

Information Alert

Design and Construction

Spring 2008



AMES & GOUGH

Atlanta ♦ Boston ♦ Philadelphia ♦ St. Louis ♦ Washington, D.C.

E-Discovery Rules and Risks: Understanding the Real-World Rules for the Virtual World of Electronic Documentation

The Federal Rules of Civil Procedure (FRCP) changed dramatically on December 1, 2006, putting more emphasis on e-discovery—production of electronic documentation as part of defending your firm in a lawsuit. For example, all e-mail is now discoverable, there's a 99-day window for a meet-and-confer session among the parties to the lawsuit, and businesses must be prepared to put a litigation hold on all e-mail that might be relevant. According to a recent survey of professionals who have faced the new rules, as many as one in five businesses have settled lawsuits rather than face the cost of electronic discovery. Nearly half of the survey respondents indicated that their legal teams were not up to the task. And the costs of litigation were pegged at an average of \$200,000, with 8 percent of respondents indicating average costs in excess of \$1 million.¹

Electronic documentation is every bit as discoverable as hard copy. For nearly 40 years, e-mail and other electronic documentation have been viewed by courts in the same light as paper documents. But the increased focus on electronic documentation in the December 1, 2006, revisions to the FRCP has raised the stakes. Because anything you write could be held against you in a court of law, it is important to understand proper creation—and prudent handling—of your electronic documents.

In this *Information Alert*, we look at e-risk, including:

1. the legal landscape;
2. the impact of technology upgrades;
3. which firm pays for discovery;
4. electronic document-retention plans;
5. corporate e-mail policies; and
6. preservation of privileged communication.

The Legal Landscape

In 1970, the federal court system changed the definition of discoverable documents—information that you must turn over to opposing counsel—to include electronic documentation. But in 1970, the impact was minimal—in part because the amount of such documentation was fairly limited. Most design work was created by hand on paper or other tangible materials.

Today, computer systems can hold terabytes of information—trillions of bytes. To put that in perspective, one terabyte is probably enough to fill 500 million pages of text. We have moved from paper documents to CADD (computer-aided design and drafting) to BIM (building information

modeling), and BIM is probably not our final destination.

As noted in our introduction, the requirements for electronic documentation were made far more stringent on December 1, 2006, by some changes to the FRCP. The new rules attempt to take into account the subtle and not-so-subtle differences between paper and electronic documentation.

While state courts are not bound by the federal rules, many states use the FRCP as the model for their own rules. Thus, it would behoove most design and construction firms to consider FRCP as a minimum threshold for compliance when a lawsuit may be in the offing and to become familiar

with the particular rules in the states in which they regularly practice.

One significant change to the FRCP is that the courts and the parties to a lawsuit, both defendants and plaintiffs, are required to give early attention to information stored electronically. The parties must meet within 99 days of a civil action to determine what information will be produced and in what format.

But the legal obligations can begin prior to litigation if the parties know—or could reasonably be expected to have known—that a lawsuit would be forthcoming. For example, firms involved in major projects that have been the subject of negative press about cost overruns, such as the Boston Central Artery/Tunnel Project, could anticipate litigation long before it happened. Before the complaint and summons hit the door, firms need to take care not to destroy any documents even if such documents were otherwise scheduled to be purged from the server or the backup tapes were scheduled to be overwritten.

You have a duty to protect any data that might pertain to a claim or a potential claim. For design and construction firms, this includes not only the contract for work, but also the plans and electronic communications exchanged among those who work at your firm and with those who work elsewhere that pertain to every project because you never know which project will result in a claim.

If your firm is involved in a lawsuit, be prepared to retrieve large volumes of information. You must make—and demonstrate—a good faith effort to identify any discoverable electronic data and notify opposing counsel.

Today, billions of electronic documents—from e-mails to CADD files—are created every day. They never go away and can always be retrieved, although sometimes at great cost. But with the aid of powerful computer programs, plaintiff attorneys can find the proverbial needle-in-the-haystack more easily than ever before.

Once you become aware of a claim or the potential for a claim, there are a number of steps you should take, including the following:

- ▲ Obtain legal representation from your professional liability insurer. Request that the services be provided as “free pre-claims assistance” if possible.
- ▲ Gather and inventory your data *before* you receive a request for documents. That way, you will know what you have, and it will be easier to find.
- ▲ Provide the opposing party with a description of the data you have by category and by location of documents.

