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

John E. Benson, Esq.

A Companion to the Presentations
Given at Blackhat USA 2008 and DEFCON 15

August 2008

Author's Note

I hope that my talks and these materials help alleviate some of the confusion that has been created by the advent of electronic discovery.

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 the 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, please feel free to contact me at john@john-benson.com.

The Current Environment of Law and Technology

Of all the talks which I've either participated in or observed which involve the crossroads of law and technology, one common theme stands out amongst all others: frustration at the lack of guidance relating to the law of technology. Whether it be the standard for information which is not deemed to be reasonably accessible under the rules of civil procedure or the applicability of the fourth and fifth amendments to the use of encryption, the answer is consistently that we don't know. This response can come as a real surprise, especially considering the consistent pattern amongst attorneys of having an answer for just about everything.

The reasons for this ambiguity will become clear as we examine the nature of the common law system, as will the conclusion that these ambiguities have little chance of being cleared up any time soon. Progress, especially the technological kind, waits for no man and therefore anyone doing business in the United States or conducting information security research need to keep in mind a few rules.

- The law always favors reasonable action
- Courts frown upon those who act to subvert or circumvent the spirit of the law
- Unless a person has the means and determination to truly challenge the law, always take the legal high ground

Why Don't We Know?

The legal systems of the United States, Canada, the United Kingdom and many of the former British colonies have what is referred to as a common law system. Common law is developed through many incremental judicial decisions on questions which are brought before the court. It is uncommon to have one decision which will have sweeping effect upon many different factual situations, in fact in many instances decisions can be so narrow in their wording that they have little future applicability.

When a case is brought before a common law court which raises a question of law[1], previous cases are cited by litigants to persuade the court to apply a previous decision to the case at hand. In order for a court to make a ruling, there must be a true question of

---

[1] It is important to contrast questions of law to questions of fact. A simple way to understand the difference between the two is to know that juries decide issues of fact and judges decide issues of law. During a trial, juries will be asked whether they find certain critical facts (elements) to be true or false. Based upon the factual findings of the jury, the law can then be applied to determine guilt in the criminal arena or liability in the civil arena. Another perspective which can be taken is often seen during popular courtroom dramas. When an attorney makes an objection to a question posed by opposing counsel the trial judge, not the jury, interprets the law based on the circumstances and either allows the question (overruling the objection) or requests that the question be withdrawn or rephrased (sustaining the objection).

law. Unless a case reaches an appropriate level of the judicial system to be answered by the court it is difficult to know what the law on a particular subject actually is. A case with the highest presidential 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 and technology will vary greatly.

Two subjects give us an excellent perspective on the principals of common law.

The law of private property is relatively well settled and predictable due to the large number of property cases which have made their way through the legal system through the ages. It is not uncommon for a property dispute to be interpreted using cases which were handed down well over a century ago. This is not to say that new situations occur which require new rulings. The issue of true ownership of the baseball hit by Barry Bonds to eclipse the home run record held by Mark McGwire in 2001 was cited a great body of case law from as early as 1805 and the final resolution was based upon a concept utilized in a case decided in 1896.[2]

A stark contrast to the well settled rules of property law is that of Second Amendment law. Until June 26, 2008 it was unclear whether the Second Amendment to the Constitution actually confers upon the people an individual right to possess firearms.[3] There have been very few cases which directly involved this question of law, therefore it remained unsettled for hundreds of years.

While this system creates uncertainty before a ruling on an issue of law, it creates firm rules which can confidently be applied to future situations. Cases in the common law system create precedent and are binding on future courts and cases through starie decisis. The principal is that once a case has been decided, future courts must follow the reasoning of previous decisions. This gives individuals a framework around which they can approach a given situation. The concept that once settled, a decision cannot be truly overturned

---

[2] Property law is far from exciting, but if you are interested in how cases are meshed together to create new interpretations, an excellent case is Lawrence v. Texas, 539 U.S. 558 (2003), which extended the right to privacy to homosexual activities within the home, opening the door to the hotly debated issue of gay marriage.

[3] This is also an excellent example of how maddening the law can be to those not fully aware of its nuances. The Second Amendment is rather clear upon its face, however once lawyers and the courts become involved it suddenly takes more than 50 pages to explain an interpretation of 27 words.

outside of extreme circumstances is missed by many individuals.[4] Thusly, once a rule is promulgated, individuals may rely upon the case's holding to guide their actions in perpetuity. One of the only instances where such a sweeping change to the law was made was the end of segregation in the case of *Brown v. Board of Education*.

If you think this seems like a bizzare way of creating law, consider the situation where previous rulings could be perpetually vacated. In this instance, cases which were handed down based on this theoretical previous ruling would also have questionable effect and destroy all predictability and future applicability of any rule under the common law system.

Cultural Hurdles

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 are missing many opportunities to find information about the data itself because their thinking is largely focused on the paper format. Even with the rule changes and increasing pressure to take technology seriously by some courts, many attorneys refuse to acknowledge that the world is different than it was as few as 10 years ago. As you read this, there are many cases which are proceeding where all exchange of information is conducted with paper and there are attorneys who will claim with all their strength that their area of law does not involve technology.

