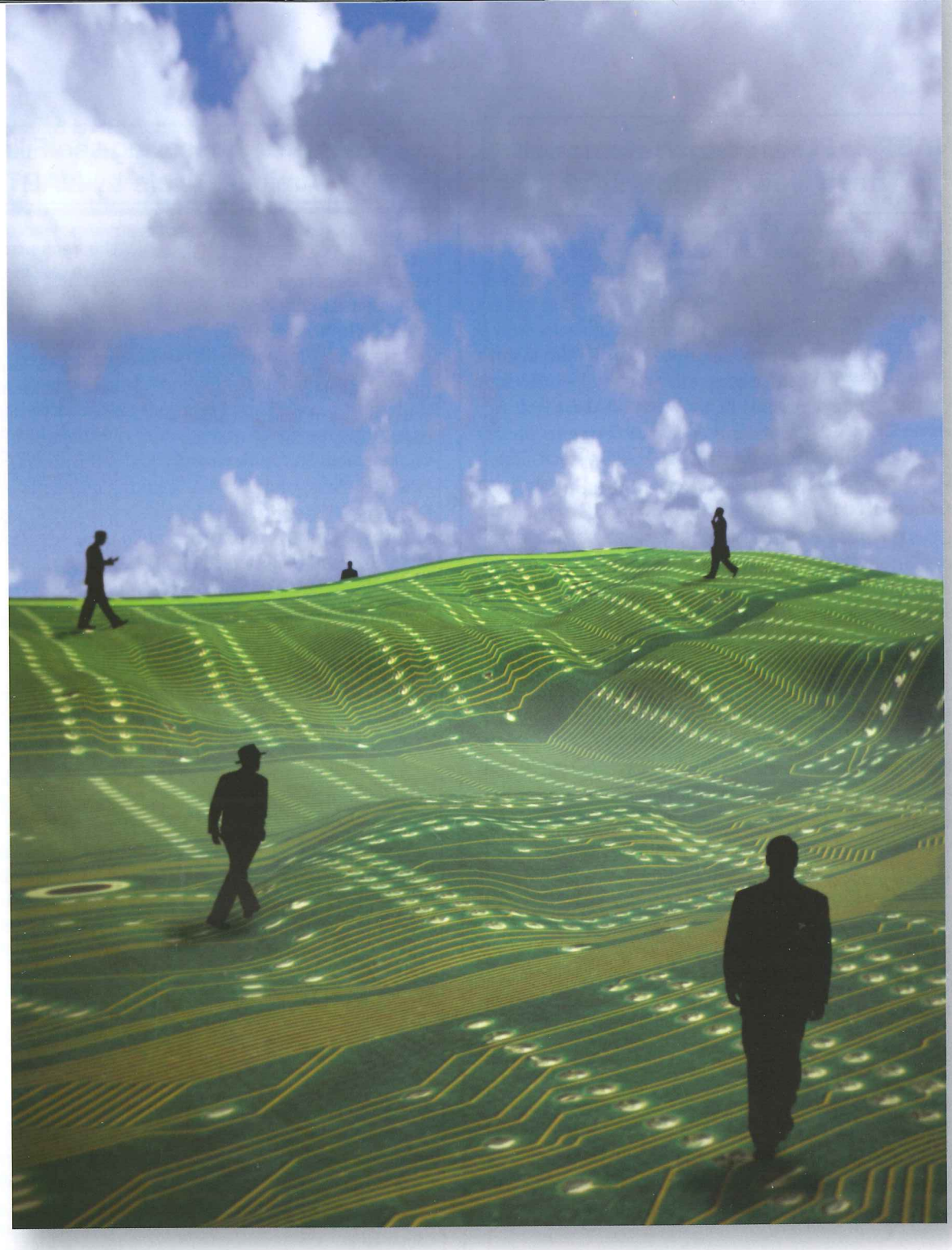


Electronic Discovery: THE BASICS

Sara Anne Hook, M.L.S., M.B.A., J.D.
Indiana University

This article is the first in a series about electronic discovery in bankruptcy. It addresses the basics of electronic discovery, including history, rules and resources. Future articles will apply electronic discovery principles to bankruptcy law practice, review current technologies that can assist with electronic discovery before and during litigation and discuss examples where the failure to properly handle the electronic discovery process properly in bankruptcy cases resulted in sanctions and the lessons that can be learned from these cases.

