

ELR

NEWS & ANALYSIS

E-Discovery: An Environmental Professional's Guide

by Brian Wm. Higgins

Editors' Summary: The e-discovery rules promulgated last December, now endorsed by several states, are sweeping in scope and have the potential to change the course of litigation. In this Article, Brian Wm. Higgins summarizes the major e-discovery requirements of interest to environmental professionals, including lawyers, managers, consultants, and information technology staff. Using a hypothetical case as an example, he provides a practical guide for navigating and complying with the new rules.

I. Introduction

Imagine you are the Chief Executive Officer (CEO) of a global manufacturing company that recently experienced an uncontrolled release of hazardous air pollutants from one of your facilities, a release that adversely affected nearby residents and the environment. At the end of a meeting with local citizens concerning the release, an attorney for a prospective plaintiff approaches you and states: "You'd better get your discovery documents in order because you'll be hearing from us."

No stranger to litigation, you question your General Counsel about the Federal Rules of Civil Procedure governing the production of electronic information that you'd heard became effective in December 2006. What you learn leaves you wondering what to do next. After all, your company generates massive amounts of electronic data, including plant status reports, e-mails, continuous emissions monitoring data, environmental management system information, and financial spreadsheets, all of which will have to be collected, scrubbed, and potentially turned over to the plaintiffs' attorneys during discovery when you are sued. Unfortunately, your company's existing and legacy computing systems, scattered databases, and backup systems, coupled with an unregulated corporate document retention policy, will make it nearly impossible to successfully comply with the new rules. With the prospect of severe sanctions potentially turning the tide during the anticipated litigation, you instruct your General Counsel and Chief Technology Officer to develop an electronic discovery plan that you can report to the Board of Directors by the day's end.

Given the myriad issues raised by the prospect of a class action toxic tort suit, it may seem contrived to suggest that the first issue on the CEO's mind is electronic discovery.

Yet, many authorities and experienced litigators have noted that the discovery of electronic documents and information has become the centerpiece of every litigation.¹ That attention is due to the ever-increasing volume of highly relevant documents and information being transmitted and stored electronically. In fact, it has been reported that up to 92% of business' new information, and up to 60% of critical information, is stored electronically, and most of that information is *only* stored electrically.² Thus, the proverbial "smoking gun" documents for which every plaintiff's attorney searches are likely to be found amid a daunting volume of what the Federal Rules call "electronically stored information."

Under the new December 2006 e-discovery rules (which have been endorsed by several states), courts now expect that all potential parties to litigation will, as soon as litigation is reasonably anticipated, put a "litigation hold" into effect to prevent (not just reduce) the destruction of electronic information and materials (as well as hardcopy information) that have been or will be created before or during the course of a lawsuit.³ But that is just the beginning of a lengthy and expensive process of complying with the new rules.

This Article presents a summary of the major requirements that will impact the environmental professional, including those professionals who have a direct hand in litigation, which may include environmental managers, consultants, in-house attorneys, and information technology/information management (IT/IM) professionals. The new e-discovery rules are sweeping in their scope, and they

Brian Wm. Higgins is an attorney practicing in the Washington, D.C., office of Blank Rome, L.L.P. He holds degrees in law and environmental engineering, and is a licensed Professional Engineer. He can be reached at Higgins@blankrome.com.

1. See, e.g., E-Discovery and Document Retention, <http://www.steptoe.com/practices-78.html> (last visited May 3, 2007).

2. Paula F. Schauwecker, *Electronic Discovery and the Environmental Litigator*, 20 NAT. RESOURCES & ENVT. 68 (2006); Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. OF TECH. & INTELL. PROP. 171 (2006).

3. See *supra* note 1.

have teeth, in the form of sanctions that can change the course of litigation.⁴

II. E-Discovery Requirements

A. When Must I Start Preserving Documents and Data?

There are two broad aspects of the new e-discovery rules: preservation of electronically stored information, and production of that information according to specific procedures early and throughout litigation.⁵ Both events are triggered when a party is put on notice of, or reasonably anticipates, litigation. Thus, compliance with the rules should begin promptly when, for example, a federal or state environmental regulatory agency initiates an action against an individual or company, such as a Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) cost recovery action or an enforcement action against a permit violator, or when, for example, an individual threatens or initiates a cause of action against others, such as the toxic tort action described in the introduction.⁶

Table 1 lists examples of environmental-related causes of action that could potentially invoke the federal (and/or state) e-discovery rules and require a litigation hold on, and subsequent production of, electronically stored information.