Once you’re in litigation, you have additional legal duties:

- ▲ You need to preserve all documentation pertaining to the case. DO NOT destroy any documents even if they were otherwise scheduled to be destroyed as part of your firm’s document retention/destruction policy. Failure to preserve all relevant documentation can expose your firm to court sanctions and penalties.
- ▲ Be careful about what you and your information technology (IT) department do with laptops and other devices that were used by employees no longer with the firm. For example, some IT departments routinely recycle laptops when someone leaves, scrubbing all the data and refurbishing the laptop for use by the next employee. But the laptop could have held information relevant to the lawsuit. Rather than just wiping out the files, the IT department should first create a backup so that the files can be retrieved if/when necessary.
- ▲ Don’t overlook all the places your documents could be “hiding.” The following is a brief, not an exhaustive, list of possible locations of electronic documents:
 - ◆ hard drives;
 - ◆ desktops;
 - ◆ laptops;
 - ◆ BlackBerry and similar devices;
 - ◆ data recorders;
 - ◆ audio and video recordings;
 - ◆ employees’ home/personal computers;
 - ◆ floppy disks/jump drives/and so on; and
 - ◆ your server or other backup storage.

As a minimum, be sure to investigate all these possibilities. In addition, you should alert all employees not to destroy any information they may have that pertains to the project or matter subject to litigation.

But don't just hand over all of your records to opposing counsel. First, meet with your own attorney to review the relevance of the information before disclosing it. This will prepare you to identify pertinent information to opposing counsel. And the court may agree, deciding that only certain types of information are material.

The Impact of Technology Upgrades

Another issue is technology upgrades and changes. This document was originally created in Microsoft Word 2007. If we were to send it to someone with an earlier version of Microsoft Word or another word-processing program, that person might not be able to open this file. Sometimes, computer program incompatibilities work in the other direction as well, with the newer program unable to read the earlier documents—particularly if your firm switches not to an upgrade of a currently used program, but to another program altogether, such as changing from Lotus Notes to Microsoft Outlook or vice versa.

When your firm changes its programs or suite of programs, there are at least four approaches to preserving electronic documentation that may not be accessible by a newer system:

- ▲ Your firm can keep the old program on at least one laptop or desktop for the sole purpose of accessing old files.
- ▲ Your firm can print all documents in the old program and store hard copies somewhere.
- ▲ Your firm can create electronic images of the old files and store them on your server.
- ▲ Your firm can have all the old files converted to the new program and continue to store them.

The option your firm selects should be based, at least in part, on how many documents it decides to keep as well as actual and virtual space limitations.

Another option that has become the storage modality of choice for many firms is to store documentation online with a company that

specializes in document storage and retrieval. This is a viable alternative for some firms, but it carries with it the usual commonsense/business-sense caveat that you should choose your storage company wisely. The cheapest deal is not always the best deal. You should choose a company with a strong track record of reliability, one that is likely to be in business when you need to retrieve your documents. The courts are not likely to look kindly on “Our storage company went belly up, so we can't find the documents” as a legitimate reason for not producing those documents.

The important thing is to *do something* proactively to preserve the documents—to pick an option, not just to let the documents be lost to your reasonable use by default.

On the upside, new laws and regulations often precipitate new technologies. There are a number of more powerful technologies available that can help you search your electronic archives more effectively, facilitating your searches for all the documents related to a particular project.

Which Firm Pays for Discovery?

The court may require opposing counsel to pay part or even all of the cost of your search if the court decides that the expense of obtaining the information outweighs the benefits of having it. Federal courts generally use a seven-factor test to determine which firm pays for the cost of discovery:

1. Is the request tailored to discover relevant information?
2. What is the availability of the information from other sources?
3. Does the total cost of production make sense when you weigh it against the amount in contention?
4. How does the total cost of production compare to the resources of each party?
5. What is the ability of each party to control the cost of discovery, and what incentive does each party have to do so?
6. What is the importance of the issues at stake?
7. What are the relative benefits of the two parties for obtaining the information?

The answers to these seven questions help the court to determine the appropriate allocation of costs, which can run into the millions of dollars.

Electronic Document-Retention Plans

The legal requirements in discovery all point to the need for a formal document-retention plan. Courts do not favor defendants that do not have a plan and destroy documents in an inconsistent manner. And the courts have been known to impose sanctions on those without a policy—or with a policy that is not followed. Sanctions have even been applied for the unintentional failure to preserve electronic information. Even worse, juries have been instructed to infer spoliation—the intentional destruction of information—based on the inability of a party to produce requested documents.

If you do not have a document-retention plan, developing such a plan should be a high priority. If you do have one, you should make sure it considers the following issues:

- ▲ Have one overall policy, and enforce it in order to maintain consistency. There should be one plan that addresses storage and destruction for both hard copy and electronic information.
- ▲ Know what is being stored, including where and how long it needs to be stored to comply with statutes and court rulings.
- ▲ Be sure that your IT department is included in the creation of your plan. The IT department should also know when certain electronic information should be destroyed.
- ▲ The firm's executives will likely be held accountable for document retention and destruction. The firm should designate one principal or executive who will serve as "Keeper of Records." That person will be responsible for testifying about the firm's document-retention/destruction policy, so be certain he/she is fully informed.
- ▲ Be certain that everyone in the firm understands that e-mail is subject to discovery. No one in the firm should have any expectations of privacy.
- ▲ Be sure that employees understand how to manage their e-mail—what should be kept and what should be cleaned out on a regular basis. Also, be sure they know not to delete any

relevant information in their possession once the company is informed of a lawsuit, claim, or potential claim.

- ▲ The plan should include a schedule for document destruction. Be sure that everyone purges unnecessary records and correspondence in accordance with the schedule.
- ▲ Consider segregating personal from professional e-mail and having different policies for each.
- ▲ Suspend regular retention and destruction policies when the firm faces litigation or a legal document request—or the likelihood of same. And of course, be sure to notify everyone in the firm as quickly as possible of the suspension.
- ▲ Specifically notify IT when there is pending litigation, and get IT involved in the process of retrieving documents.
- ▲ Do not just trust that employees will follow the plan—particularly when it comes to document destruction. Some of us have hard drives cluttered with aging documents we never get around to discarding; others purge information much too quickly. Audit the server and employees' hard drives periodically to be certain the plan is being followed.
- ▲ Last on this list, but first in importance, is management commitment. Management buy-in is critical to the success of your document-retention plan.

As with the rules of evidence, the length of time documents—both electronic and hard copy—should be retained varies from state to state. Every state has a statute of repose that defines the time period during which, for example, a design or construction firm can be sued for a defective design that results in the damage to or the failure of a structure. More importantly, the statute defines the time *after* which said design or construction firm *cannot* be sued for the damage or failure.

One common length of time for statutes of repose in a number of states is 10 years, but this time period is not a universal constant.

- ▲ For design and construction firms operating in only one state, the document-retention policy should reflect the statute of repose plus some nominal time period to allow for documents

that have been sent, but not received. To be ultra-safe, that nominal time period should be at least one year. So in a state with a 10-year statute of repose, your firm would keep documents for 11 years.

- ▲ For design and construction firms operating in more than one state, there are two possible approaches:
 - ◆ You can determine the statute of repose for each state in which you operate and establish a separate document-retention policy for each state equal to the statute of repose plus one year. The upside of this is that you are keeping only the minimum number of documents necessary; the downside, that multiple periods for document retention could be confusing to your firm's staff and IT department.
 - ◆ You can determine the longest statute of repose for any state in which you operate and establish a document-retention policy for that length of time plus one year for all states. The pros and cons here are the mirror image of those for having multiple periods. The simplicity of keeping everything for the same length of time may be counterbalanced by excessive document storage requirements. Even a terabyte gets used up eventually—and faster than you would anticipate.

Corporate E-Mail Policies

E-mail transmissions are not private, according to judicial decisions. The courts have ruled that e-mail is inherently public, so e-mail users have no reasonable expectation of privacy. The only exception to this is specific privileged communications between an attorney and his/her client. Even then, the courts may challenge the attorney to demonstrate that the communication is privileged.

Your firm should consider including an e-mail policy in the employee handbook. The following are some of the issues that should be covered in your firm's policy:

- ▲ E-mail transmissions are not private. There should be no expectation of privacy.
- ▲ The firm reserves the right to read any or all e-mail transmissions at its sole discretion.

- ▲ E-mail should be used primarily for the firm's business. E-mail may also be used to contact family members and personal friends; however, this usage should be minimal.