Introduction

With the series of five decisions in *Zubulake v. UBS Warburg*[1] and the revisions to the Federal Rules of Civil Procedure (FRCP) in 2006, it is fair to say that the legal world entered the electronic age in 2007, particularly as it involves the collection, preservation and use of information in digital form.[2,3] Estimates indicate that between 95 – 99 percent of the information that is being created today is being generated in electronic form. Moreover, studies suggest that as much as 70 percent of this information will never be reduced to paper or other hard copy format. Electronic discovery is not a luxury; it is a necessity in order to glean the information that will be needed to build a case for litigation. The importance of digital assets is clear – and commentary indicates that many corporations that are faced with ongoing litigation are not only proactively preparing for electronic discovery but also adopting an enterprise-wide approach to information management. Another essential point is that there is a natural lifecycle to information.

Clients, counsel, judges and bankruptcy trustees need to understand the requirements for how to handle electronically stored information (ESI), as articulated under the revisions to the FRCP and by evolving case law. Other rules may also be relevant, including the Federal Rules of Evidence, various state court rules and the ABA Model Code of Professional Responsibility (as adopted by each state), as well as federal and state statutes on the privacy of various types of personal, financial, health and government information. Proper handling of electronically stored information is particularly important in order to defend against a claim of spoliation and to avoid being subject to some of the increasingly significant sanctions that are being imposed. This paper provides a framework for understanding electronically stored information and where it might be located, discusses a model of the steps in collecting and preserving electronically stored information, offers some sample preservation letters and considers the risks of spoliation and sanctions.

Depending on the complexity of a client or third-party's computer systems and networks and on the amount of electronically stored information that needs to be collected, preserved, processed and presented, it may be necessary and prudent to utilize the services of a computer forensics expert or a vendor that offers electronic discovery services. This is particularly true as many companies, organizations and individuals turn to cloud computing and Software as a Service (SaaS) vendors to run their software and to manage their confidential information. Likewise, mobile devices, collaborative computing environments and social networking sites may mean that an even larger array of potential sources for electronically stored information must be identified, protected and analyzed. Fortunately, the products and technology that can be deployed as part of an electronic discovery process continue to advance and improve, which will hopefully reduce the time and expense of the process and mitigate the risks of human error, especially for the most labor-intensive stages of the process. A computer forensics expert can be particularly effective in gathering electronically stored information that may have been intentionally or inadvertently altered and in reconstructing a digital footprint of what transpired.

Defining the Concept of Electronic Discovery

According to Lange and Nimsger, electronic discovery is defined as the "application of litigation discovery to electronic documents and data including email, Web pages, word processing files, computer databases, and virtually anything that is stored on a computer."[3] Lange and Nimsger further clarify the definition by noting that documents and data are "electronic if they exist in a medium that can only be read through the use of computers."[4] They note that such media include cache memory, magnetic disks, such as computer hard drives or floppy disks, optical disks, such as DVDs or CDs, and magnetic tapes.[5] Cornick states that "electronic discovery refers to the process of producing and receiving litigation documents in electronic format."[6] Another source defines electronic discovery as "a multi-step process of actively managing, locating and making relevant ESI available for legal, regulatory or compliance reasons."[7] It is thus important to point out that electronic discovery is not limited to litigation or civil law cases.

One important principle behind the revisions to the Federal Rules of Civil Procedure and corresponding changes to state court rules is the desire to consolidate electronic discovery into as streamlined and timely a process as possible. The *Zubulake v. UBS Warburg* decisions were significant in identifying the ongoing duties of counsel, especially related to the preservation of a client's information, the factors to be used in determining whether to shift costs from the producing party to the requesting party and a suggested method for analyzing whether electronically stored information is accessible versus inaccessible. More recently, in *Pension Committee of the University of Montreal Pension Plan, et al. v. Bank of Am. Secs., LLC*,[8] Judge Scheindlin repeated the duty to preserve, described preservation obligations and outlined how to determine the level of culpability (negligence, gross negligence, willfulness) when there is discovery misconduct.[8] Another overarching theme is the expectation that opposing counsel will work cooperatively to develop an elec-

