

e Discovery Demands Better Email Management



The eDiscovery risks for corporate counsel have never been higher. In light of recent, highly publicized cases it is no longer possible to ignore E mail and electronic document management. How do you protect yourself? ImageX's Web Secured E mail (WSE) with built in electronic document management, by mitigating risk through a well-documented, companywide, consistent and enforceable process for preserving potentially relevant information is a cost effective way to manage all your e mails during a case that requires eDiscovery.

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.

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 a 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 ArthurAnderson'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 acquisition and retention 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 needs to know where to find it. In an age of electronic information, where 80% of corporate communications are conducted by email without reduction 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 needs 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 responsible for the management and storage of that information (IT, IS, Records Management, etc.) . 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 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.
- 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.

Image X's Web Secured Mail (WSM) has been designed to incorporate all of the requirements of FRCP regulations by providing a means of exchanging information between parties involved in the case e.g. attorneys, accountants, auditors, and consultants in a secure fashion.

Features

- Archiving every mail and attached documents using the proven MINDS system, which has been used by courts and organizations since 1990 to archive legal and protected documents.
- Converting and stamping of every document authenticating the date of receipt and providing the information to sender and receiver about the status of message as it travels from sender to receiver.
- Generating complete reports that provide who, when and from where documents are accessed.
- Providing firewall and encryption at server level.
- Interfacing to popular mail server software to provide a means of converting and stamping all documents from any persons that are sending documents using normal E-mail system.
- Incorporates Web based faxing which can be used to distribute briefs, notes, day sheets, information by organizations that use Fax machines. Fax machines.
- Uses SQL database to provide secure login and password-based access to authenticated users, and data backup and storage systems to ensure system continuity and recovery.
- WSM-IDS and Mail-Firewall have security features designed to detect suspicious internal computer user behavior and thwart subversive attacks, including the ability to automatically detect and respond to e-mail anomalies; generate log files and reports that are useful for audit trails.
- Detects malicious code including viruses, worms, and Trojan horse applications.
- Customizable policies, alerts, and notifications for handling messages containing malicious code.

One of WSM's unique features is the secure archiving of relevant documents. Typical e mail transactions include document or image transmission as well. WSM's use of the Image X date stamp system should provide value to many different trading partners. The use of industry standard MS SQL databases and appropriate internal access and authentication controls along with encryption should also provide assurances of compliance with the emerging identity theft regulations.