ASA's
THE CONTRACTOR'S Compass
THE OFFICIAL EDUCATIONAL JOURNAL OF THE AMERICAN SUBCONTRACTORS ASSOCIATION
WWW.ASAONLINE.COM MARCH 2015

Negotiation Strategies

Beware of Inadvertent Disclosure of Electronic Information

by James Yand

Information is the lifeblood of any business. It documents the work performed and often serves as the center point of a dispute, especially when a lawsuit is filed. Our litigation system is designed to allow each side to find and use relevant nonprivileged information in proving its case or defense. Therefore, the modern business owner must be able to navigate the information repositories, regardless of their form, including the ability to ask for and produce electronically stored information (ESI).

In addition, the business owner and its legal counsel must be able to comply with the duty to preserve information once a lawsuit is reasonably anticipated, including the obligation to identify, locate, and maintain ESI held by the business. The failure to do so may result in serious sanctions and referral to disciplinary counsel.

New terminology helps define whether you are familiar with, and prepared to handle, the challenges of the digital world. For example, do you know what a "litigation hold" is, and how to use it? If asked by a judge, would you be familiar with your company's computer systems, and what your record-retention policy states? Could you craft a discovery request asking for production of electronic records in a form that is readily searchable and adaptable to your litigation database?

Pitfalls of E-Discovery Requests

More than 95 percent of all information is now generated in electronic form. Yet, the discovery rules that exist in many state courts are designed to deal with the world in which typewriters and copiers were the primary means of generating and duplicating documents.

Electronic records offer a very different reality and require knowledge of a medium that is different in nature and quantity. For example, Microsoft receives from 250 million to 300 million email messages per month from outside the company. It generates another 60 million to 90 million internal emails a month. Its firewalls delete 85 to 90 percent of all incoming emails.

This task of controlling electronic information can cost millions of dollars and dwarf the dispute underlying the lawsuit itself. This has serious implications for our justice system that are contrary to the notion of cases' being resolved on their merits in a just and efficient manner. See Fed. R. Civ. P. 1.

ESI Is a Dynamic Medium

Paper is one-dimensional. It can be stored in a file and then copied when needed. Electronic information is alive. It changes as its environment changes. It contains metadata that describes the "DNA" of the record: how it was created, when, and by whom; and how it was changed, when, and by whom. Thus, when electronic information is disconnected from its lifeblood and rendered one-dimensional by being sent to the printer, it loses its very essence. This is why digital information is best collected, reviewed, analyzed, and offered into evidence in its electronic form. Without its DNA, the electronic information lacks authenticity, and may be easily manipulated or faked. This fact fundamentally drove the changes in the federal rules to recognize that the world of documentation now exists in electronic form in addition to paper.

Electronic discovery refers to any process in which electronic data is sought, located, preserved, and collected with the intent of using it as evidence in a civil or criminal legal case. The key is to know what you have and where it is stored and backed up.

Metadata and Unauthorized Disclosures

In addition to final product data stored in the locations mentioned above, metadata is embedded within each document. The simplest definition of "metadata" is that it is data about data, similar to how DNA is the building blocks for one's body. This metadata includes information beyond its printable content, such as previous revisions (think "Track Changes" even if you do not see it), hidden text, comments, document properties, user email addresses, server names, and routers. Be aware that even a document that you copy for reuse (e.g., "Save As") brings with it all previous metadata.

In everyday work product, do you want to provide recipients with a document's hidden changes and modifications? A solution to this critical problem is to implement an outgoing email policy at your business — the sender must always scan (or at least create a PDF of) or "scrub" any electronically transmitted file. Creating a read-only PDF or scanned file breaks the metadata chain, since only an image is created. If you create a PDF file from your desktop computer rather than a scanned image, however, metadata will still exist. Using these measures to protect your electronic records and files reduces risk of embarrassment.

The best way to avoid this risk is to establish a comprehensive policy of rules to scrub metadata from all outgoing documents before they leave the company. A successful security software application will not ask the end user to remember to do something, but will automatically scrub documents before sending. Even with the best of intentions, employees will still forget to manually scrub metadata on each document.

What Is the E-Discovery Problem?

The ediscovery problem is essentially a result of the sheer volume of business conducted electronically. Go back even 10 years — how much of your firm's business was done via mailed letters and other documents? Do you remember waiting for a signed document to be mailed or couriered back before proceeding? Now think about how much work is accomplished based on emails, scanned documents, file-sharing, or AutoCAD. Computer forensics is booming for those companies tasked with analyzing a firm's electronic records, everywhere they reside. And even unsolicited, deleted emails are recoverable and discoverable.

What Are Effective E-Discovery Solutions?

What kinds of ediscovery solutions are most effective? First steps involve defining record-retention policies, determining what processes and technologies will be used, training staff on those processes and programs, and then implementing them. The following are some common methods or work practices:

- Doing regular backups, preferably automatically, so that reliance on human effort is not necessary. Backups can be disk-based/online, or on tapes.
- Using programs that start each document clean of prior metadata, but allow the same template to be used again.
- Centralizing data storage so that multiple copies are not in multiple locations.
- Managing your documentation to enable data hierarchy, versioning, and classification. There are programs to help manage tags and metadata, but they are not the whole solution.
- Saving only what is truly needed for project records. Avoid the "let's keep everything because we may need it someday" philosophy. It may come back to bite you.
- Using email archiving programs or services. Establish an email retention policy with limits on what kind of email is to be sent and received in the workplace. Unwanted email should be blocked or deleted immediately. Do not allow personal email to mix with business email.
- Consistently using the email subject line to identify the topic or email attachment. Send a follow-up email to the recipient to verify that he or she received what was needed. Also, do the same for email attachments you receive. It is hard to make or defend a case with holes in communication.
- Requesting each party that you subcontract with to abide by the same rules and policies that your firm follows.
- Eliminating potentially embarrassing or incriminating metadata before sending documents electronically. Metadata scrubbers are available from a number of sources.
- At the genesis of a project, establishing with clients, consultants, contractors, etc., the ground rules for dealing with electronic information.
- Considering increasing insurance coverage for potential retrieval of network/electronic document-type scenarios, and taking a hard look at your insurance limits to ensure that they cover your potential risks.
- Establishing a written document-retention policy, and being prepared to issue a litigation hold on all paper and electronic files once a lawsuit is filed or reasonably anticipated.

A company is only as strong as its weakest link, and with this area of risk, the damage from being hacked or inadvertently disclosing electronic data can be fatal to the company and its business reputation. To mitigate this risk, create a comprehensive document-retention policy and follow it! In a legal proceeding, this may be your ticket to avoiding sanctions and resting assured that the company is protected from these risks.

James Yand is a partner with Miller Nash Graham & Dunn, LLP, Seattle, Wash. He has more than 20 years of experience resolving disputes for business owners and individuals in construction law, products liability, e-discovery, franchise and commercial law. He can be reached at (206) 622-8484 or james.yand@millernash.com.