NACUANOTES
February 22, 2008
Vol. 6 No. 2

TOPIC:

PREPARING FOR E-DISCOVERY

INTRODUCTION:

Responding to litigation discovery requests is no longer a matter of simply turning over boxes of hard copy documents for photocopying and review by an opposing party. Electronically stored information, or "ESI," is now more than fair game for discovery, and opposing parties are routinely seeking production of ESI – particularly e-mail. Effective December 1, 2006, the Federal Rules of Civil Procedure ("Federal Rules") were amended in various ways that have substantially affected electronic discovery ("e-discovery") and records management obligations. In addition, more than 30 U.S. District Courts have adopted local rules on e-discovery, and many states (including Kansas, Delaware, Mississippi and Texas) also have amended their rules of civil procedure to address e-discovery.

Preparing for e-discovery requires coordination between various offices and individuals on any college or university campus, including counsel's office, the IT department, and faculty and staff members. This Note will focus on the practical aspects of preparing for e-discovery in state or federal court litigation and will offer suggestions for ways that colleges and universities may reduce risks and control costs in tackling the new challenges.

DISCUSSION:

I. What are Discovery, E-Discovery and ESI?

"Discovery" is the phase of state and federal court litigation in which parties seek information from each other to investigate the facts of the case and to develop claims and defenses in preparation for trial. Discovery can come in numerous forms, including interrogatories (a set or series of written questions answered in writing under oath), requests for admission (written statements to either admit or deny key facts), depositions (oral testimony), and requests for production of documents. The term "documents" has now been construed by the courts and/or legislatively defined to explicitly include electronically stored information.

E-discovery involves the identification, retention, and production of ESI during litigation. ESI consists of dynamic data and information that, in most instances, would be incomprehensible if separated from the system that created it. As explained in an advisory committee report to the Federal Rules of Civil Procedure, ESI will exist in exponentially greater volume than the hard-copy documents that parties have traditionally produced in response to litigation discovery requests [1].

ESI resides many places, including:

- Office equipment – including personal computers, lap tops, smart phones, voicemail systems, networked photocopiers, Blackberries®;

- Home equipment – including home computers, personal PDAs;
- Portable Media – including jump drives, CDs, DVDs, magnetic tapes, diskettes, memory cards;
- Servers – including email servers, SPAM filter servers, Blackberry® servers, document management servers, instant messaging (IM) servers, file servers, print servers, firewall servers, HR database servers, payroll database servers, and internal and external web servers;
- Proprietary applications (software or other programs licensed exclusively to the institution); and
- Back-up tapes.

The two critical responsibilities that arise with respect to electronic discovery are (1) the duty to preserve ESI and (2) the duty to produce pertinent portions of that information to the other parties to the litigation. Document preservation obligations generally arise once an institution reasonably anticipates that it is likely to be a party to private litigation or a government investigation. The preservation obligation, therefore, may arise even before a case is filed or an investigation is commenced. Once a preservation obligation is triggered, an institution has the obligation to preserve all information – including ESI – that may potentially be relevant to the dispute. The amount of information preserved will likely be far greater than the amount of information ultimately turned over to the other parties in the litigation. It should also be noted that constantly evolving technology is available that may assist counsel, IT personnel, and records managers in retaining, searching, and reviewing information for the purposes of e-discovery. Although utilizing such technology may create upfront costs for an institution, it may be needed in certain cases and could also ultimately help reduce costs in major pieces of litigation.

Failure to comply with e-discovery obligations can have disastrous consequences. Institutions could face adverse jury inferences, which, in the much publicized *Zubulake* case [2], resulted in a $29 million jury award to the plaintiff. In addition, courts can impose stiff monetary penalties against parties that do not adequately preserve discovery materials, as seen in a recent $15 million fine imposed by the Securities and Exchange Commission (SEC) against Morgan Stanley [3]. Additional potential civil penalties may include dismissal of claims or defenses and orders to pay opposing counsel's attorneys' fees and costs. In government investigations, egregious failure to meet e-discovery obligations can result in charges of obstruction of justice charges and criminal prosecution, as seen in the highly publicized *Arthur Andersen* case [4]. Finally, failure to treat confidential consumer information appropriately through institutional records management and e-discovery policies and procedures can result in regulatory violations under the Health Insurance Portability and Accountability Act ("HIPAA") and other privacy laws, including the Gramm-Leach-Bliley Act.

