When Lawyers Attack! - Dealing With the New Rules of Electronic Discovery

John E. Benson, Esq.

A Companion to the Presentation
Given at Shmoocon IV

February 17, 2008

Author's Note

My thanks are extended to everyone who had the opportunity to attend my talk bright and early on Sunday morning. I hope that I was able to alleviate some of the confusion that has been created over the past 24 months which have seen the 2006 amendments to the Federal Rules of Civil Procedure come into effect.

I chose to create this handout instead of posting my slides because they hold little value on their own. I am of the firm belief that presentations are conversations with the audience and that slides should enhance the experience, not be a substitute for it. I hope that this material will serve as a worthwhile supplement to our conversation.

This is not intended to be an academic paper nor definitive text on electronic discovery in any way (as you can see by the lack of references) and certainly shouldn't be relied upon for any kind of legal advice. This is merely a collection of the major points which I believe everyone should understand after participating in my presentation.

If you have any questions about the material or the subject in general, please feel free to contact me at john@john-benson.com.

What Is Electronic Discovery?

To fully understand what electronic discovery (e-discovery) is, one must understand the nature of the legal profession and the litigation process. During litigation, both sides exchange information about the case. This can be in the form of depositions (verbal examination under oath), interrogatories (written questions) and document exchange. The rules governing this process come from the Federal Rules of Civil Procedure in the case of litigation in Federal court or your state rules of civil procedure for state cases.

Prior to December of 2006 there were no provisions that specifically addressed how electronic documents should be handled during the discovery process. This is not to say that electronic data was never used during litigation. Electronic data was addressed for the first time in the early 1980s. There were, however, no real rules for the form that a production should take (paper v. electronic, tiff v. native format, etc.) and productions largely depended on the relative savvy of each attorney involved.

The legal profession is relatively technology averse. Many attorneys, especially ones who handle large corporate litigation, don't understand technology and its implications. Quite simply, they previously missed many opportunities to find information found about the data itself because their thinking is largely focused on the paper format.

The legal system itself develops in a slow and methodical manner by design. The common law system develops incrementally and law is interpreted only on facts which have been brought to the courts. While this may seem like an illogical way to handle things, especially in light of how fast technology advances, it creates a system where law is consistent, stable and predictable based on prior case law.

This can lead to a great deal of confusion when new laws and factual situations come into effect because law is never really set until the facts are litigated and make their way through the appellate process. A great example of this is the issue of whether or not an individual can be compelled to produce to law enforcement encryption keys or passwords in a criminal case against them. I remember this topic coming up in the desert heat during Jennifer Granick's talk at DEFCON 13. Until recently (in the United States at least) this issue had not been addressed by the courts, meaning that the discussion was left to debate during cocktail parties and internet discussions.

In general, the standard answer you will receive from an attorney on just about any question is, "It depends." Within areas of emerging law, especially those surrounding technology, the answer is, "We don't know yet."

This confusion is compounded by how cases become well settled and applicable throughout the country. A case with the highest precidential value and binding effect is one which has been decided by the US Supreme Court. At the other end of the spectrum

is a decision by an individual judge at the District Court level. Many of the decisions regarding issues of technology and e-discovery occur at this lower level. This means that your milage from any decision regarding e-discovery will vary greatly.

What Do the Electronic Discovery Amendments Change and Require?

It is important to realize that the Federal Rules apply to the litigation process and place no explicit requirements on organizations to change their practices. The Rules now require that attorneys from both sides meet and discuss issues relating to electronic productions within 99 days of the start of litigation at what is known as the 26(f) conference. This (in theory) should encourage litigants to look for relevant documents in digital form, which can reveal a great deal more about a set of facts than the printed page can.

The specifics of discovery are negotiated between the parties which leads to different types of productions for different cases. In some cases, discovery remains entirely paper based. In others native files will be exchanged. The form of production that should occur depends on what the underlying issue is and whether native files will reveal important information.