Table 1. Types of Environmental Actions Potentially Triggering Rules Regarding Production of Electronically Stored Information⁷

Federal/State Agency Actions	Private Party Actions
Cost Recovery Under CERCLA/State Law	Toxic Tort Suits
Enforcement of Resource Conservation and Recovery Act Violations	Other Class Action Suits
Enforcement of Clean Air Act Violations	Nongovernmental Organization Litigation
Enforcement of Clean Water Act Violations	Citizen Suits Under Environmental Statutes
Enforcement of Toxic Substances Control Act Violations	Cost Recovery/Cost Allocation
Other Enforcement Compliance Assurance	Petitions of/for Agency Review
Enforcement of State Permit Violations	

But what exactly does “on notice” mean in the context of those actions? The Federal Rules do not clearly define when someone is on notice of litigation in every situation identified in Table 1. Some examples, such as the service of a summons and complaint, are obvious; but others are less clear.

4. Paul Benson & Juan Ramirez, *Avoiding the Electronic Discovery Trap: Weighing the Burden of Production Against Benefits of Compliance*, Wisconsin Technology Network, Apr. 17, 2006 (“Companies that do not keep pace with evolving laws related to electronic discovery do so at their own peril and invite a finding of spoliation, which often signals the death knell to an otherwise meritorious case.”).

5. See generally Fed. R. Civ. P. Rules 26(a), 26(f) (Dec. 1, 2006).

6. Schauwecker, *supra* note 2.

7. *Id.*

Some have suggested that a party is on notice of litigation when it receives pre-litigation communications from another party.⁸ For example, a private party may, as a prelude to litigation, send a cease-and-desist or demand letter to another party, or provide an oral warning, such as in the case of the introductory hypothetical. A regulatory agency may issue and serve on a party a written Notice of Noncompliance or a Notice of Violation concerning an operating permit, which can lead to litigation.⁹ The U.S. Environmental Protection Agency (EPA) may send a communication to a potentially responsible party seeking historical information about wastes it disposed of at a National Priorities List site, which could ultimately result in a cost recovery action by EPA or third parties.

Others have suggested that, in addition to pre-litigation communications, a party may be on notice when it receives a discovery request from a third party or a discovery order issued by a court.¹⁰ A party may also be on notice as a result of a prior lawsuit, or when it has actual knowledge of a violation of an environmental operating permit that may lead to enforcement actions or the issuance of a Notice of Violation. A party that obtains a patent on an environmental technology, where a noninfringement opinion was sought from an attorney because the new technology was viewed as potentially infringing patents owned by a competitor, should act as if it is on notice of potential litigation by the mere act of selling the new technology in the market.

Thus, in some circumstances a party will have little trouble understanding that it has been put on notice of actual or potential litigation, but other circumstances may not be so clear.¹¹ Unfortunately, one looking for judicial opinions that have addressed the issue of notice will find little guidance, and until the body of judicial interpretations concerning the new e-discovery rules grows, potential litigants will have to work through the notice issue on a case-by-case basis. Rather than struggle to identify a bright line when a company should begin complying with the new rules, however, it may be prudent to instead weigh the risks of not complying, and then consider taking a long-term conservative approach that avoids potential sanctions. Of course, with such unclear legal boundaries, it would also be wise to seek legal input when analyzing situations that fall within the gray areas.

B. What's the First Thing I Must Do After I've Been Put on Notice?

As suggested above, once a party is on notice of actual or potential litigation, it must promptly put a litigation hold on its documents and information to prevent the unintentional destruction or loss of what could ultimately be discoverable evidence. This is especially important in the context of electronically stored information because of the increased chance (compared to paper documents) that the

8. *Id.*

9. *Id.*

10. See, e.g., *id.*

11. Withers, *supra* note 2 (noting that “the duty of preservation has consistently been held to attach when a person knows of or reasonably anticipates litigation involving identifiable parties and identifiable facts.”).

information might be overwritten or deleted in the normal course of business.¹²

Recent statistics support the need to put a litigation hold on electronically stored information as soon as possible. One analysis of 2006 e-discovery opinions issued by judges in the United States (over 175 cases) found that 43% of those opinions addressed the related issues of document preservation, litigation hold, spoliation of documents, and related sanctions.¹³ A comparatively smaller number of cases addressed the merits of the electronic discovery requests themselves. What this suggests, of course, is that courts are increasingly focusing on the procedures litigants employ to preserve information.