About the Author

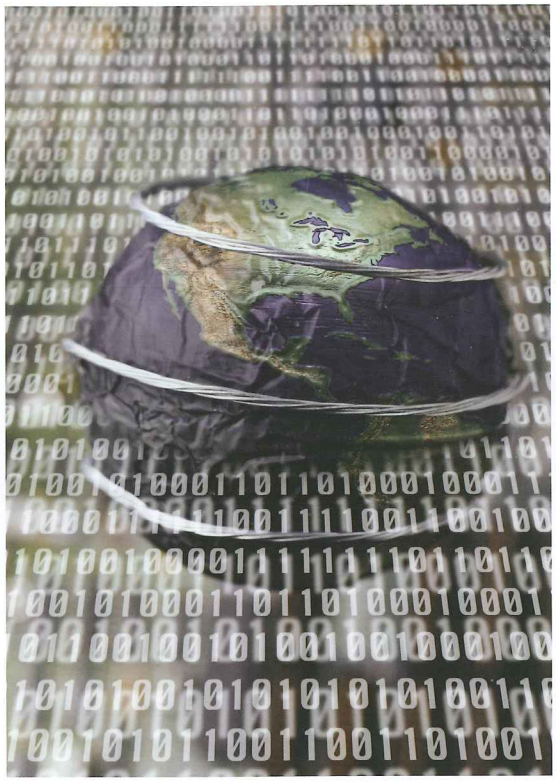
Sara Anne Hook is Professor of Informatics, Indiana University School of Informatics, IUPUI, where she has developed a suite of online courses in the emerging field of legal informatics as well as a course on entrepreneurship. She has also served as Adjunct Professor of Law in the Indiana University School of Law - Indianapolis, where she has taught courses in intellectual property law and professional responsibility. Professor Hook's research interests include intellectual property law, the emerging field of legal informatics, electronic discovery, legal technology, legal research techniques and issues related to privacy and security. She is a member of the American Intellectual Property Law Association (AIPLA), the Indiana State Bar Association and the International Legal Technology Association (ILTA).

tronic discovery plan. An essential facet of electronic discovery is that clients, counsel, third-party vendors and others must act in good faith as well as take reasonable steps to prevent the loss, corruption, or deletion of potentially relevant electronically stored information (ESI) and to be able to document those steps. For example, as stated in the Court of Chancery Guidelines for Preservation of Electronically Stored Information (Delaware), "[w]hat steps will be considered reasonable will vary from litigation to litigation. In most cases, however, a party and its counsel (in-house and outside) should:

• Take a collaborative approach to the identification, location and preservation of potentially relevant ESI by specifically including the discussion regarding the preservation processes an appropriate representative from the party's technology function (if applicable);

• Develop written instructions for the preservation of ESI and distribute those instructions (as well as any updated, amended or modified instructions) in the form of a litigation hold notice to the custodians of potentially relevant ESI;

• Document the steps taken to prevent the destruction of potentially relevant ESI." [9]



Types of Data or Materials Included in "Electronically Stored Information" (ESI)

The term "electronically stored information" or ESI was chosen to encompass not only current information technology, but also to allow for new technology in the future. This term was also selected to make it clear that the intent of the discovery process is that parties be allowed to cast a fairly wide net when thinking about requests for information that might be relevant to a case, at least at the beginning stages of a matter, and when considering a party's duty to preserve. As stated by Cornick, ESI is "a term of art and it is intentionally referred to extremely broadly by the FRCP so that any new form of electronic information will be covered by the rules."[10] Various kinds of ESI that might be discoverable include email, RAM, text messages, chat rooms, message boards, social networking sites, sound recordings and data from any digital device capable of storing information.[11] Note that the language from FRCP Rule 34(a)(1)(A), incorporated by reference in the bankruptcy rules through FRBP 7034, that parties can request "any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[12] As stated by Lange and Nimsger, Rule 34(a) "was specifically amended to expressly recognize ESI as a type of discoverable information" and that "any reference to documents should be understood to include ESI unless it is expressly stated otherwise."[13] It is important to note that requesting parties now can test or sample materials requested under the rule, in addition to the former right to inspect and copy, although testing and sampling is not a routine right.[14] Another point to remember is that the language of the revised FRCP moves beyond a narrow concept of "data compilations" to include all types of electronically stored information.