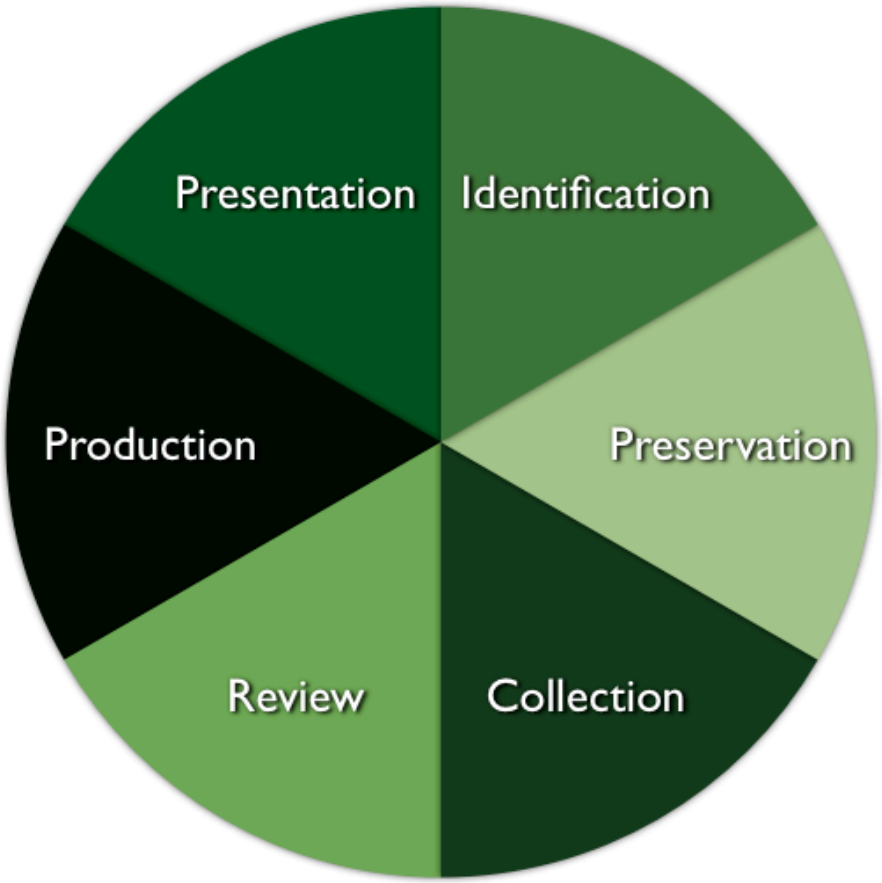
Considering the wide range of technology knowledge within the legal community, it would be advantageous for those who are savvy and involved in the litigation process to confer with their attorneys to help them understand what they should request.

Unlike Sarbanes-Oxley which placed many new requirements directly on organizations with a deadline for compliance, the electronic discovery amendments only affect them through the litigation process. Many companies faced with tight budgets aren't taking many steps to prepare in advance for litigation. This is clearly, their right to do so. It is, however, foolish and can lead to astronomical costs of litigation when it finally does occur.

Penalties for failing to comply with a duty to preserve data range from monetary sanctions all the way to an "adverse inference" instruction. In this situation, a jury is instructed that they can assume that any files and communications not produced were harmful to the defendant. Such an instruction all but guarantees defeat for a defendant.

Increasingly, judges are also holding attorneys themselves responsible for the negligent acts of their clients in preparing for discovery. Recently a number of California attorneys were reported to the state bar association for discipline after it was discovered that their client had withheld electronic evidence from the court. These sanctions are forcing attorneys to take e-discovery much more seriously, but they may still lack a fundamental understanding of technology leading them to focus conversations on a certain number of terms and topics which have been discussed at continuing legal education seminars. When working with attorneys, always do your best to educate them about technology as much as they educate you about the legal process.

How Does the Electronic Discovery Process Work?