II. Preparing for E-Discovery

E-discovery can be daunting, and preparing for e-discovery requires expenditure of considerable resources—including personnel time and money. Indeed, as e-discovery becomes a regular part of most litigation, many institutions are now finding that the cost can be staggering, and it has not generally been included in either counsel or IT budgets. Pro-active preparation for e-discovery, however, can help you reduce risks, control costs, and efficiently and effectively respond to discovery once litigation arises.

A. Records Management

Effective records management practices can help limit the universe of ESI ultimately at issue in any future litigation. Institutions are encouraged to review their records management policies and procedures to ensure that they encompass ESI and satisfy all legal, business, and regulatory obligations. A retention schedule should be in place identifying the institution's key categories of records and the corresponding retention periods. As a part of the ordinary course of business, records should be destroyed at the expiration of the retention period, unless subject to a preservation notice. Before records are destroyed pursuant to an established records management policy, the destruction should be authorized in writing by an appropriate manager or other administrator and the actual destruction of the records should be certified by the responsible individual or entity (e.g., mail room personnel or outside shredding vendor).

B. Back-up Tapes

Owing to the excessive costs associated with restoration and attorney review of back-up tapes, which can contain data amounting to millions of pages each, institutions should do everything possible – keeping in mind any pre-existing litigation preservation obligations – to limit their inventory of back-up tapes. Back-up tapes are intended to be used for disaster recovery, and, as the name "back-up tapes" suggests, the tapes go stale as soon as a new set of back-up tapes is made. Once stale, back-up tapes can and should be disposed of or recycled, absent an existing preservation notice on the tapes.

To justify an institutional back-up tape retention policy in any future litigation, a back-up tape retention policy should be established. The policy should:

- Clearly state that back-up tapes are for disaster recovery purposes only;
- Implement a standard rotation cycle (e.g., 28 days – if justified by your institution's needs and practices);
- Implement a uniform rotation schedule (e.g., across all schools, servers, locations, and divisions);
- Require use tracking/inventory software, barcodes, and other computerized features to maintain and track tape inventory;
- Address how expired and obsolete tape inventory will be handled;
- Ensure backup tapes are identified and accounted for at all times;
- Establish procedures requiring IT personnel to obtain approval prior to creating special back-up tapes and requiring notice to in-house counsel of any such action;
- Clearly state that litigation preservation notices override standard policies and practices for back-up tape disposal;
- Create procedures for the identification and isolation of tapes subject to preservation notices and the disposition of such tapes once preservation notices expire;
- Expressly prohibit freelance creation of backup tapes without special approvals and safeguards; and
- Ensure the backup tape policy complements and is consistent with the institution's other records management and preservation notice policies and practices.

As with any written policy, a back-up tape retention and disposal policy will be effective only to the extent that it is properly implemented and followed. Administrators, university counsel, and IT personnel should work closely in developing such a policy and should not put anything in writing that the institution cannot effectively implement and consistently follow.

C. IT Infrastructure

Institutions should consider creating schematics of their IT architecture. Identifying all servers and applications will provide a roadmap of where to apply preservation notices and collect relevant ESI once litigation is threatened or commenced. In fact, many courts are now requesting such schematics when addressing discovery disputes. Schematics can be created by either internal IT departments or outside vendors.

D. Preservation

To ensure a consistent process that is defensible in future court proceedings and to avoid spoliation allegations, institutions should have an effective preservation notice policy in place. The policy should:

