Zubulake and the Duty to Preserve Electronically Stored Data

by Christopher B. Little

In 2002, Laura Zubulake sued her employer, UBS Warburg, LLC, for gender discrimination; eventually, she obtained a judgment in excess of $26 million.[1] Her employer and the attorneys for her employer did not adequately manage the disclosure and production of electronically stored information.

Zubulake I–V [2] is a series of cases that resulted in decisions by the federal district court in the Southern District of New York. These holdings, which deal with the preservation and discovery of electronically stored data, have been adopted into revised Rule 26 of the Federal Rules of Civil Procedure (Rules). The Official Comments for the 2006 Amendment state that Rule 26(a)(1)(B) is amended to parallel Rule 34(a) by recognizing that a party must disclose electronically stored information.

The *Zubulake I–V* opinions collectively suggest that it is incumbent on a party involved in litigation to maintain, preserve, and protect electronically stored evidentiary material that is relevant to the issues presented by a lawsuit. In these opinions, the trial court addressed the duty to avoid spoliation of evidence, as well as the duty to preserve e-mails and other electronically stored data. According to the court, at the point when one "reasonably anticipates litigation," a prospective party to litigation has an affirmative duty to (1) suspend its routine document retention and destruction policies; and (2) instruct employees to preserve any information that may be considered evidence in the case."[3]

The Sedona Principles

Storage and discoverability of electronic data are matters of significant import to the legal profession. Computers preserve information that users sometimes forget (and may not want to remember) ever existed.

The Sedona Conference, which comprises lawyers, jurists, and experts in matters related to antitrust law, complex litigation, and intellectual property rights, has dealt specifically with the issue of electronic information storage and has developed a "Working Group Series" that focuses on electronic document production and preservation.[4] In July 2005, the Sedona Conference produced "The Sedona Principles Addressing Electronic Document Production" (Sedona Principles). These Sedona Principles were updated in June 2007.[5]

The Sedona Principles recognize that electronic data storage is here to stay. Information stored electronically is discoverable and should be disclosed under Rules 26 and 34.[6] The Sedona principles require anyone storing electronic information to preserve it if and when litigation is anticipated or begun.

The accompanying sidebar contains a glossary of terms of art that litigators should understand before preparing a document retention letter and making Rule 26 disclosures. The terms in the sidebar evolved from the July 2005 Sedona Principles.[7]

Balancing Approach

There is a burden and cost associated with the production or disclosure of electronic information. Reading an opponent's e-mails might involve reviewing thousands of saved e-mails wishing happy birthday or offering condolences between friends—and may never reveal the "smoking gun" being sought. The Sedona Principles suggest a balancing approach of the cost, burden, and need for the information. The attorney should recognize the burden and cost of reading irrelevant information, and weigh that against the need for information relevant to the lawsuit.

The Sedona Principles require parties to litigation to confer early in the discovery process to discuss and compare the technological feasibility and realistic cost evaluation of recovering electronic data next to the nature of the litigation. If and when discovery of electronic information is sought, the request should be specific and the responses should disclose the scope and limits of what is being produced. The attorney also may be obligated to declare in a privileged

About the Author

Christopher B. Little is a director at Montgomery Little Soran & Murray, P.C.—(303) 773-8100, clittle@montgomerylittle.com. He specializes in representing lawyers who have been sued or who have been asked to respond to a professional conduct complaint.

This Department is sponsored by the CBA Lawyers' Professional Liability Committee to assist attorneys in preventing legal malpractice. The Department welcomes articles and ideas or suggestions for article topics. For more information, for writing guidelines, or to submit an article or topic suggestion, contact Andrew McLetchie—(303) 298-8603, a_mcletchie@fsf-law.com; or Reba Nance—(303) 824-5320, reban@cobar.org.

(confidential) log what is not being disclosed or produced (for example, the birthday greetings).

The Sedona Principles recognize that it may be impossible to recover every bit of electronically stored information. Computers get replaced, damaged, destroyed, or stolen. The Sedona Principles require a good-faith effort to locate and obtain the stored information, and are the backbone of the *Zubulake* opinions.

