporations when it comes to document production. Failure to understand the world views of prosecutors and regulators can lead to corporations making decisions they later may regret.

When a corporation and its employees become the subjects or targets of a governmental investigation, whether by the Department of Justice, the Securities and Exchange Commission, or other regulators, trained investigators will look at the office as a potential crime scene. This is particularly true with respect to

Ronald L. Marmor is a partner in the New York and Chicago offices of Jenner & Block. **Andrew Weissmann**, a partner in the firm's New York office, is the former director of the government's Enron Task Force and was lead attorney in the trial of Arthur Andersen, discussed in this article.



ART BY ISTOCK/DIGITALVISION

criminal investigations, where the focus is on evidence of individual liability—the actions and intent of corporate employees.

Indeed, even where the corporation itself is in the government's crosshairs, it is only through the actions of its employees that the company can be held criminally liable. Thus, the location of documents in a particular office or on a specific computer will be an important source of

evidence for the criminal prosecutor in order to determine the knowledge and intent of a corporate employee.

The problem, of course, is that none of us thinks of our office as a potential crime scene. Prior to Enron, the typical investigation would be civil or regulatory in nature, and the willfulness of individual employees was far less frequently the center of attention.

Even post-Enron, depending on the timing of an investigation, the corporation may have little reason to be thinking about preservation of crime scene evidence in an employee's office. Typically, corporate counsel will be tasked with undertaking an internal investigation into an allegation of employee misconduct as a result of one of two events: either the company has itself uncovered a potential issue, or the company learns of the issue from a governmental source, often in the form of a subpoena or request for documents. In either case, the manner of documenting what is found in a particular office can be crucial, but can be overlooked by an internal investigation.

The two problems discussed below—recording the chain of custody of data, and preservation of seemingly identical copies—are quite different depending on whether one is dealing with hard-copy data or electronic information. Here, for once, electronic data has a distinct advantage, as will be seen.

Harvesting Documents

The first problem often occurs in the manner of harvesting documents for review by company counsel, whether internal or external.

It is customary for counsel for large corporations to have the individual employees themselves collect relevant hard-copy documents from their own offices after receiving instruction, usually in the form of an e-mail, regarding what to collect. An employee may then send responsive material through interoffice mail or provide it to a paralegal or even, in a significant matter, to an attorney.

The manner of documenting the chain of custody of documents culled from an individual office may be of great importance later to governmental investigators and, consequently, the paralegal or attorney may now be a witness. The prudent corporation, keeping an eye on the fact that it may seek to prove its good corporate citizenship down the road or may itself want to prove chain of custody, will document the chain with respect to such harvesting, leaving as little as possible to individual employees—who may not be available to the corporation if an investigation later targets them.

It is far easier to avoid the pitfalls inherent in hard-copy data collection when harvesting electronic data.

In many large corporations, collection of such electronic data is performed centrally, and not left to individual employees. And computer forensics frequently enables one to examine metadata to determine the history of access to, and alteration of, a particular electronic document. Computer forensics also may allow recovery of seemingly deleted electronic records. Indeed, even when harvesting an employee's hard drive or other electronic media, such as Palm Pilots, the data itself will likely identify the user and will make the problem of tracing the evidence to a particular employee far easier to accomplish than with hard-copy data.

'Identical' Copies

In large document harvesting cases, seemingly identical copies of hard-copy and electronic documents are often ignored. Disregarding such material may seem entirely rational as it reduces the time and cost of document review with no apparent downside. That, however, is not always the case. Production of such copies can be advantageous to both the government and defense.

The production of copies was addressed in the much-cited decision from the Southern District of New York, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003). In *Zubulake*, Judge Shira Scheindlin set forth a series of standards to guide companies with respect to document preservation.

Zubulake, who had brought suit for gender discrimination and retaliation, sought sanctions against her employer for its failure to preserve documents. Specifically, *Zubulake* claimed that evidence that would support her claims would be contained in e-mails among various company employees. The defendant, however, failed to retain a subset of the relevant e-mails. The court found that the defendant's failure to retain a small subset of documents was "negligent and possibly reckless."

