
DISCOVERY OF ELECTRONIC EVIDENCE IN CIVIL LITIGATION: A DEFENSE PERSPECTIVE

By David H. Schultz and Michele C.S. Lange

KROLL ONTRACK, INC.



Winning or losing a case may hinge on that one piece of evidence that could be buried among the pages of produced documents resulting from a broad-scale discovery request. That's why lawyers in America spend more time on discovery than they spend on most other aspects of their case. Given today's rapid techno-

Given today's rapid technological advances, the complexities of discovery have only increased, placing even more significance and scrutiny on the discovery process.

logical advances, the complexities of discovery have only increased, placing even more significance and scrutiny on the discovery process. As stated by U.S. Magistrate Judge Sidney Schenkier this means that, "At some point, a party and/or its attorneys must be held responsible for knowing what documents are discoverable and where to find them." *Danis v. USN Communications*, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000). He prefaced this statement by reasoning that attorneys cannot create a loophole in the discovery rules by allowing counsel to argue: "Judge, we just didn't know those tapes existed."

DAVID H. SCHULTZ (dschultz@krollontrack.com), a Senior Legal Consultant at Kroll Ontrack Inc. in Eden Prairie, received his law degree from Hamline University School of Law and his undergraduate degree from the University of Wisconsin – Eau Claire.

MICHELE C.S. LANGE (mlange@krollontrack.com), a Staff Attorney at Kroll Ontrack Inc., received her law degree from the University of Minnesota Law School and her undergraduate degree from the University of Wisconsin – La Crosse.

As a defense attorney in the twenty-first century, you no doubt have heard about – or maybe even experienced – Judge Schenkier's warnings or the impact that the electronic explosion is having on legal discovery. You have likely made or received a discovery request like one of the following:

- Request #10: Provide all financial/accounting records (including paper and electronic records) for the years 2002 - present.
- Request #26: Produce all records (email and attachments inclusive) relating to the marketing, development, and sale of the product for the past five (5) years.

Counsel defending today's companies are encountering new challenges given the proliferation of electronic evidence. As judges across the country and right here in Minnesota have noted, you now have a duty to know where electronic evidence resides and how you are going to produce this information in litigation. This article seeks to guide Minnesota defense lawyers through the e-discovery process – from preservation to production – to help you gain the strategic edge in your next case involving anything "e."

RETENTION, PRESERVATION AND SPOILIATION

Years ago, corporations tended not to retain hard copies of documents for long time periods because paper documents took up volumes of physical space. Corporate executives gave document purging more attention because storage rooms and warehouses had a physical limit on the amount of data that could be saved. Today, however, because of the relative ease and little expense with which data can be stored, companies save copies of nearly every electronic document somewhere. For example, a single 40 gigabyte backup tape can hold between three- and four-million pages of text and a single two gigabyte hard drive can hold between 150,000-200,000 pages of text. A closet full of antiquated backup tapes, hard drives and floppies that was long forgotten by the document retention team could now potentially house billions of documents in electronic form – thereby creating a discovery nightmare without the appropriate policies in place.

Most electronic evidence resides on backup tapes which are typically created for disaster recovery purposes. These backup tapes usually are rotated in a regular fashion (e.g., a set of seven tapes are recycled weekly when creating daily backups). Volumes of other data also commonly reside on individual hard drives on computers used by employees. This data is highly fluid, and documents and metadata (i.e.,

information about a document or “the data about the data,” which is typically saved automatically within a document) may be altered and overwritten with each use of the machine. In addition, trails of electronic data can also exist on a myriad of other media, including: removable media (e.g., floppy discs, CDs, DVDs, USB devices), personal digital assistants (e.g., Palm Pilots, Blackberries, cell phones with email capabilities), and various archival data media (e.g., cartridges, optical disks).

Retention and preservation is perhaps the single most dangerous sub-topic under the umbrella of electronic evidence – that is, the retention of electronic documents, databases and emails in an organization’s ordinary course of business and the preservation of those documents when litigation is either anticipated or pending.