The *Qualcomm* Case

Zubulake established guiding principles for any litigator to follow when disclosing electronically stored information. Recently, those principles have been followed by a number of courts. The effect of the failure to adequately manage the storage of electronic information is explained in *Qualcomm Inc. v. Broadcom Corp.*[8]

On February 7, 2008, the U.S. District Court for the Southern District of California held that the attorneys for plaintiff Qualcomm should have inquired into the sufficiency of their client's response to the defendant's discovery requests. Qualcomm failed to disclose and produce some 46,000 electronically stored, relevant documents. The evidence adduced in a hearing on a motion for sanctions showed that the attorneys and representatives of Qualcomm knew that documents had not been disclosed or produced. The eventual sanction totaled more than $8 million and included a referral of Qualcomm's counsel to the California State Bar for disciplinary matters.

The lawyers for Qualcomm recently have been permitted the opportunity to lay blame on the client. This followed Qualcomm's accusations of attorney misconduct in declarations seeking to avoid the imposition of sanctions. In essence, the client opened the door for the attorneys to break through the attorney–client privilege and seek to exculpate themselves by accusing their client of wrongdoings.[9] The practicing lawyer probably does not want to ever experience this problem.

Glossary of Terms*

The following are basic terms that an attorney should understand before advising a client about document retention and electronically stored information.

- **Accessible data:** Data that is accessible with little or no targeted modification or reconstruction or special effort to produce. Accessible data includes active data and, usually, archival data.
- **Active data:** Data that resides in storage media on computers actively in use and readily visible to and immediately accessible by the system with which it was created.
- **Archival data:** Data that is maintained for long-term storage and record-keeping purposes, usually on removable storage media (such as CD-ROM or tape). Although archival data may be relatively easily accessed in readable form, it may require some modification and generally is not stored on computers in active, day-to-day use by end-users.
- **Backup data:** Data that is maintained in separate, portable media to permit data recovery in the event of disaster. Backup data generally is stored in relatively inaccessible formats, requiring extensive reconstruction or modification in order to be read, searched, or used in any meaningful way.
- **Computer forensics:** The use of specialized techniques for recovery, authentication, and analysis of electronic data, including reconstruction or mining of deleted or residual information.
- **Deletion:** The act of deleting data removes the data from active files or storage systems and, at a minimum, renders it accessible only through specialized recovery tools. Deleted data generally resides in designated storage space where it remains until it is overwritten in whole or in part through regular computer usage. It also may be permanently removed ("wiped" or "erased") by software designed specifically to do so.
- **Disaster recovery tapes:** Also known as "backup tapes." Portable tapes used to digitally store backup data.
- **De-duplication:** Also known as "de-duping." Identifying and eliminating documents that are exact duplicates of one another. De-duping can decrease the volume of data by 30 to 40 percent on average, and sometimes by as much as 90 percent.
- **Erased data:** Also known as "wiped data." Data that has been permanently removed from storage of any sort. Erased or wiped data cannot be recovered; however, directory entries, pointers, or other data relating to it may remain.
- **Forensic copy:** An exact bit-by-bit copy of the entire physical hard drive of a computer system.
- **Inaccessible data:** Data that is accessible only through highly targeted and specialized efforts that may include computer forensics techniques and expertise.
- **Metadata:** Literally, data about other data. Data imbedded within files that provides information about file activity. Some metadata is system-driven, generated automatically by the software itself. Other is user-defined and created only at the instigation of the end-user.
- **Native format:** Format in which data originally was generated and/or the format in which it is stored at the time of preservation.
- **Off-line systems:** Computers and other equipment that are used to create and store electronic information and are not centrally managed. Examples include laptop computers, PDAs that are not connected to a server, and cell phones.
- **Residual data:** Data that resides in but is not active on a computer system. Residual data includes data that has been designated for erasure but has not yet been fully overwritten. Retrieval requires undelete or other special data recovery techniques.
- **Routine operation of IT system:** The way an electronic information system generally is designed and programmed to meet technical and business needs; would include routines and procedures for regular document retention and destruction.

* This glossary of terms is excerpted from materials prepared by Emily Eichenhorn for the participant book distributed at CNA's 2006 ALADN Lawyers' Risk Management Seminar, "Packing Your Parachute: Preparing for Law Practice Risk."

Implications of *Zubulake* and *Qualcomm*

The attorneys for UBS Warburg and Qualcomm may have to pay many millions of dollars in sanctions for the judgments, and they will have to answer to their disciplinary counsel. Therefore, the litigation attorney or the attorney advising a client about document retention should be aware that failure to give proper counsel could have serious financial and professional ramifications.