How Does E-Discovery Differ from Traditional Methods of Discovery?

The basic principles that have always operated in the discovery process have not changed with the revisions to the FRCP or the inclusion of electronically stored information in the set of what can be requested as part of the discovery process. Although attorneys might think about casting a wide net at the outset of litigation in terms of the material that might be requested from the opposing party as well as the duty of their clients to preserve material, the traditional limitations on what is truly discoverable will still apply. These limitations include, but are not limited to, the best evidence rule, foundation and authentication requirements, hearsay, the attorney-client privilege and the attorney work-product doctrine, relevancy and reasonableness. Some new twists in the discovery process that have been introduced through the revisions to the FRCP, the *Zubulake* case and more recent decisions and the changing nature of technology are:

• The multitude of places where ESI may be stored – not just a file cabinet

• The ongoing duties of counsel, especially with respect to issuing and overseeing litigation holds

• The sheer volume of material that must be preserved and reviewed prior to production

• The risk that information that could have – and should have - been protected under the attorney-client privilege or as attorney work-product will be inadvertently produced

• The expense of the electronic discovery process, especially when thinking about clients in a bankruptcy proceeding who may have limited resources

• Native versus image formats - spreadsheets and databases as example, to allow the requesting party to conduct searches and analysis. For a spreadsheet, the requesting party might want to be able to see the formulas and any hidden cells, which would not be apparent if provided only with the final financial report as a stand-alone file or printed/scanned (PDF). Also beware of redacting – which can often be manipulated through software features to reveal the information.

• The increasing harshness of sanctions for spoliation and for failure to participate in good faith in the development of an electronic discovery plan

• The reality that many attorneys are not prepared for – or even aware of – electronic discovery

• The fact that the electronic discovery industry as a whole is still in its infancy – with many more robust technologies still to be developed

• Portable devices, home computers and any other places where parties may be storing information.

• Email messages and other places where information might be located that counsel, trustees and clients may not even think of (photocopiers as example)

• Although The Sedona Conference and other groups have attempted to outline best practices, there is still no standardized approach for how to handle an electronic discovery process

• Clients may be ill-prepared to deal with an electronic discovery process, especially clients in bankruptcy proceedings

• Electronically stored information is fragile and can be altered even by booting up the computer

• There may be a lack of clarity on some issues, such as when information is reasonably accessible versus when it is inaccessible

• The need to hire outside consultants and experts, including computer forensics experts

• The decision on how much of an electronic discovery process should be handled in-house by the client versus outsourced to an electronic discovery vendor – and the selection and ongoing oversight of that vendor

• Metadata and the duty to preserve it in a way that links it with its corresponding files. Metadata is data about data and is generated automatically by nearly any software, including Microsoft Word, without the user even being aware of it. Some of the metadata is also created by settings that the user chooses, such as Track Changes. Metadata is a rich repository for electronically stored information and most courts will insist that files either be produced in native format with the metadata intact or that any documents produced (on paper, for example) are matched with corresponding metadata.

• The opportunity to use sampling and testing

• The requirements for a meet-and-confer conference and for opposing counsel to cooperatively develop an electronic discovery plan

• The safe harbor provision and whether the client has a document retention policy that it is following consistently

• Clawback and quick peek agreements

• The short timelines and deadlines for some of the requirements in an electronic discovery process, including the timing of the meet-and-confer conference and the scheduling order

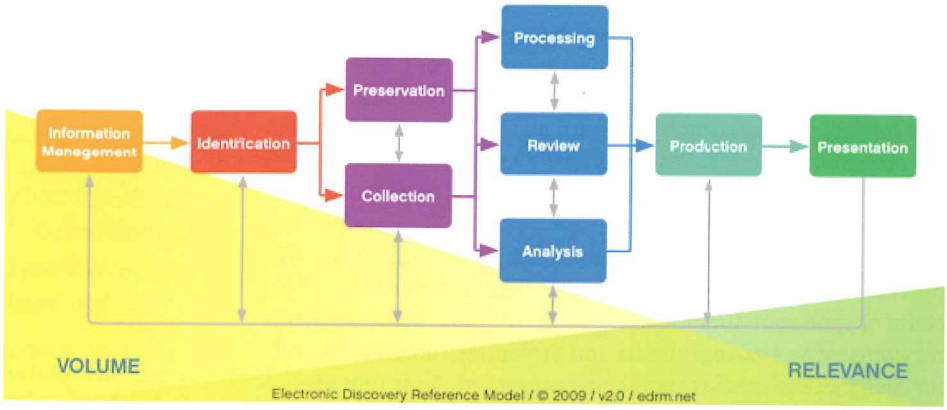
• New training and certification opportunities in electronic discovery