For a litigation hold to work as it was intended, a company that is on notice of actual or potential litigation should immediately communicate its expectations concerning the destruction or loss of documents to all employees, and then monitor employee compliance on a regular basis. A single communication at the beginning of a lawsuit may not be sufficient to avoid sanctions, especially when it can be foreseen that the litigation will extend several months (or years), such as in the case of a complex toxic tort matter potentially involving dozens or hundreds of plaintiffs and/or class members.

There is a wide range of electronically stored information that is generated by companies doing business in the environmental sector, all of which may need to be secured from destruction and loss and then eventually produced. Electronically stored information includes writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained.¹⁴ Thus, e-mails, consultant-generated or internal-generated reports, environmental management system data, stack continuous emissions monitoring data, process parameter monitoring data, laboratory test data and reports, modeling input and output files, compliance reports, hazardous material and hazardous waste transportation records, storage and inventory data, and meeting notes, are all fair game under the e-discovery rules. Table 2 summarizes some of the types of electronically stored information commonly associated with environmental sector activities that could be covered by the rules.

Table 2. Categories of Environmental Information Potentially Subject to Discovery

E-mail
Locally stored on individual computers and peripherals
Centrally stored on e-mail servers
Backup storage tapes
Reports
Emissions inventories
Routine maintenance
Unit operations analyses
Consultant evaluations
Property records
Employee activity records
Environmental monitoring system data
Input/output data
System status data
Waste tracking
Material tracking
Stack monitoring data
Continuous emissions monitoring
Sample collection and conditioning data
Manufacturing information
Parameter monitoring data
Status data, e.g., temperatures, pressures, flow rates
Lab results
Quality assurance test results
Sample testing
Modeling data
Permit-related air dispersion modeling
Accidental release modeling
"What if" scenario assessments
Meteorological data
Health risk assessments

Obviously, a company cannot prevent the destruction and loss of discoverable electronically stored information if it does not know the location of that information. Thus, as discussed below, it would be prudent to immediately begin developing an inventory of that information.

C. My Litigation Hold Is in Effect, Now What?

Once those responsible for complying with the new e-discovery rules have implemented procedures to preserve discoverable electronically stored information, the physical or virtual location of that information must be identified. This requires a comprehensive understanding of how a companies' computer and back-up systems work, followed by the preparation of an inventory of every computing and storage device in the company, i.e., desktop, laptop, peripheral, mobile computing device, etc., that may contain discoverable electronically stored information, and an inventory of software applications used to create or archive that information.¹⁵ Identifying the general categories of information that are likely to be relevant in a litigation matter, or responsive to a discovery request, will help sharpen the focus of the inventorying process.

12. Schauwecker, *supra* note 2.

13. E-mail from Scott Roseland, to Brian Wm. Higgins, Attorney, Blank Rome, L.L.P., 2006 Wrap-Up on E-Discovery (Jan. 16, 2007) (on file with author).

14. Fed. R. Civ. P. Rule 34(a) (Dec. 1, 2006); *see also* Withers, *supra* note 2, at 173 ("While neither the amendments nor the accompanying Committee Notes explicitly define [electronically stored information], it is understood to mean information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software.").

15. *See supra* note 12.

Because most General Counsel and retained outside counsel will not have the technical qualifications necessary to adequately perform the inventorying function themselves, the need to consult a company's IT/IM professionals early in the discovery process to help identify the location of relevant information among the company's various electronic storage media and information systems becomes clear.¹⁶ In fact, in some jurisdictions, e.g., Delaware and New Jersey, local rules concerning electronically stored information require that parties identify an "e-discovery liaison" that will work with the attorneys during the early stages of identifying where and how electronically stored information is being stored.¹⁷ Since a judge can question that individual during discovery if issues concerning compliance with the rules come up, the selection of the liaison should be made with careful consideration of the person's ability to effectively communicate technical issues in a layman's fashion.¹⁸ Some have suggested that a trend is developing where courts are inclined to actually require that counsel be accompanied by the e-discovery liaison when meeting with opposing counsel and/or the court.¹⁹

Another role for the IT/IM professional during this early stage of discovery is to help counsel understand whether the other parties' disclosure concerning its electronically stored information is adequate, where the opposing parties' relevant documents are likely to be easily found, and how best to begin sorting through the mounds of data formats and storage media that will be produced.²⁰

When it is unclear whether a party is on notice of actual or potential litigation, and because the task of inventorying every electronic data storage device and software application can be daunting, it may make sense to develop the required inventory long before litigation is on the horizon. Conducting a thorough and methodical analysis of one's information technology assets and software over time, without the pressures imposed by the new 2006 rules or the scrutiny of an opponent's lawyers once litigation commences, will probably be cheaper, contain fewer errors, and is generally good practice.