Document Retention Letter

A lawyer who is involved in litigation or advising a client on document retention should send a separate engagement letter and a document retention letter every time a client is involved in or anticipates litigation.[10] The client should be advised that it must maintain all files and records, including electronically stored information related to the case. The client should be advised that it cannot allow any of its files to be lost, destroyed, or erased. The client may have to be told to discontinue or put a hold on any routine or scheduled document destruction policy.

At the inception of any agreement to represent a client in litigation, a lawyer might want to make it a practice to send a document retention letter. The letter should:

- advise the client that he, she, or it may have possession or control of paper documents or electronically stored information relevant to the case, and that this information may be contained in personal digital assistants (PDAs), servers, disc drives, thumb drives, laptops, and other hardware sources
- advise the client to cease all document destruction protocols, including electronically stored information
- contain some reference to electronically stored information in terms of letters, reports, client files, faxes, tax records, e-mails, voice messages, backup tapes, CDs, DVDs, accounting records, diaries, and communications with family members and friends
- tell the client that any source for the information must be preserved, which means that networks, laptops, PDAs, wireless phones, snap drives, and any number of other hardware sources must be protected
- instruct that the retention and cessation of document destruction should be absolute and in effect until further notice from the attorney.

Counselor Obligations

The *Zubulake* and *Qualcomm* cases may impose an affirmative obligation on attorneys to thoroughly understand the client's computer systems, including the cost of restoring data that may have been inadvertently destroyed before the case is filed. Specifically, *Zubulake I–III* adopted a seven-prong analysis to address:

1) the extent to which the request is specifically tailored to discover relevant information;
2) the availability of such information from other sources;
3) the total cost of production, compared to the amount in controversy;
4) the total cost of production, compared to the resources available to each party;
5) the relative ability of each party to control costs and its incentive to do so;
6) the importance of the issues at stake in the litigation; and
7) the relative benefits to the parties of obtaining the information.

Conclusion

The sum of the *Zubulake* cases and the related *Qualcomm* case tells us that litigation counsel should have knowledge about their clients' active and stored data systems. This may cost some money, but the spoliation instruction that could be given in the event a court determines that the destruction of electronically stored information resulted in the loss of potentially relevant evidence is much more damaging than the time the attorney will spend assembling this information.

Notes

1. *Zubulake v. UBS Warburg, LLC*, No. 02 Civ. 1243(SAS), 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (*Zubulake V*).

2. *See Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (*Zubulake I*); *Zubulake v. UBS Warburg, LLC* 2003 U.S. Dist. LEXIS 7940 (S.D.N.Y. May 13, 2003) (*Zubulake II*); *Zubulake v. UBS Warburg, LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (*Zubulake III*); *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*); *Zubulake V, supra* note 1.

3. *See generally Zubulake V, supra* note 1.

4. For more information about the mission of the Sedona Conference, *see* www.thesedonaconference.org/content/tsc_mission/show_page_html.

5. The Sedona Conference, "The Sedona Principles Addressing Electronic Document Production, Second Edition" (June 2007), available at www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf.

6. *See* F.R.C.P. 16(a)(3)(B)(iii) (requiring counsel to discuss and provide the mechanics for the disclosure of electronically stored information).

7. The author would like to thank Emily Eichenhorn, Lawyers Risk Control Consulting Attorney with CNA Insurance, the CBA-sponsored lawyer's professional liability carrier. The glossary of terms and discussion on Sedona principles are taken from materials prepared by Eichenhorn for the participant book distributed at CNA's 2006 ALADN Lawyers' Risk Management Seminar, "Packing Your Parachute: Preparing for Law Practice Risk."

8. *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D.Cal. 2008).

9. *See id. See also Treppel v. Biovail Corp.*, 249 F.R.D. 111 (S.D.N.Y. 2008).

10. In Colorado, this date is very important, because the Colorado Supreme Court has ruled that documents created in routine accident investigations are not subject to attorney–client communications or the work product doctrine if the investigation was done before there "existed a substantial probability of imminent litigation over [the] claim." *Compton v. Safeway, Inc.*, 169 P.3d 135, 138 (Colo. 2007). ■