Chapter 1:
Introduction to eDiscovery Concepts

Terms:

Discovery: *the pre-trial phase in a lawsuit in which each party can obtain information from the opposing party via the use of requests for documents and the answering of submitted questions*

eDiscovery: *refers to discovery in civil litigation that deals with the exchange of information in an electronic format*

Litigation Hold: *a notice or communication from legal counsel to an organization or party issued as a result of current or anticipated litigation to avoid evidence spoliation that suspends the normal disposal or processing of information*

Spoliation: *destruction or alteration of evidence or the failure to preserve evidence*

Records Custodian: *a person or team tasked with the safekeeping, organization and control of information within defined parameters for a particular entity(s)*

Metadata: *data that itself describes the contents and context of its parent data file(s)*

Defining Discovery

The word *discovery* describes the process of opposing parties involved in civil litigation giving and receiving of information regarding the complaint at issue. This exchange of information is a crucial element in the litigation process as it gives both parties a chance to view the other party's information. Knowing the contents of the opposing party's files, for example, can then help the receiving party determine what cause(s) of action the other side may emphasize, what avenues of thought the opposition may be pursuing, or even serve to highlight issues or concerns notable because of their very absence.

When discovery occurs

Discovery occurs after a lawsuit has been commenced and ideally after a *litigation hold* has been sent to the required people or entities. Required parties are those the plaintiff (or defendant) believes may have access to or knowledge of pertinent information necessary to the impending litigation.

Importance of litigation holds

In the past, a litigation hold (also known as a *spoliation letter*), was usually a letter or fax sent to opposing counsel and other parties instructing them to retain all information related to the subject of the complaint.

However, simply not throwing a piece of paper away is no longer enough to satisfy a litigation hold and an entire protocol has been developed around the process that helps (supposedly) assure that important information is preserved. These protocols provide protection for both the requesting and receiving parties.

Basic Discovery Timeline

A suit is filed. A summons is served. People start sweating. Attorneys are hired. Strategy begins to form. Targets are assessed. Litigation holds are disseminated. Records custodians are identified. Depositions are requested. Set one of each party's discovery Interrogatories and Requests for Production (commonly abbreviated as ROGs and RFPs) are drafted and sent to the opposing party. Paralegals start receiving massive amounts of information. People keep sweating.

Discovery continues until a paralegal dies under an avalanche of paper, the deadline for discovery requests is reached (often ninety or even sixty days prior to the start of trial), one—or both—parties are driven to the edge of bankruptcy through a massive War of Paper, enough objections to discovery are made to halt the process or the attorney handling the case feels they have gathered the requisite information.

eDiscovery v. Traditional Discovery

Electronic discovery, or *eDiscovery*, is simply the discovery of information that is held in an electronic format. Paper is, naturally, still produced during the course of business but electronic information is becoming more and more the format of choice.

Information requested in eDiscovery is often referred to as *electronically stored information* (ESI) and the people involved in creating, maintaining, and producing this information are referred to as records custodians, data management specialists, content management specialists, litigation specialists, or litigation support technicians.

As you can see, many terms for a single process or job can quickly lead to chaos; this is precisely why the field of eDiscovery is so confusing and difficult to understand—especially for those who do not have a strong technology background.

What eDiscovery Covers

All information is, at heart, basically the same—a transfer or record of knowledge (data) from one source to another in a format that is accessible by at least one party.

Thus, handwritten secret Cracker Jack decrypto codes are, effectively, the same as WEP or WPA2 internet encryption protocols. Notes locked in a safe buried in the kitchen of a banking executive's summer home are the same as incriminating photographs cleverly hidden in a computer file marked TAXES—1996. The only thing that has changed is the *format* of the information, how it is *stored*, and how it is *retrieved*.