Increasingly, defense counsel will see that plaintiffs with little or no electronic data themselves will aggressively pursue email and other electronic files from their opponents.

Increasingly, defense counsel will see that plaintiffs with little or no electronic data themselves will aggressively pursue email and other electronic files from their opponents. The goal, from the plaintiffs’ perspectives, is more commonly to create a spoliation problem instead of actually obtaining and reviewing hundreds of thousands of pages of electronic files. Courts have not shied away from sanctioning attorneys for e-data spoliation as a result of their failure to fully discontinue backup tape recycling policies (intentionally or negligently) or improperly collect and image hard drives. Sanctions for spoliation of evidence vary but include: adverse inferences or presumptions, inadmissibility of evidence, monetary sanctions, assignment of costs, and, worse, dismissal or default.

Organizations can protect themselves against a potential spoliation accusation and its consequences by striking a balance between appropriate destruction of stale documents and adequate preservation of potentially significant documents. Such balance leads to effective electronic document management and the protection of a company’s information assets.

Successfully addressing the issue of document retention requires your clients to:

1. Develop and implement a thorough and thoughtful electronic document retention policy.
2. Create a litigation response team, comprised of outside counsel, corporate counsel, human resources department, business line managers, and IT staff, and charged with handling electronic document preservation efforts should litigation or investigation ensue.
3. Cease document destruction policies at first notice of suit or reasonable anticipation of suit.
4. Audit your document retention policies to ensure they are adhered to.
5. Regularly train employees on your data retention policies.

As a member of the team developing an electronic document retention policy, you should note that a document retention policy that is right for one organization in one industry might not be right for the next one. These policies will vary depending on the size of the organization and the industry in which the organization operates. Nevertheless, the bulk of any retention policy should include a method for determining retention classes for various document types (e.g., human resource documents, payroll documents, tax documents, research and development documents), the retention periods for each class, the retention procedures, and a records custodian. The policy should create an index of active and inactive records and implement “log books” in which all destroyed documents are recorded.

Most important, a corporation must retain all relevant documents when they know, or should have reason to know, that the documents will become material at some point in the future. Courts recognize willful destruction of documents as a serious offense, and they tend to issue severe sanctions for intentional spoliation.

In the wake of pending or impending litigation, you should consider the following action-items:

- Company executives should give a preservation notice to all employees who may come in contact with potentially relevant data.

- Litigation response teams should be called into action to enforce document preservation.
- If the company uses automated software to destroy records, these programs should be halted.

THE E-DISCOVERY PROCESS

Once the initial preservation considerations have been addressed, defense counsel should keep in mind the ongoing need to manage electronic discovery using legal tactics and technical tools. The e-discovery process can best be broken down into five basic steps.

Step 1: Define the Scope of E-Discovery

Most important, a corporation must retain all relevant documents when they know, or should have reason to know, that the documents will become material at some point in the future. Courts recognize willful destruction of documents as a serious offense, and they tend to issue severe sanctions for intentional spoliation.

Defense counsel can reduce the scope of electronic documentation subject to discovery through either stipulation or protective order. In doing so, four classes of electronic data should be addressed: (1) active data (i.e., that which is immediately and easily accessible on the client's systems today) (2) archived data (i.e., that which resides on backup tapes or other storage media) (3) deleted data (i.e., that which has been deleted from a computer hard drive but is recoverable through computer forensic techniques, and (4) legacy data (i.e., that which was created on old or obsolete hardware or software). Typically, litigation will require production of electronic files from only one or two of these classes of data. By either agreeing that discovery will not encompass certain of these data sets or obtaining a court order preventing discovery of them, all parties and the court will benefit.

If faced with a broad-based document request or subpoena for "all electronic data," you should consider objecting based on the burden and expense as courts have been unsympathetic toward litigants merely engaging in costly e-fishing expeditions. Rather, courts have ordered parties to limit their requests by time frames, data locations, and subject matter. Defense counsel would be wise to consider consulting an experienced electronic discovery expert at this point to help quantify the volume of data involved and assist in demonstrating the unreasonable burden and expense to the court if necessary.