- Create a reporting mechanism to ensure that once the institution has information sufficient to conclude that it should reasonably anticipate litigation, the preservation process is timely initiated (including a process for faculty and staff to report circumstances that may trigger the institution's duty to preserve);
- Ensure preservation notices are sent out promptly under the signature of a senior administrator once the duty to preserve triggers;
- Create a process to identify the key players who should receive the preservation notice;
- Create a mechanism to evaluate whether the preservation notice must go to third parties or affiliates;
- Ensure a proper means of distribution of the notice, including a mechanism to confirm receipt (such

as email notification) and compliance;
- Create a process to account for preservation of information from former faculty and employees who are key players;
- Include a mechanism to follow-up with key players who do not confirm receipt of the notice;
- Require cooperation with IT department to address suspension of auto-delete of email and other ESI, if necessary, of relevant information;
- Require documentation of how IT implements the preservation notice;
- Require documentation of what sources of ESI (applications, software, backup tapes, physical locations, etc.) were preserved;
- Create a mechanism to send supplemental preservation notices when scope of litigation or identity of key players change;
- Ensure circulation of periodic preservation notice reminders;
- Ensure timely termination of the preservation hold;
- Include provisions for faculty and employee training on e-discovery and retention obligations; and
- Provide for auditing of practices to ensure compliance with policy.

Institutions may choose to create a template preservation notice as part of this policy. The notice should be amended as needed for each dispute. The preservation notice should include sufficient information to allow the key player custodians to identify potentially relevant information that is subject to preservation, including a description of the matter, relevant dates, and likely sources and locations of information (including ESI) [5].

III. Ways to Reduce Risks and Control Costs

In addition to the practices and policies discussed above, institutions may take additional measures in preparing for e-discovery to reduce risk and control costs once litigation actually commences. Institutions may want to evaluate, based on the size of the litigation matters they generally face, the posture of any actual or threatened litigation they are facing, and their internal IT capabilities, whether the collection of ESI should be done internally or by an outside vendor. If outside vendors are being considered, in-depth research on any potential vendor should be conducted, and discounts should be aggressively negotiated.

To limit the scope of e-discovery in any future dispute, institutions may want to consider setting policies and limitations on the use of developing technologies by faculty and employees (instant messaging, Voice over Internet Protocol (VOIP), blogs) or the use of personal computers for business purposes, or at least require that such technology be implemented centrally rather than on an *ad hoc* basis. Administrators and in-house counsel may also consider meeting with their institution's IT department to understand the litigation implications of new technologies before such technologies are purchased and implemented.

Institutions should also consider providing training to faculty and employees on issues of e-discovery, preservation notices, and records management. No matter what course of action your institution chooses in implementing an e-discovery preparation program, all steps taken should be documented by memorandum or meeting minutes and the program should be periodically audited to ensure compliance.

Issues relating to the litigation meet-and-confer process and the actual production of ESI during discovery are not within the scope of this article. Institutions should be aware, however, that the federal rules of civil procedure and many state rules require the parties to meet early in the course of litigation to discuss discovery, including the preservation and production of ESI. Institutions that have been proactive in addressing issues of records management, IT infrastructure, back-up tapes, and information preservation will be in the best position to aggressively negotiate preservation and discovery agreements with opposing counsel. The more your institution understands its own practices and policies, IT infrastructure, and ESI capabilities the more effective it will be at educating and addressing the concerns of opposing counsel and the court, and the better armed it will be to accurately speak to the costs and burdens associated with any proposed discovery in a given case.

CONCLUSION:

E-discovery is here to stay. There are numerous steps that a college or university can take to help prepare the institution for e-discovery and to help minimize litigation risks and costs in the process. In-house counsel, outside counsel, administrators, and IT personnel need to work together to learn how their institution's existing network operates and to establish effective and consistent ESI policies. When litigation is threatened, the more expeditiously an institution acts to meet its ESI obligations, the more effective the institution will be in controlling costs and reducing risk down the road.

FOOTNOTES

AUTHORS:

Wendy Butler Curtis

Caroline M. Mew

RESOURCES:

NACUA Resources:

- Electronic Discovery and Electronically Stored Information Resources and Links

Additional Resources:

- ABA Legal Technology Resource Center, Electronic Discovery
- ARMA International
- Electronic Discovery Reference Model (EDRM)
- Federal Judicial Center, Education Programs and Materials (including Managing Discovery of Electronic Information: A Pocket Guide for Judges, Barbara J. Rothstein; Ronald J. Hedges; Elizabeth C. Wiggins, 2007.)
- The National Archives Records Management
- The Sedona Conference
- Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information (August 2006; Conference of Chief Justices)
- EDUCAUSE: ESI and E-Discovery Resources
- DiscoveryResources.org

"To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve."