Legal Brief

Electronically Stored Information and E-Discovery: Understanding Through Clichés

The 2007-2008 New England Patriots. Any recent Seann William Scott movie. Ralph Nader. What do they have in common? All three had a lot of hype but in the end were a letdown. In contrast, electronic discovery (e-discovery) lives up to the massive hype surrounding it. But what is it, and how can an organization get its arms around it? Like a bad motivational seminar, this article uses clichés to illustrate the concept and the steps that an organization can take to mitigate the threat that electronically stored information (ESI) poses.

Cliché 1: They Are Who We Thought They Were.

This legendary Dennis Green cliché describes electronic discovery. ESI is what you think it is: e-mails, instant messages, word processing documents and any communication or record that is produced "electronically." Discovery is the stage in civil litigation in which a party can request documents and other evidence to use at trial (responsive documents). As such, e-discovery is discovery that takes the form of ESI.

Cliché 2: The Will to Succeed is Nothing Without the Will to Prepare.

This overused cliché has no apparent attribution. Regardless, unmanaged ESI poses numerous risks to an organization. The general rule is that a party must produce all relevant information within the scope of a discovery request. Before ESI, this was fairly straightforward: determine the physical documents that were relevant to a discovery request, pull them out of the files, make photocopies, and voilà, discovery obligations were fulfilled. Meeting this burden in the era of e-discovery is dramatically more complicated, raising issues relating to locating ESI, as well as determining what ESI should be provided.

Fortunately, an organization can help to meet this burden by implementing a reasonable ESI policy. For example, the Internal Revenue Service generally requires an organization to maintain seven years worth of certain tax-related data. It follows that it may be reasonable for a company to delete such data that is over seven years old. Of course, establishing deletion schedules for e-mail and other uncategorized ESI is a little more nebulous. Courts will continue to define the contours of this reasonableness standard, but as a general rule, arbitrary and capricious data-deletion time frames will not withstand court scrutiny and could result in court sanctions or unnecessarily providing incriminating responsive documents to an opposing party. Moreover, not having an understanding where data resides (servers, personal computers, PDAs) can lead to expensive court-ordered searches.

Accordingly, an organization should implement an ESI policy that sets forth the types of ESI that it controls, the locations of ESI, and the time frame that such data is maintained. The policy also should include a litigation hold process, whereby when a litigation threat emerges, procedures are put in place to ensure responsive ESI is not deleted.

Cliché 3: Always Follow-Through.

In the clichéd words of every basketball coach on the planet, follow through is key. An ESI policy that is not consistently followed is going to draw scrutiny and result in increased litigation costs and risk exposure to an organization. The nightmare scenario is where a policy calls for the deletion of all e-mails older than five years; but an IT staffer has been making rogue backup DVDs of older e-mails "just in case." It comes out in discovery that these backup DVDs exist, and the DVDs contain responsive evidence. To avoid this, an organization should conduct regular audits to ensure that its ESI policy is being adhered to.

Conclusion (and Cliché 4): Just Do It.

Now is not the time to ignore the perils of a non-existent or poorly implemented ESI policy. The up-front costs pale in comparison to the back-end risk. Recently, in California, a business was sanctioned by a court to the tune of $8.5 million for e-discovery abuses. So, just do it: 1) understand what ESI exists in your organization; 2) establish an ESI policy; and 3) adhere to the policy and be ready to document that it is being followed.

MacDonald, Illig, Jones & Britton LLP attorneys are familiar with IT issues and the current state of the law, and can advise on e-discovery and ESI with an eye toward reducing organizational risk and minimizing legal expenses.

Patrick J. Mondi is an associate at the law firm of MacDonald, Illig, Jones & Britton LLP. A graduate of Purdue University and Chicago-Kent College of Law, he practices in the areas of business transactions, commercial litigation and real estate.