- Identification: The stage at which an organization finds all potential sources of responsive data. This can be anywhere from archival backups to employee home computers.
- Preservation: When litigation is reasonably anticipated, either through service of a complaint or consultation with an attorney to consider litigation, an organization has an affirmative duty to preserve any and all responsive data.
- Collection: Data can be collected through a variety of means ranging from manual active data collection by employees to the use of a forensic expert to make whole disc images of machines.
- Review: Attorneys (or in some cases paralegals) will sift through the collected data to determine whether the documents are responsive (a much broader term than relevance) to the lawsuit. They will also review for potential privilege, build logs of data which is retained under privilege, redact irrelevant information, employee personal information and any other data to be kept secret under the law (such as HIPAA).
- Production: The actual exchange of responsive information between parties.
- Presentation: Use of electronic evidence at a tribunal such as an arbitration, mediation or trial.

Why Does Electronic Discovery Cost So Much?

Electronic discovery is extremely costly due to the amount of hours that it takes to sift through the data retained by organizations. As storage has become inexpensive, companies have chosen to retain more and employees have become more likely to spread information throughout the organization instead of keeping it in one place.

The review process can be tedious and repetitive. While there are methods of identifying duplicate documents (using MD5 or SHA1 hashing), many near duplicates remain. Current technology lacks the ability to redact passages across nearly duplicate documents, resulting in many hours of attorneys redacting the same passages from long email threads.

Processing costs from e-discovery vendors can also be very expensive. Restoring data from backups, imaging files, metadata extraction and OCR is very processor intensive which forces many projects to be handled outside law firms, placing data in the hands of a third party.

What Can Organizations Do To Keep Costs Down?

If there is much good news in the world of electronic discovery for security and information technology professionals it is that e-discovery may serve as a major driver to change corporate policy decisions. The parallels between law and security are clear:

- Unless data can be identified and located it can neither be secured nor examined for relevance.
- The lower the volume of information an organization holds, the easier it is to secure and review for responsiveness.
- By centralizing data storage, costs of storage and potential costs of litigation response can be decreased.

Much of the early stages of the electronic discovery process can be completed before litigation is contemplated. An organization would be well served to fully document all policies and procedures relating to data handling and backup, infrastructure diagrams and supported applications. In addition, working with inside and outside counsel to formulate a litigation response strategy and incorporating it with all business continuity plans can help streamline the early stages of litigation.

Besides working to develop policies and information architecture maps, user education can alleviate much of the repetitive nature of the review process. Topics to consider addressing with employees could include:

- How to properly respond to and forward e-mail: There is no need for email threads to extend what is necessary to understand a response.

- How to avoid death by CC: Does the entire sales team really need to receive an attached copy of daily cumulative sales reports?
- Knowing what data you don't need on your machine: Customer databases should reside in a central location and never give multiple copies to individuals unless there is an absolute need.
- How to use the delete key: I think this speaks for itself.
- How to use the telephone: Many conversations should not be carried out over email, which will be retained and potentially become part of a court record.

Security Risks Posed By Electronic Discovery

Financial risk is not the only one which is growing as a result of the use of electronic discovery. By it's very nature, discovery means giving your data to another party whom you do not control. The discovery process can mean large volumes of data leaving your control and falling into the hands of:

- Your e-discovery processing vendor
- Your law firm
- The opponent's law firm
- The opponent's processing vendor

More e-discovery vendors are popping up every week, and many of them don't take security as seriously as they should. These organizations are a large target for attackers because they hold the data for not merely one, but often multiple organizations. As your organization chooses a vendor to help you through the process, demand from them more than a cursory comment about granular user access controls and 128 bit SSL connections.

As you work with inside and outside counsel, all parties will benefit greatly from the perspective offered by security specialists. Attorneys have a difficult enough time understanding technology in the larger sense, let alone the intricacies involved in hardening data security. Help them understand that things like third party security audits and increased expectations of vendors decreases the risk of an information breach and helps them better to comply with their ethical obligations of confidentiality.