Resources for Learning More about Electronic Discovery

One excellent guide for explaining the process of discovery is the Electronic Discovery Reference Model (EDRM).[15] An important point about the EDRM is that it illustrates that electronic discovery is an iterative process, especially in the middle stages. Note especially how the arrow moves between preservation, collection, processing, review and analysis. Another consideration is that some technologies, such as de-duplication and filtering, may reduce the set of information that then has to be reviewed prior to production by as much as 75 percent.

Another excellent resource for learning more and staying current on electronic discovery is The Sedona Conference.[16] As stated on its website, "[t]he Sedona Conference exists to allow leading jurists, lawyers, experts, academics and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights, to come together - in conferences and mini-think tanks (Working Groups) - and engage in true dialogue, not debate, all in an effort to move the law forward in a reasoned and just way."[17] The Sedona Conference has been a leader in the electronic discovery movement, having promulgated principles and guidelines related to electronic discovery that pre-date the revisions to the Federal Rules of Civil Procedure.[18] Although not binding on courts, the 14 principles and commentary from The Sedona Conference have become an important guideline and may be used as a standard for best practices when determining if an electronic discovery process has been handled appropriately. The Sedona Conference continues to provide publications, conferences, institutes, working groups and other initiatives in support of electronic discovery as well as specialized and complex areas of the law.

Electronic Discovery Reference Model



One of the best resources for information on electronic discovery is the K&L Gates website. Its database provides case summaries, updates on rules and regulations and current news about electronic discovery matters.[19] The law firm is embarking on a project to classify the more than 1,800 cases in its database according to EDRM standards and the cases will be searchable by EDRM classification.[20] Another excellent source for case summaries, rules and statutes and other materials is Kroll Ontrack.[21]

Because of the complexity of the world of digital evidence and the various places that electronically stored information might be located, an important step in any electronic discovery process will be to issue preservation letters – to clients, to opposing parties and to third parties – to any person, company or organization that could have electronically stored information which might be relevant to the case. Two sample preservation letters are avail-

able from Kroll Ontrack – one for the client and the other for an opponent or third party.[22,23] Note some of the preservation obligations outlined on pages 1-2, including the duty to discontinue all data destruction and backup tape recycling policies per FRCP Rule 37(e).[24] In the section Description of Data Sought, note how many different types of data are covered and that the sources of the data include computer systems, removable media and other locations. Notice that in addition to electronic files of various kinds, the preservation letter covers hardware, emails, Internet web activity (remember social media sites and collaborative computer environments), activity logs and supporting information.

The party receiving a preservation letter has the responsibility to disseminate the information to its employees (especially its IT staff and any key employees who were involved in a matter) and for monitoring compliance with all of the terms outlined in the preservation letter. Pages 4-5 of the sample preservation letter describe the expectations regarding data preservation for both online and offline data storage devices. Other important aspects of the preservation phase of an electronic discovery process that will help a party or attorney to defend against a claim of spoliation include using an activity log, securing a mirror image of any storage media and providing a chain of custody for each piece of media that is being preserved. Note that preservation obligations and appropriate protocols extend to electronically stored information that is created even after the letter is received. In other words, there may be an ongoing duty to continue to preserve electronically stored information that the client or third party creates in the future.

Conclusions

Electronic discovery has become a mainstay of law practice and should be a mainstay of trustee practice. Although the process of electronic discovery may seem daunting, there are many resources that can be consulted for a more complete understanding of each stage of the process and where the potential risks might be. As the electronic discovery industry evolves, the technology offered by vendors will evolve to provide more innovative solutions designed to reduce costs and minimize the chances for human error and the spoliation of evidence. As more cases are decided, there will be more guidance available on some issues related to electronic discovery that may not be clearly resolved at this point, but there will also be a greater expectation from courts that attorneys, clients and bankruptcy trustees will handle the process in keeping with the rules, tools and best practices.