Of note for purposes of this article is the guidance the court gave for future litigation. Judge Scheindlin held that a party "must retain

all relevant documents (*but not multiple identical copies*) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter." *Id.* at 218 (emphasis supplied). The court did not offer any rationale for its pronouncement that identical copies need not be retained.

That language has led to parties failing to preserve evidence that later may be useful to government regulators and the company itself.

To the extent that "identical" refers to the document itself—as opposed to the document, location, and metadata associated with it—the *Zubulake* decision provides guidance that may be too narrow. For instance, where identical copies of a relevant document are located in the offices of employees who may be subjects or targets of an investigation, preservation of the identical documents and creation of a clear chain of custody regarding the location of each identical document can be critical. Corporations no less than

Seemingly identical copies of hard-copy and electronic documents can be advantageous to both the government and defense.

government investigators seeking to determine what an employee knew and intended will want an accurate record on which to base a judgment.

Similarly, corporations that choose to cooperate with government investigators may find it advantageous to be able to demonstrate that they have processes in place to enable outside regulators to assess individual liability.

The government's criminal prosecution of Arthur Andersen illustrates the relevance of copies of electronic data.

In *United States v. Arthur Andersen, LLP*, 374 F.3d 281, 298 (5th Cir. 2004), *rev'd*, 544 U.S. 696 (2005), Andersen was charged with obstruction of justice arising out of destruction of documents in the fall of 2001, seemingly in anticipation of an imminent SEC investigation. Because the partnership was charged, each Andersen agent's actions and intent were relevant in determining Andersen's criminal liability.

During the trial, Andersen claimed that the government had not established that documents of any note were destroyed. In response, the government pointed to an e-mail of an Enron internal accountant that had been sent to an Andersen employee and then deleted. The government argued that the content of the e-mail demonstrated "Andersen's adoption of a previously rejected accounting practice that allowed Enron to avoid a restatement of earnings." *United States v. Andersen*, 374 F.3d at 300.

Andersen noted, however, that a copy of that document was extant and, when Andersen was subpoenaed by the SEC for Enron-related documents, Andersen had produced that e-mail. Andersen thus objected to the government being allowed to argue to the jury that the e-mail was relevant to the obstruction charge, since a copy had been produced.

Both the district court and Fifth Circuit rejected that analysis (and that ruling was not appealed). The government argued that the deleted e-mail was relevant to show the actions and intent of an individual Andersen employee, even if not all copies of the e-mail had been destroyed.

The court agreed with the government's argument that "the destruction of a copy of an important document is significant because a copy could indicate who had the document, when the person received it, and whether the person destroyed it." *Id.* The deletion of a copy was thus used by the government, to show the actions of an individual employee, even though seemingly identical copies of the e-mail were not destroyed by other employees.

The same case provides an example of extant copies being used by the defense to counter government accusations.

Andersen sought to use the fact that numerous copies of documents were not destroyed—i.e., that little or no unique data were rendered unavailable to the SEC—in order to establish a lack of intent to obstruct the SEC. The defense argued, in short, that if there were a sincere attempt to shred documents to keep material from the Commission, one would expect the employees to have done a better job of sanitizing the record of offending material, and not left identical copies to be discovered by investigators.

The Court of Appeals found that such use by the defense of extant copies had undeniable relevance. *Id.* at 287-88. Thus, in *Andersen*, for both parties the existence and deletion of copies of documents were relevant and important.

Preserve Your Options

If the government is especially concerned about identical copies and chain of custody, it may, of course, seek a warrant to search the offices in question. A search enables the government to determine exactly what is located in a particular office, including original documents, and to take any precautions to preserve fingerprints.

But the government may not have probable cause to search, and even where it can meet this threshold, it so far has properly been reluctant to search the offices of a large on-going business in all but the most unusual cases. Instead, the government will resort to the use of a grand jury or civil subpoena. This practice may change, however, if the government is unable to overcome perceived errors by companies in harvesting responsive data.

The company that seeks to preserve its ability to cooperate fully with the government, or to use the existence of identical copies affirmatively in its defense, will accordingly need to see the workplace through the eyes of the criminal investigator—an office in which a crime may have occurred.

This article is reprinted with permission from the May 30, 2006 edition of the NEW YORK LAW JOURNAL. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit www.almreprints.com. #070-05-06-0043