(A policy that restricts e-mail use strictly to the firm's business could be difficult to enforce and is probably an unrealistic goal. Allowing a small amount of personal e-mail is more realistic. On the other hand, defining "minimal" could also be difficult. This is a judgment call that each firm must make, and the policy must be applied fairly to all employees.)

- ▲ Unauthorized use of the firm's e-mail system may be grounds for discipline, up to and including termination of employment.

In addition, there should be rules or at least guidelines for authorized e-mail. These may vary, depending on your firm's "style"—formal or informal—and that of its clients and suppliers.

The rules for effective e-mail communication are particularly important when the e-mail pertains to the firm's projects. The following are some suggestions for project-related e-mail:

- ▲ E-mail should convey concise information with the appropriate background so that the meaning of the message is not misconstrued.
- ▲ All project-related e-mail should be preserved in the project work file in hard copy—this, in addition to being filed electronically in a virtual project work file on the server.
- ▲ Adhere to the general rules of file documentation, including the following:
 - ◆ Do not speculate.
 - ◆ Do not offer opinions as facts.
 - ◆ Do not express feelings about the project itself or about anyone involved in the project.
 - ◆ Provide concise, consistent, and factual statements only.
 - ◆ Address only one project in any given e-mail. Addressing issues for both Project A and Project B in the same e-mail will pose problems regarding where to store the particular e-mail.

- ◆ *Never* hit the send button right away—particularly if you’re not happy with the request to which you are responding or the person to whom (or about whom) you are writing. It’s all too easy to let a little “attitude” creep into your words. Reread the e-mail to be certain your meaning is clear. A good rule of thumb before hitting that send button is to ask yourself if you would want to see the contents of the e-mail on the front page of a newspaper—or perhaps worse, in front of a jury.

Once your communication leaves your hard drive, it’s floating out there in cyberspace forever. This is true of your e-mail and of any documents attached to your e-mail.

Preserving Privileged Communication

The one type of e-mail that may be exempt from disclosure is attorney-client communication. For communications to be effective, the attorney’s client must be able to expect confidentiality. Substantive e-mails to and from the firm’s attorney—and to and from in-house counsel—are, thus, not discoverable. All such communications should be clearly marked with the words “Privileged and Confidential: Attorney-Client Communication” or with some similar phrase.

The law, however, is always a moving target. Before sending privileged information via e-mail, have a conversation with the attorney to get his/her opinion about privilege.

Do not forward communications to or from your firm’s attorney to other parties. This may negate any privilege that would otherwise be in effect.

This issue of *Information Alert* was prepared by the following Ames & Gough professionals: Mike Herlihy, ARM, and Gregg Bundschuh, JD. Editor: Meike Olin, PCPU, CIC, CRM.

i “Survey Shows One in Five Businesses Have Settled a Lawsuit to Avoid the Cost of Recovering and Searching Through Email,” November 27, 2007, Fortiva, Inc., <http://technology.findlaw.com/articles/01179/011040.html>.

For additional information, please call the Ames & Gough office nearest you:

ATLANTA
Phone: (770) 552-4225

BOSTON
Phone: (617) 328-6555

PHILADELPHIA
Phone: (610) 547-0663

ST. LOUIS
Phone: (314) 835-0026

WASHINGTON, D.C.
Phone: (703) 827-2277

© Ames & Gough 2008. All rights reserved. The information contained herein should not be relied upon as legal or insurance advice for specific facts and circumstances and is not intended to be a substitute for consultation with legal or insurance counsel.

Communications should be *strictly* between you and the attorney.

In Summary

The rules for electronic documentation are essentially the same as for hard copy, but the December 1, 2006, revisions to the FRCP have put more emphasis on the virtual world and e-discovery. Remember the basics:

1. Know the legal landscape. Understand your firm’s legal obligations for preserving and providing electronic documentation.
2. Plan proactively for the impact of changing technology on the accessibility of your electronic documentation.
3. Understand that you may not have to pay for discovery. The court may put that burden on the party suing you in certain circumstances.
4. Have a formal document-retention plan, and enforce it.
5. Keep e-mails factual and concise, but also be sure to provide the appropriate background and context so that information will not be misconstrued.
6. Follow procedures to preserve confidentiality of privileged communications.

Sample Document Policy

If you would like a copy of the sample document-retention policy developed by Donovan Hatem LLP, please send an e-mail requesting a copy to news@amesgough.com. Please put “Sample Document-Retention Plan” in the subject line of your e-mail.