Footnotes:

1. 217 FRD 309 (*Zebulake I* SD NY 2003), 55 FRS 3d 622 (*Zebulake II*- SD NY 2003), 216 FRD 280 (*Zebulake III* SD NY 2003) , 220 FRD 212 (*Zebulake IV* SD NY 2003) and 229 FRD 422 (*Zebulake V* SD NY 2004).
2. Kroll Ontrack, Zubulake v. UBS Warburg, http://www.krollontrack.co.uk/zubulake/, accessed 8/1/11.
3. Cornell University Law School, Legal Information Institute, Federal Rules of Civil Procedure, http://www.law.cornell.edu/rules/frcp/, accessed 8/1/11.
4. Lange, Michele S.C. and Nimsger, Kristin M. *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, 2nd ed. Chicago, IL: American Bar Association, 2009, p. 404.
5. Id.
6. Id.
7. Cornick, Mattew S. *Using Computers in the Law Office*, 6th ed. Clifton Park, NJ: Delmar Cengage Learning, 2012, p. 148.
8. US Dist. LEXIS 4546 (S.D. NY 2010)
9. E-Discovery in Bankruptcy Cases: Everything You Need to Know to Be Prepared (White Paper), RenewData, March 2009. http://www.renewdata.com/, accessed 2/11/11.
10. *Pension Committee of the University of Montreal Pension Plan, et al. v. Bank of Am. Secs., LLC,* 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).
11. Court of Chancery Guidelines for Preservation of Electronically Stored Information (Delaware), http://www.delawarebusinesslitigation.com/2011/01/articles/case-summaries/electronic-discovery/court-of-chancery-guidelines-for-preservation-of-electronically-stored-information/, accessed 8/1/11.
12. Cornick at 150.
13. Wilson, William L. Digital Copiers & Confidential Information – What You Need to Know. *Res Gestae*, July/August 2010, pp. 34, 36.
14. Legal Information Institute, Cornell University Law School, Federal Rules of Civil Procedure, Rule 34, http://www.law.cornell.edu/rules/frcp/Rule34.htm, accessed 8/1/11.
15. Lange and Nimsger at 47.
16. Id.
17. The Electronic Discovery Reference Model, http://edrm.net/, accessed 8/1/11.
18. The Sedona Conference, http://www.thesedonaconference.org/, accessed 8/1/11.
19. TSC Mission, http://www.thesedonaconference.org/content/tsc_mission/show_page_html, accessed 8/1/11.
20. The Sedona Principles: Second Edition. Best Practices Recommendations & Principles for Addressing Electronic Document Production, June 2007.
21. K&L Gates E-Discovery Case Database, http://www.ediscoverylaw.com/articles/ediscovery-case-database/, accessed 8/1/11.
22. K&L Gates, EDRM Collaborate to Enhance E-Discovery Database, http://www.ediscoverylaw.com/2011/01/articles/news-updates/kl-gates-edrm-collaborate-to-enhance-ediscovery-database/, accessed 8/1//11.
23. Kroll Ontrack, Resource Library, http://www.krollontrack.com/resources/, accessed 8/1/11.
24. Kroll Ontrack, Sample Preservation Letter – To Client, http://www.utahbar.org/cle/fallforum/materials/sample_preservation_letter.pdf, accessed 8/1/11.
25. Kroll Ontrack, Sample Preservation Letter – To Opponent or Third Party, http://www.utahbar.org/cle/fallforum/materials/sample_preservation_letter_opponent.pdf, accessed 8/1/11.
26. Legal Information Institute, Cornell University Law School, Federal Rules of Civil Procedure, Rule 37, http://www.law.cornell.edu/rules/frcp/Rule37.htm, accessed 8/1/11.

JOURNAL OF THE NATIONAL ASSOCIATION OF BANKRUPTCY TRUSTEES

NABTALK®

IN THIS ISSUE:

Stern v Marshall: Bleak House Revisited

Electronic Discovery: The Basics

Practical Compliance With Bankruptcy Code Section 704(A)(11)

First Circuit Adopts the "Separate Filings Rule" In Allocating a Refund Between a Debtor and a Nondebtor Spouse

Problems of Dealing with Limited Liability Company Interests

FALL 2011
VOLUME 27
ISSUE 3