

eDiscovery Risks for Corporate C

The eDiscovery risks for corporate counsel have never been higher. This paper explores some of the reasons for that, identifies the aspects of eDiscovery that present the most risk, and suggests how those risks might be mitigated.

The time when corporate counsel could rely on outside counsel to handle the entire eDiscovery process, from drafting and issuing litigation hold notices through overseeing data collection, processing, review, and production, is over. Certainly the judgments against corporate defendants in two recent highly publicized cases driven in large part by eDiscovery missteps — \$29 million against UBS in the Zubalake case and \$1.45 billion in Ronald Perelman’s lawsuit against Morgan Stanley in the Coleman case (later reversed for reasons unrelated to the eDiscovery issues) — are large enough to attract the attention of most corporate counsel. In addition, recent court decisions, holding counsel personally responsible for the proper execution of the eDiscovery process, place a premium on corporate counsel management, or at least active oversight, of the entire eDiscovery undertaking.

In Qualcomm v. Broadcom, a current case pending in the Southern District of California, the court sounded

an even stronger warning. On August 13, 2007, the court issued an Order to Show Cause against fourteen attorneys for the plaintiff, Qualcomm, plus “any and all other attorneys who signed discovery responses, signed pleadings and pre-trial motions, and/or appeared at trial on behalf of Qualcomm,” based upon Qualcomm’s failure to produce over 200,000 pages of relevant emails, memoranda, and other company documents until four months after the patent infringement jury trial had concluded (and which plaintiff Qualcomm lost). At issue is whether the court will impose sanctions on Qualcomm’s counsel, including “monetary sanctions, continuing legal education, referral to the California State Bar for appropriate investigation and possible sanctions, and counsel’s formal disclosure of this Court’s findings [of egregious conduct and aggravated litigation abuse] to all current clients and any courts in which counsel is admitted or has litigation currently pending.” Although the Order was directed against Qualcomm’s outside counsel, it is probably no coincidence that Qualcomm’s General Counsel suddenly resigned the week the court issued the Order. The court’s prior order, granting Broadcom’s claim against Qualcomm for some \$8.5 million in attorney’s fees, is on appeal.



ounsel

by Jeff Jacobs*

Once litigation (or a government investigation) has commenced, or is reasonably likely, the party to the litigation (or the target of the investigation) has an immediate duty to preserve information that may be relevant to the litigation or investigation, even in advance of a discovery request or subpoena.

Outside of the litigation context, eDiscovery issues most commonly arise in merger reviews by the Department of Justice and the Federal Trade Commission, and in the course of criminal investigations by the Department of Justice and civil investigations by the Securities and Exchange Commission and other governmental agencies. It is far from career-enhancing for General Counsel to have to report to the CEO that a corporate acquisition cannot be closed because of delays or glitches in producing electronically stored information to the reviewing government agencies. Most counsel, not to mention a large part of the general public, are all too familiar with the consequences of Arthur Anderson's and Enron's failures, whether perceived or actual, to preserve evidence sought by government investigators.

Although these cases indicate that corporate counsel need to be intimately familiar with, and ultimately responsible for, the entire eDiscovery process, two aspects of that process — data preservation and collection — have been the particular focus of most of the recent case law, and therefore present the most risk to corporate counsel.

Once litigation (or a government investigation) has commenced, or is reasonably likely, the party to the litigation (or the target of the investigation) has an immediate duty to preserve information that may be relevant to the litigation or investigation, even in advance of a discovery request or subpoena. Failure to do so in a litigation context may result in the imposition of sanctions under FRCP Rule 37, up to and including exclusion of evidence in support of the party's case, the issuance of "inference" jury instructions, and the imposition of an obligation to pay the attorney's fees of the requesting party. In the context of a governmental investigation, such failure is one of the factors to be taken into account in determining whether the Department of Justice will seek indictment of a corporation, and may also result in a criminal prosecution for obstruction of justice.