At the beginning of any e-discovery project, counsel must define the scope of the project. Consider the following questions:

- What type of information is involved? Where is this information located?
- Which employees are involved in the suit? How do they typically maintain their data?
- What is the best manner for collecting that information?
- How will the documents be reviewed for responsiveness and privilege?
- What are the deadlines for completing the discovery review?
- What format must the documents be produced in to the opposing party?

Step 2: Collect the Data

After identifying the data sought, locating where it resides, and exhausting all objections to limit the production, defense counsel must collect the data for review and prepare for production.

Before the e-explosion, a partner in charge of litigation, when faced with a discovery request, typically sent a team of associates into a client's offices to collect and copy documents from the key users or "document custodians" who likely possessed discoverable materials. On average, this "discovery sweep" could amass as much as 50,000 documents per case – or enough documents to fill 15-20 standard bankers' boxes. This process was a feat, but not unconquerable. If the opposing party pushed for email and electronic files, the producing party routinely had to print those documents as well. Again, this was a feat, but not unconquerable as long as the number of documents and emails only totaled in the several thousands of pages. But with regard to electronic evidence in the modern era, producing parties might very well have to sift through as much as three million documents, making opening and printing each and every document simply untenable.

The e-explosion has necessarily changed the way a partner in charge of litigation responds to discovery requests. The partner will still likely send a team to collect information. But today's document collection teams will typically gather back-

up tapes, hard drives (if the hard drive can be removed from commission), and floppies instead of gathering voluminous paper documents.

Step 3: Filter & Process the Data

In most cases, keeping the data in an electronic format makes sense. Typically parties retain a computer expert to convert the data to a common, read-only format such as "tiff" (tagged image file format) to ensure authenticity. This conversion allows documents and emails, including all attachments, to be processed rapidly without the need to open the file in its original format. It also permits documents to be automatically Bates numbered and "branded" with overlays in the margins (e.g., "Confidential" or "Work-Product"), if desired. Other benefits include the ability to search for keywords more quickly and efficiently and to allow for annotations and redactions directly on the documents without altering the original electronic file.

- **Custodian filtering** – segregating the key custodians who may be relevant to the case and isolating the files associated with those specific individuals;
- **Time and date filtering** – targeting discrete periods of time, which are particularly relevant to a case or which are required to be produced in accordance with a pending court order;
- **File Size Filtering** – capturing files between a certain size range in order to isolate mid-sized files from exorbitantly large files;
- **Keyword searching** – applying a set of keywords and terms to segregate potentially responsive information for further review and scrutiny; and,
- **De-duplication** – identifying documents that are duplicates of one another and eliminating these duplicate documents from the review and production set of documents.

Step 4: Choose Review Options & Conduct Review

After gathering the data on hard drives, floppies, backup tapes, and servers and reducing the universe of discoverable documents using a variety of filtering techniques, the coordinating attorney must determine the data format for the internal review and contemplate the next step – the physical production of those documents to the court, governmental agency, and/or opposing party. In most cases, two options exist for review – paper and electronic.

If the coordinating attorney chooses a paper review, the electronic documents are printed. This process requires counsel to verify that each document's metadata will be burned to a slip-sheet or cover sheet in front of the document text. In the alternative, counsel may choose to brand the document with a printed overlay on the corners of the document containing the same pertinent metadata information. Failure to provide this valuable information about the document (such as create, access, or modification dates) and email (such as "bcc" recipients and attachments) could potentially lead to the loss of this information since it might not print when the "print" button is pushed. Once the documents are printed, they are shipped to a team of reviewers who divide up the boxes and review them document by document.