The problem of a technological averse attorney is a difficult one to deal with for a number of reasons. Many of these attorneys have been practicing law for decades and are heralded as experts in their field. Their grasp on the underlying issues of a legal issue has not diminished in the least as a result of the emergence of e-discovery, but they fail to understand the breadth of information which exists both as a liability to their client as well as a potential asset in defeating claims. Attorneys who began their legal education during the 1980s and 1990s did so with full awareness of the booming business of technology and chose to take a different path. The law was (and still is from an academic perspective) a safe haven from such subjects as high level math and computer programming languages. Many of these individuals were perfectly happy not knowing more about a computer than how to turn it on and off. Now they find themselves being forced to learn a new set of vocabulary and make arguments in court about systems which they may never fully understand.

I have found that despite being an easy scapegoat, age has little difference when it comes to technology understanding. Over the past few months I have met attorneys who started

---

[4] This misunderstanding is consistently perpetuated by the discussion of the issue of abortion. Every time that a commentator brings up the idea that Roe v. Wade will somehow be miraculously overturned with a change in the composition of the US Supreme Court is absurd. It is true that that decision may be interpreted and refined with future factual situations but the original decision will remain. (note: The specific issue of abortion is brought up for illustrative purposes only.)

practicing before the Vietnam War who are more comfortable with a computer than many members of my own law school class. Moreover there are are few judges whose knowledge of how computers function on a low level eclipses that of attorneys who argue before them.

What Is Electronic Discovery?

To fully understand what electronic discovery (e-discovery) is, one must understand 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.

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 normal business practices outside of a litigation setting. Instead, the Rules govern how litigation is conducted and frames the topics of discussion which should be occurring throughout the process. 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.

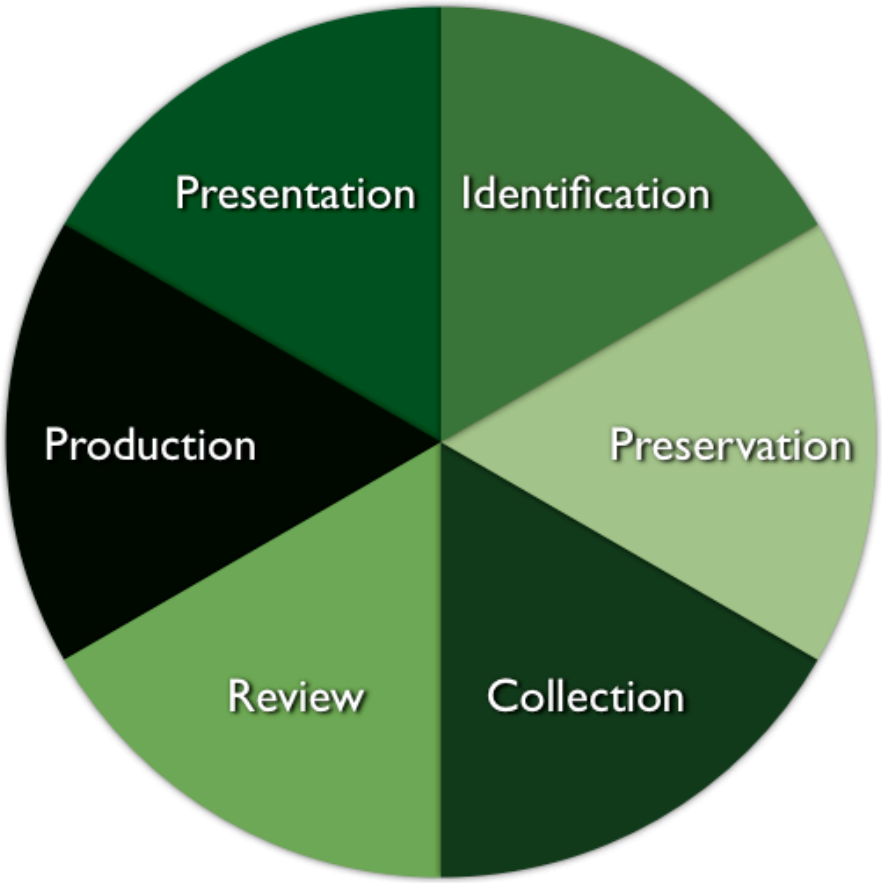
Considering the wide range of technology knowledge within the legal community, it would be advantageous for those who are savvy and involved in the litigation process to confer with their attorneys to help them understand what they should request.

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.

The Electronic Discovery Process



- 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 Shmoocon in February 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 has the potential to level the playing field for litigants in much the same way that the internet has for individual expression.

It is always a pleasure to speak at DEFCON and I appreciate the opportunity to speak at Blackhat, and I look forward to seeing you all again 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, future 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, the sweet spot in the hallway where an open AP could be found at the Washington Marriott, and the Smoking Oasis in Pasadena. The font used in the presentation and this accompaniment is Helvetica Neue.