D. What Will Happen With the Inventory Data?

Once the physical location of discoverable electronically stored information has been identified, it must be retrieved and produced on a storage media and in a format that has been agreed to between the parties or ordered by a court. Often, this is the Achilles heel of compliance with the new rules because it can be the most expensive part of compliance, and it is fraught with potential problems, including the inadvertent production of confidential, highly sensitive, and privileged documents and information.

For example, the parties may agree to produce on compact disks or external hard drives all of the electronically stored information in their original application or native format, or in a readily usable format that can be read using conventional word processing, text editing, or image displaying

software, which means that all files and backup files of any kind may need to be retrieved and converted to one of several different possible formats (which is not always as easy as it sounds, as many archiving systems do not simply copy files in their standard application or native format). This means that proprietary software files relating to, for example, stack continuous emissions monitoring data, will need to be processed through some sort of conversion application. That could be an exhausting and expensive task, given the potential amount of data that a manufacturing plant generates.

One aspect of e-discovery that will impact the process of producing relevant electronically stored information is that data is often stored on multiple computers within a company, with multiple copies that can be edited by different people.²¹ And unlike paper versions, electronic data is not always made up of discrete documents or even discrete pieces of information; rather, it will simply be megabytes of data that are constantly changing and being updated from multiple data sources,²² such as in the case of stack emissions monitoring and meteorological data.

The job of screening all that information can be made easier by using computer hardware and software specially designed for this process. Here, attorneys, environmental, health, and safety managers, and others with knowledge of a facility's operations will need to work closely with the company's IT/IM professionals to identify search terms and search concepts to simplify the process of extracting electronically stored information. Of course, in litigation, it makes sense to work with opposing counsel *before* investing time and resources to identify discoverable electronically stored information, because opposing counsel may not be interested in every document or data in a company's possession.²³ But, beware: the process of searching volumes of electronically stored information may become transparent to opposing counsel, and a judge, so the searching process must be carefully thought through. A narrow search may be expeditious and relatively inexpensive, but it can be found by a judge to be inadequate if challenged by an opposing party. There is no shortage of commercial vendors that can provide consulting services to a party who is screening its electronic systems for relevant electronically stored information.

After the electronically stored information has been identified and retrieved, but before it is converted to an agreed-upon format and saved on a pre-determined storage media for production to another party, it must be reviewed to determine what portion of the documents and information is actually relevant to the pending or anticipated litigation issues (or is responsive to a court order). This is a critical step in complying with the new rules, as the sheer volume of information raises the possibility (some would say inevitability) of inadvertently producing not only irrelevant documents (which can actually be a strategy employed by some parties to "bury" an opponent), but also confidential or privileged documents and information. In addition, electronically stored information can often contain hidden or nonapparent information that will be produced with the data. For in-

16. John J. Coughlin, *E-Discovery: Identifying Internal Resources to Facilitate Electronic Discovery*, 14 INTELL. PROP. TODAY 32 (2007).

17. *Id.* at 33.

18. *Id.*

19. *Id.*

20. See *supra* note 12.

21. Jason Krause, *E-Discovery Gets Real: Revisions to the Federal Rules of Civil Procedure Still Leave Many Questions About Discovery of Electronic Evidence*, ABA J., Feb. 2007, at 44-51.

22. *Id.*

23. Withers, *supra* note 2, at 196.

stance, electronic data files may include metadata (embedded records of the creation and management of the document), editorial comments and changes (which may be kept in the native file format for later revision), and functions (such as the mathematical formulas that determine the relationship of cells in a spreadsheet or records in a database).²⁴ Knowing the kinds of hidden or nonapparent information contained in data is crucial before producing electronically stored information.