Using some type of local litigation support database or Web-based document review repository provides another option for reviewing documents for responsiveness or privilege. Litigators faced with electronic document productions have found using an electronic reviewing option more appealing since it typically provides greater flexibility and efficiency over paper review. Such a review can generally occur in three ways: (1) looking at a collection of "loose" electronic files in their "native" format on a CD-ROM or DVD, (2) using a local database (like Summation or Concordance) or (3) working with an online document review repository – a Web-based database into which the data files have been loaded for viewing, categorization and searching. While a review team may conduct an electronic review exclusively in one of the three general forms mentioned above, the size and nature of the case may dictate the use of all three in varying amounts.

Step 5: Choose Production Options & Produce

Once completing the review identifying all documents as responsive, non-responsive, privileged, or the like, counsel must focus on producing the responsive documents to the opposing party, court, or government. Counsel must address these two questions: (1) what format will the documents need to be produced in, and (2) in what timeframe must the production occur? Defense counsel are advised to address these questions long before the document review ever begins, typically at some of the first discovery planning conferences with the opposing party or court. Given the fact that an overwhelming majority of corporate documents appear in electronic form, production in electronic format is becoming an increasing requirement and should not come as a surprise to counsel.

YOUR ETHICAL OBLIGATIONS

The complexities associated with e-discovery come with increased ethical obligations and risks – not unlike other areas of the law. Lawyers with busy practices often operate in a head-down, shoulder-to-the-grindstone fashion – and managing a heavy caseload while finding time to stay abreast of litigation trends may seem like an untenable task. Yet, a single e-discovery oversight could have sizeable consequences, placing you and your client at risk for judicial sanction, in addition to any ethical violations or malpractice claims you could face on your own.

Judicial Sanctions – Attorneys who are uneducated about e-discovery best practices or knowingly shun the duty to produce electronic documents in their cases may face unsympathetic courts. For example, in a labor dispute case, *Metropolitan Opera Assoc., Inc. v. Local 100*, 212 F.R.D. 178 (S.D.N.Y. 2003), the defendants failed to comply with discovery rules, specifically failing to search for, preserve, or produce electronic documents. The court found that defense counsel: (i) gave inadequate instructions to their clients about discovery obligations; (ii) disregarded that the defendant had no document retention system; (iii) delegated document production to a layperson, who was not instructed as to the scope and procedure of producing documents; and (iv) blatantly disregarded the courts' and plaintiff's repeated discovery requests by responding with baseless representations that all documents had been produced. The court granted severe sanctions, finding liability on the part of the defendants and ordering the defendants to pay plaintiff's attorneys' fees necessitated by the discovery abuse by defendants and their counsel. Other common law sanctions for improper handling of e-discovery have included: adverse inferences, dismissal or default judgment, restrictions on admissible evidence, assignment of costs, or monetary penalties.

Ethical Violations – In addition to judicial sanction, most states have professional responsibility rules requiring attorneys to perform legal services with diligence, competence, faithfulness and good judgment and not unlawfully obstruct, alter, or destroy another party's access to evidence. For example, in Minnesota, Rule of Professional Conduct 1.1 states, "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation" and Rule 3.4 states, "A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document

or other material having potential evidentiary value." Failing to understand the e-discovery process, neglecting to consider electronic documents and email, or hiding potentially relevant digital evidence could put counsel at risk for an ethical violation. While the first ethical charge for failing to properly handle e-discovery has yet to be notably published, understanding e-discovery best practices will help counsel gain a strategic edge in their cases and avoid disciplinary action by their state bar under these and other professional responsibility rules.

Malpractice Claims – Lastly, it is reported that the number of legal malpractice cases is increasing at a rate greater than the growth of the legal industry, and the ABA reports that substantive errors account for 46% of all legal malpractice claims – failure to know the law, follow deadlines, or conduct adequate discovery. Failing to stay abreast of technology's impact on the law could place counsel at risk for a malpractice claim. At a Washington, D.C. conference in the fall of 2003, Judge Preska, the author of the Metropolitan Opera decision, explained that it is "hard to say" whether an attorney's failure to seek electronic discovery in a case could support a finding of legal malpractice. "The rules talk about the production of relevant information, so we seem to create the burden to seek e-data," Judge Preska wrote. While noting that the increased costs associated with e-discovery "have changed the game," she added that she "can't imagine how counsel who is responsible cannot seek relevant electronic information." (See Patrick F. Dorrian, *Jurists Offer Perspective, Tips on Electronic Discovery*, Metropolitan Corporation Counsel (Nov. 2003).