Conclusion

I often find it difficult to explain to people what I do. Most individuals, understandably, would have expected that the legal system would have been aggressively pursuing the rich opportunities for finding relevant information within computer systems years ago. That is, unfortunately, not the case.

Electronic discovery is currently creating a great deal of frustration for clients and attorneys because of the complexity and costs involved. I believe that these are simply growing pains that the law is going through as we adjust to the new environment. Anyone who has even a cursory knowledge of the US legal system knows that a plaintiff suing a large corporation is at a distinct disadvantage due to the costs involved in sifting through huge volumes of information. Thankfully the days of a major corporate firm arriving at a small firm with trailers full of documents and microfiche are now behind us.

When I was in Washington for the conference I made it a point to visit our seat of justice, the US Supreme Court. The front of the courthouse reads “Equal Justice Under the Law.” I believe that electronic discovery will level the playing field for litigants in much the same way that the internet has for individual expression.

It was a pleasure speaking at this year’s Shmoocon, and I look forward to seeing you all soon.

Res Ipsa Loquitur,

jur1st

Recommended Resources

http://www.law.cornell.edu/rules/frcp/ - The Federal Rules of Civil Procedure

http://www.edrm.net - The Electronic Data Reference Model has a wealth of information about the e-discovery process, including a tightly regulated wiki containing the current leading thoughts on the process.

http://www.thesedonaconference.org/publications_html - The Sedona Conference is an organization which has led the way in developing principles for attorneys and organizations to follow when using electronic data within litigation. The Conference predates the 2006 amendments and they were extremely influential on the Advisory Committee.

http://www.ediscoverylaw.com/ - The law firm of K&L Gates (yes...that Gates) does an amazing job of compiling information on current electronic discovery laws. Here you will find a free (as in beer) database of over 900 cases as well as links to state rules of electronic discovery.

http://del.icio.us/jur1st/ediscovery - I spend about an hour per day reading up on new developments in electronic discovery. I do my best to mark good materials for my own, and now for your, reference.

About The Author and Presenter

John Benson currently works as an electronic discovery consultant for the Kansas City law firm Stinson Morrison Hecker LLP. A graduate of the University of Missouri from both Columbia and Kansas City campuses, he is a member of the Missouri Bar Association and serves as the chairman of the Kansas City Metropolitan Bar Association Computer Law and Technology Committee. He has taught law, ethics and (oddly enough) finance as an adjunct professor at The Colorado Technical University. He has presented at hacker cons around the country including LayerOne, Pumpcon, Shmoocon and DEFCON. He can be found on the DEFCON boards and assisting with radio communications at DEFCON. His website can be found at http://www.john-benson.com.

Colophon

Brainstorming and drafting of the presentation was done by hand in a Moleskinne notebook. Computers were never meant to be an outlet of creativity when it comes to the written and spoken word.

The slides were created using Keynote 08 on various pieces of Apple hardware using photos from iStockphoto and Google in locations ranging from my fortified compound in Waldo to Midway Airport, the Wardman Park and that sweet spot in the hallway where an open AP could be found at the Washington Marriott. The font used in the presentation and this accompaniment is Helvetica Neue.

Acknowledgements

Bruce, Heidi and the rest of Shmoo for putting on such a great conference
The whole ShmooshiCon crowd for a great dinner with no bill disputes
Noid for the intel and breakfast recommendation
EricM and Nick Farr for playing tour guide
Deviant Ollam for missing another con to run the Villiage (and of course the Got Wiffy shirt)
Jeff for not pulling a blade this time
Jackalope for the new tunes
GM1 and Freshman for all the logistical support
Mouse for all the kind words and research in support of democracy
The guy who recognized a Shmooball baiting comment and responding accordingly
Everyone at Stinson for being open minded enough to support me in presenting at a hacker con with such a funny name
Everyone who woke up early and shook off the booze to come to such an early talk
My beautiful fiancee for letting me get away with leaving her alone on Valentines Day two weeks after we got engaged