



E-Discovery: Do Your Clients Know the Rules?

Data spoliation and email/voicemail discovery rules ... you understand them, but do your clients? A client who doesn't can very well hamper its own defense and run up huge expenses.

As companies transform themselves from ink-on-paper to electronically networked environments, many are doing so with little true appreciation for the consequences. For instance, the office email explosion has resulted in archives of informal, often-candid messages living on long after they're forgotten. The ubiquitous word processor has likewise created digital reams of information — where even deleted language or edited ideas are discoverable.

Helping Clients Keep Pace

Companies have generally not kept pace with this technological transformation. With that in mind, now might be a good time to share with clients what their obligations are under electronic discovery rules, and how that may impact them in the event of litigation.

It's a different ballgame. The needs for evidence disclosure are very different from the data or disaster recovery models that most corporate IT departments operate under. First and foremost, clients need to understand that whatever their document-retention policy may be, it can be overridden by legal action.

Companies have been sanctioned for destroying documents, even though the destruction was consistent with a well-constructed corporate document-retention policy. This has typically happened in cases where it was determined that

the company could “reasonably have anticipated” that the documents could be relevant to a lawsuit that was clearly foreseeable.

The stakes are (incredibly) high. Morgan Stanley’s 2005 adverse judgment of \$1.45 billion came in large part from a judge's ruling that the Wall Street giant had acted in "bad faith" in failing to turn over relevant emails. The stakes in litigation can be enormous, far exceeding the cost of the related legal and IT fees.

Disorganization is no defense. Companies naturally raise their concerns about potentially huge costs and the burdens of discovery to the judges administering the discovery rules. Certainly, judges may limit discovery when the burden of discovery outweighs its likely benefit.

But when the high cost of discovery can be attributed to the respondent company’s failure to organize itself efficiently, judges are likely to impose the cost of discovery on the company. The situation is of the company’s own making, the argument goes, created by the company’s decision to adopt an information system from which it has benefited overall but which has made the desired discovery difficult.

Preservation obligations need to be understood. When a company is sued, an obligation arises for it to preserve evidence relevant to the suit. Typically, your client will need to take all necessary steps to assure that the company’s “employees, agents, accountants and attorneys refrain from discarding, destroying, erasing, purging or deleting any relevant documents including but not limited to computer memory, computer disks, data compilations, email messages sent and received and all back-up computer files or devices.”

Avoiding spoliation is key. It's important that the procedures followed for collecting electronic evidence are meticulous and meet appropriate standards. The data must be collected without being spoiled or altered, and someone must be able to attest to the chain of custody, showing how the evidence was collected and kept safe and unaltered from first to last.

It’s important to know the “what” as well as the “where.” Finally, it's not enough to simply locate all of the

requested files. Clients must know what's in them and must weed out documents that need not be handed over. They also need to have a good understanding of the content in the documents they hand over so their legal team can prepare the best legal strategy.

It's A Brave New World

Once recorded, electronic data is remarkably persistent. In fact, looming in the future is the possibility of near-perfect information systems in which all actions are recorded, stored and subjected to electronic retrieval and analysis, leaving a complete data trail.

As clients race to catch up with the implications of these technological changes, make sure that you are the trusted advisor they turn to for guidance.