The bottom line is that if your client, under your advice and direction, does not properly retain, preserve, collect, and produce electronic documents, the mistakes could be costly. To help avoid judicial sanctions, ethical violations, or malpractice claims practitioners must understand the details of preserving, requesting, and producing email, word processing documents, spreadsheets, databases and more.

CONCLUSION

Now more than ever before, for attorneys to effectively litigate a matter, they require a basic understanding of technology (and in some cases thorough computer proficiency). No longer can parties or their defense counsel claim to be unaware of digital data as judges are increasingly expecting e-savvy litigators in their halls of justice. While in Minnesota very little binding precedent exists in this area – stay tuned –

such authority likely lurks right around the corner. Additionally, astute Minnesota litigators will consider developments across the country when seeking e-discovery guidance, as courts outside Minnesota consistently reference a handful of seminal cases on these technical issues.

The moral of the story: e-discovery presents new challenges for today's defense attorney. The good news is that the problem is not unconquerable. Defense counselors have several options for dealing with electronic documents and email and finding the most appropriate, cost-effective solution for each particular matter. ▲

SEMINAL CASES

Electronic Evidence is Discoverable: "The law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced...[T]oday it is black letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995). See also *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003), *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001); *Linnen v. A.H. Robins Co.*, 1999 WL 462015 (Mass. Super. June 16, 1999).

Deleted Data can be Discoverable: Deleted electronic evidence is fully discoverable. *Dodge, Warren, & Peters Ins. Servs. v. Riley*, 2003 WL 245586 (Cal. Ct. App. Feb 5, 2003); *Simon Property Group v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000).

Duty to Preserve E-Evidence: There is a duty to preserve evidence that parties know, or should know, is relevant to the ongoing litigation, including preservation of all data compilations, computerized data and other electronically-recorded information. *Kleiner v. Burns*, 2000 WL 1909470 (D. Kan. Dec. 15, 2000); *Danis v. USN Communications*, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000).

Spoilation Sanctions Defined: Failure to preserve email and electronic documents (whether intentional or inadvertent) is sanctionable as spoliation of evidence. *Metropolitan Opera Assoc., Inc. v. Local 100*, 2003 WL 186645 (S.D.N.Y. Jan. 28, 2003); *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d. Cir. Sept. 26, 2002).



The Manual... everything you need to know about Minnesota's automobile coverage law and more...

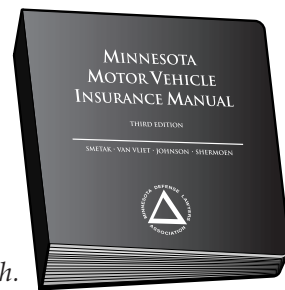
is covered in the now available *Minnesota Motor Vehicle Insurance Manual* (3d Ed). Authored by Theodore J. Smetak and Eugene Shermoen, Jr., Arthur, Chapman, Kettering, Smetak & Pikala, P.A., and Karen Melling van Vliet and Gregory J. Johnson, Johnson & van Vliet, LLP.

Now includes 2004 Update!

An absolute "must have" reference tool for any attorney, plaintiff or defense, working in the automobile accident areas.

A masterful treatise!!!

It is really a first rate piece of work – clear, concise and thorough.



To order
Minnesota Motor Vehicle Insurance Manual (3d Ed.)
call MDLA office (612) 338-2717, fax (612) 338-9148,
or fill out the form below.

MDLA members	\$145
Non-Members	\$165
Includes Shipping and Handling	
SPECIAL Judicial/Library Rate	\$ 75
Quantity discounts available.	
2004 Update!	\$ 30

ORDER FORM

NAME _____

FIRM _____

ADDRESS _____

CITY _____

STATE _____ ZIP _____

TELEPHONE (____) _____

E-MAIL _____