But in order to preserve the necessary information, corporate counsel need to know where to find it. In an age of electronic information, where 80% of corporate communications are conducted by email without redaction to paper, that information may seem to be everywhere. Employees' email may be found on personal computers, laptops, network shares, BlackBerries or other PDAs, home computers, personal backups (ZIP, thumb drives, etc.), enterprise backups, and even text messaging on cell phones. Enterprise data may be found on email servers, backup servers, and storage

media such as tapes and disks. And of course non-email information may be scattered across the company's electronic systems and applications, including financial and HR systems and databases. When a case is filed or reasonably likely, corporate counsel need to know where all of the potentially relevant information can be found, who is responsible for generating, managing, and storing it, and how any routine, automated processes for deleting or overwriting such information can be stopped immediately. Notices putting a "hold" on such deletion and overwriting, whether manual or electronic (often called "litigation hold notices"), need to be sent to all potential custodians of relevant information as well as employees in the departments. Failure to identify the relevant custodians in a timely manner, or to put in place a hold on potentially relevant information, may result in the imposition of the sanctions outlined above.

In the Zubulake case, counsel for defendant UBS Warburg had issued a litigation hold after Zubulake filed EEOC charges against the company but never mentioned backup tapes in the hold instructions. Some employees deleted relevant emails in spite of the instructions, while others failed to provide all relevant information to counsel. As it turned out, the backup tapes (which had been overwritten) might have contained some of the deleted emails. The consequence was the imposition of adverse inference instructions to the jury, which essentially ensured plaintiff's victory in the case.

In her Zubulake V opinion, Judge Scheindlin outlined a list of responsibilities that counsel would be well-advised to follow. They include obligations to:

- Actively monitor compliance with a litigation hold, noting that it is insufficient to simply advise a client of the hold and then expect the client to retain, identify, and produce the relevant evidence;
- Become fully familiar with the client's document retention policies, as well as the client's data retention architecture and electronic systems, which will invariably involve speaking with the client's information technology personnel;
- Communicate with all key players involved in the litigation, ascertaining how and where they store their information, and advising them of their retention obligations; and
- Ensure that relevant backup tapes or other backup media are retained.

Although these guidelines may be regarded as dicta in the Zubulake case, there is no question that subsequent court decisions have imposed an obligation on both corporate and outside counsel to know their clients' IT systems well enough to be able to articulate how and where electronically stored information is backed up. This obligation has been codified, to some extent, in the recently revised FRCP Rule 26(b)(2)(b), which among other things requires the parties to identify sources of electronically stored information that support their case or defenses.

Once the relevant custodians and potentially relevant information have been identified and preserved, it is necessary to collect the information. The type of case may dictate the method of collection — in some very routine cases, employees may be relied upon to simply review desktop information and download relevant materials to a CD for transmittal to corporate or outside counsel. More contentious matters may call for collection by forensic experts, who can preserve all of the informational metadata (such as the time and date of creation and modification of the email or document) and can certify to the chain of custody of the evidence in case of challenges to its authenticity. Of course the larger the matter, the more information that needs

to be collected, and the more custodians at issue, the more likely it is that the use of a third-party eDiscovery vendor, with specialized expertise in the collection and management of large amounts of data, will be desirable. The risk of erring in the collection of this information — of failing to preserve necessary metadata, or destroying information in the process of collecting it — is that an adverse litigant may claim spoliation of evidence and seek — perhaps successfully — the sanctions outlined above.

How can corporate counsel protect themselves against these risks? Perhaps the best way is by knowing where the company's information is located and who is responsible for it, and by having in place a well-documented, enforceable process for handling every eDiscovery matter in the same way, across the entire company. A process that goes into effect immediately when litigation commences or is reasonably likely, that ensures the rapid identification of potentially relevant information sources, that ensures the preservation of potentially relevant information, and that provides for the collection of information in a defensible manner, is the best insurance against claims of eDiscovery abuse and the spoliation of evidence.

The type of case may dictate the method of collection — in some very routine cases, employees may be relied upon to simply review desktop information and download relevant materials to a CD for transmittal to corporate or outside counsel.

*Jeff Jacobs, Senior Consultant, Electronic Evidence Discovery, Inc. Mr. Jacobs is a graduate of Williams College and the University of Chicago Law School. He spent ten years as a Special Counsel in the litigation group of the Washington, DC office of Sullivan & Cromwell, joined MCI WorldCom as an Associate Litigation Counsel, managing all electronic discovery in connection with the governmental and independent investigations into WorldCom's accounting irregularities, the securities litigation stemming from those irregularities, and the WorldCom bankruptcy. Following the Verizon-MCI merger in 2006, Mr. Jacobs joined the Washington, DC office of DLA Piper as a Special Counsel in the litigation group, where he continued to advise the former MCI (now known as Verizon Business) on electronic discovery, general litigation and records management matters