Once documents and information that should not have been produced are in fact produced, it may be difficult to get them back, even under the “clawback” provisions of the new rules, as a recent case in New Jersey illustrates.²⁵ In that case, a judge reversed a Magistrate Judge’s order forcing the defendants to return over 500 mistakenly disclosed confidential documents. As a result, the confidential, and some privileged, documents may not need to be returned to the originator in that case. And once the cat’s out of the bag, it may be impossible to retrieve it, depending upon the jurisdiction where the parties are located. Moreover, the clawback provision does not alter the rules relating to attorney-client privilege, so even if the party that inadvertently produced privileged documents is able get them back, it will likely have waived the attorney-client privilege.²⁶

E. How Do the Rules Apply to the Hypothetical?

In the toxic tort litigation matter described in the introductory hypothetical, the plaintiffs’ attorneys will certainly want the defendant manufacturing company to produce all electronically stored information that is relevant to the elements of negligence and that concern the computation of damages, including documents and information concerning manufacturing processes, such as logged data associated with any manufacturing processing unit that was involved in the hazardous air pollutant release, all e-mails discussing the release before and after the event, routine safety reports, maintenance reports, stack emissions monitoring data, financial records, etc. Obviously, that is a lot of information, and it should not be a surprise when it is learned that the information is being stored in different formats on different computing systems that may not integrate well with each other.

The defendant’s General Counsel (and any retained outside counsel) and IT/IM personnel must take primary re-

sponsibility to ensure that every employee of the company that possesses relevant documents and information concerning the hazardous air pollutant release take measures to protect those documents and information from destruction or loss until the threatened lawsuit is over or no longer anticipated. It would be advantageous to send out a “litigation hold” e-mail to all employees, then follow up with additional communications over the course of the next few weeks and months if the lawyer for one of the plaintiffs files suit. It would be prudent to immediately speak with those in charge of sensitive and potentially highly relevant electronically stored information, such as those overseeing the collection of electronic manufacturing records and stack emissions data, so that the data at the time leading up to and after the hazardous air pollutant release can be preserved and collected in a forensically appropriate manner so none of the nonapparent or hidden data are modified. Of course, the defendant’s IT/IM personnel responsible for backing up e-mails must be put on alert, too, as e-mails are an important source of discoverable evidence and regularly get deleted in the normal course of business. For example, the normal procedure for rotating e-mail backup tapes should be modified immediately to “freeze” the historical documents that existed at the time of the hazardous air pollutant release.

As in any business decision, the CEO in our hypothetical will certainly understand that there is a risk-reward balance involved in complying with the new electronic discovery rules. Consider, for example, the case of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*,²⁷ in which a jury awarded over \$1.4 billion to a plaintiff after a court sanctioned Morgan Stanley for its practice of destroying electronically stored information, primarily e-mails, by instructing the jury that it could draw an adverse inference against Morgan Stanley due to that and other failures in producing electronically stored information. In addition to overwriting e-mails, the judge found that Morgan Stanley had failed to produce backup tapes, failed to conduct court-ordered searches for documents, and failed to produce responsive documents in a timely manner, even after certifying that it had complied with the court’s electronic discovery order.²⁸ In view of the sanctions imposed against Morgan Stanley in that case, its risk-reward analysis was flawed, as the sanctions imposed as a result of its failure to comply with the then-existing e-discovery rules and the court’s discovery orders far exceeded any burden of searching for, preserving, and then producing documents.

In our hypothetical, the CEO and his litigation team can expect to be rewarded with a high level of compliance with the new e-discovery rules if an adequate amount of resources are invested early and consistently throughout litigation, and as long as the company’s lawyers are forthcoming and adequately disclose information about the company’s electronic systems to opposing parties. On the other hand, skimping on resources and trying to hide the ball can be expected to lead to monetary or other sanctions, as several recent court decisions have demonstrated.

24. *Id.* at 175.

25. *Amersham Biosciences Corp. v. PerkinElmer, Inc.*, 2007 WL 329290 (D.N.J. Jan. 31, 2007 (Unpublished)).

26. *But see* Proposed Rule of Evidence 502, <https://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp> (last visited May 6, 2007) (noting that under the proposed FRE 502, the disclosure of the attorney client or work product protected material does not operate as a waiver in a state or federal proceeding if the disclosure was inadvertent and made in connection with federal litigation or administrative proceedings and if the holder of the privilege took reasonable precautions to prevent disclosure and took reasonably prompt measures once the holder knew or should have known of the disclosure, to rectify the error, following the procedures in Fed. R. Civ. P. 26(b)(5)(B)).

27. 2005 WL 679071 (Fla. Cir. Ct. 2005).

28. *Id.*