

New Technology, New Rules: Current Trends in e-Discovery

"Blogs by their nature tend to be more personal than other communications, and it is easy to think of situations where directors or officers cross the line and inadvertently get themselves and the company into trouble."

Former SEC lawyer Broc Romanek, as quoted in Corporate Boardmember Magazine

"...as it is a system of restricting rights of access to the information and predetermining deletion of information, people adopting DRM must consider that the documents (information) may, in the future, be required for a criminal or tax investigation or be required to be produced in Court."

Computerworld

Electronic discovery is nothing new. As far back as the 1970s the courts were working to address the production of electronic information and to define the reasonable limits of e-discovery. Fast forward to today, and we find organizations using information technology as their primary means of doing business and generating business information – but the same challenge remains. Companies, courts and litigators alike are still trying to define the reasonable limits of electronic discovery, even as rapidly evolving technologies continue to change how business is done and litigation is resolved.

A common theme concerning technology is that its use often extends beyond what was originally intended. Consider that in only the past decade it has become common to see:

- Contract negotiations using electronic communications technologies
- Marketing through text messaging
- Business transactions through email
- Instant messaging (IM) as evidence in court

Technology has transformed the way we do business; and it appears as if it may continue to do so indefinitely. In the midst of this change it has become increasingly clear that too many organizations are failing to meet their legal responsibilities relative to the preservation and production of information. This has resulted in an ongoing effort to refine organizations' means of complying with their discovery responsibilities. As technology and the rules surrounding it continue to evolve, the importance of digital information and the way organizations are required to preserve and manage it for the purposes of litigation continues to be a critical issue for the enterprise.

"Informal" Technologies. Similar to the way that email and instant messaging crept into the workplace, many organizations have begun experimenting with technologies that have generally been considered "informal." Some companies and their CEOs are creating web logs, or "blogs" to advertise and provide information to the public. Others are experimenting with internal blogs, online syndication (RSS feeds) and collaborative networks (wikis) to encourage information sharing on the corporate intranet. While benefits can be gained from using these technologies, organizations need to be aware that the legal risks involved in the business use of email and IM apply to these newer technologies as well. Moreover, the "informal" nature of blogs, both internal and outward facing, may create potential liability if employees aren't clear as to how such technologies should be used. Prosecutors aren't naïve when it comes to digging for digital evidence – blogs and similar technologies can be fair game for e-discovery. In fact, in an ongoing case, a computer company is seeking to subpoena records related to a popular blog to determine which of their own employees leaked trade secret information onto the web.

Digital Rights Management (DRM) and Discovery. The popularity of DRM as a tool to control the access and use of content is increasing in the enterprise. DRM can protect digital content by controlling which individuals in the organization can access a document and how they can use it – including whether or not a document can be

"If destruction of relevant information occurs before any litigation has begun, in order to justify sanctions, the requesting party must show that the destruction was the result of bad faith. Bad faith need not directly be shown but can be implied by a party's behavior."

*E*Trade Secs. LLC v. Deutsche Bank AG*

The company "has engaged in repeated improper discovery conduct during this litigation and its withholding of a large quantity of relevant and damaging e-mails until nearly ... the very end of ... discovery, was inexcusable and has harmed the defendant."

Lava Trading, Inc. v. Hartford Fire Ins. Co

printed, copied or deleted. But similar to blogging, the use of DRM technologies can also pose legal challenges. Organizations must carefully consider how they use DRM, as DRM encryption tools can render documents inaccessible. While the ability to lock down a document has considerable use in protecting an organization's information, it can also have serious implications for discovery - for example, finding out in the midst of litigation that you cannot find the encryption key for responsive documents, and that the employee responsible for that key has long since left the company. In light of these risks, organizations that use DRM to protect their information and records must make an effort up front to train employees in its proper use to avoid making discoverable information inaccessible.

Proposed Changes to e-Discovery Rules. Aside from the challenges involved in producing information from newer technologies, many organizations still don't fully understand how to manage "common" technologies such as e-mail and IM, or unstructured data on media such as disaster recovery backup tapes. In response to growing concerns, the federal government is considering amending the Federal Rules of Civil Procedure (FRCP) that govern the discovery process for litigation. One suggested change to the Rules advocates that information that is not readily accessible, such as the contents of backup tapes, might not be required to be produced. But before companies breathe a sigh of relief, they should know that if this proposed change is passed it will not give organizations carte blanche to mismanage information. Information that is inconvenient to access and produce can still be required for discovery if it's relevant to the case. What's more, such changes to the Rules might lull some organizations into a false sense of security that could potentially lead to the failure to preserve responsive information and records.

"Sport of dirty tricks". Currently, acts of bad faith relative to e-discovery are very much on the radar screen, even as the debate over the proposed changes to the FRCP are underway. In an ongoing 2005 fraud case involving e-discovery, a securities firm was accused of turning "the litigation process into a sport of dirty tricks." The judge apparently agreed with this assessment and imposed sanctions against the firm. In another case this year, a company withheld thousands of pages of responsive email and other evidence until just prior to court conferences and critical depositions, limiting the opposing counsel's ability to use the materials provided. Again, the judge imposed sanctions that hurt the company's case. In yet another ongoing case, an investment banking company has seriously damaged its case by "deliberately and contumaciously [violating] numerous discovery orders," and faces damages in the amount of \$485 million, in addition to possible penalties for their e-discovery failures. Courts and prosecutors will continue to be sensitive to acts of "bad faith," no matter what changes are made to the federal e-discovery rules.

Developing technologies will certainly continue to take companies to new levels of growth and efficiency, while ushering in new legal considerations and risks. As these new technologies reach the corporate mainstream, debates over an organization's legal responsibilities to preserve and produce their information will continue to arise. Despite the rapid pace of change, organizations should strive to consistently assess the legal impact of their technology before it is implemented and exhibit good faith relative to the e-discovery process. By consistently showing good faith and carefully managing their digital information, organizations can go a long way toward protecting their legal interests, no matter what challenges the current legal or regulatory landscape brings their way.