Metadata

As if it couldn't possibly be more confusing, consider that electronic data itself occasionally contains hidden information. This information could be the author of the

© 2015 National Paralegal College

document, its date of creation, time it was last edited and by whom. Sometimes the electronic records of changes made to a document are either incorrectly removed—or not removed at all—which allows a savvy party on the opposing side access to things they would *never* have been given during paper-based discovery.

This type of hidden data is referred to as *metadata* and has no counterpart in physical documentation even though the subject matter of each basic piece of overlying data may be exactly the same. Courts have ruled that inadvertently sending metadata doesn't constitute an automatic breach of privilege but that using metadata against a party or person when that party obviously didn't know the information was there *did* constitute unethical behavior. It all is quite confusing in a chicken-egg sort of way. *In re Verisign Sec. Litig.*, 2004 U.S. Dist. LEXIS 22467 (N.D. Cal. Mar. 10, 2004).

Nowadays, it's common to hear people say, "It's not *my* fault they didn't know it [the potentially damaging hidden information] was there. What was I *supposed* to do with it?! Just ignore the fact that the document they gave us in discovery shows their original settlement offer was *twice* what they initially offered us?" You can't unring a bell, is the common saying, but what to do when you didn't even know there was a bell to ring?

Controversy continuously surrounds these rulings as some technologically adept users feel they are being penalized for their opposition's willful (or feigned) lack of technological skill. In short, many practitioners who do comfortably span the chasm between law and technology feel court opinions in certain areas not only provide protection for morons and idiots but effectively quashes the supremely useful skills these multidimensional litigators bring to the table often to their client's detriment.

This field has begun to reshape the classic *duty of zealous advocacy* that reigns supreme in every lawyer's hierarchy of responsibility. What is truly "zealous" when there are sliding scales of competency that appear to be situationally dependent? What is "advocacy" if certain parties are restricted from using particular tools or processes simply because opposing counsel or, (dare I even say it) the judge, simply lack the skills necessary to adjudicate a cause of action according to increasingly common principles. In this emerging field, it may actually be a hindrance to be the smartest person in the room.

Limits to Discovery

Most of the same restrictions apply to eDiscovery that apply to regular, paper-based discovery. The same difficulties arise in eDiscovery as in any other discovery methodology when parties are trying to determine what should be protected.

Material produced during the course of litigation as work product or covered under attorney-client privilege retains those protections regardless of the format it holds. But, the methods of determining those protections have changed during the course of technological advance.

Information protection strategies, protective orders, privilege logs and other methods of identifying and retaining confidential information are all discussed in future classes.

© 2015 National Paralegal College

Categories of electronic data. Unlike paper-based discovery, information stored electronically can appear in varied formats. Here are five common electronic data categories considered when determining what is discoverable:

1. Online data
2. Near-line data
3. Offline storage
4. Backup tapes
5. Fragmented, erased and damaged data.

These categories have emerged through a series of precedent-setting court decisions beginning with the landmark case *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003), the passage of the December 1, 2006 amendments to the Federal Rules of Civil Procedure as well as the new FRCP amendments currently before the Supreme Court for consideration.

Types of Common Electronic Discovery

1. Email
2. Instant Messages
3. Twitter tweets
4. Facebook posts
5. Smartphone and PDA data
6. Voicemail
7. Databases
8. Photographs and Drawings
9. Website plans and coding
1. Raw data

The Beginning of the End: *Zubulake v. UBS Warburg LLC* (2003)

Zubulake v. UBS Warburg, id., is usually referred to as just *Zubulake*. This case occurred in the Southern District court of New York prior to the 2006 amendments to the FRCP. In *Zubulake*, the plaintiff (Laura Zubulake) filed suit against her ex-employer (UBS Warburg *aka* UBS) alleging retaliation, failure to promote and gender discrimination. 217 F.R.D. 309 (S.D.N.Y. 2003).

The opinions in *Zubulake* are known as *Zubulake* I, III, IV, and V and are still some of the most widely quoted and most influential in the eDiscovery field. The responsibilities arising from the court's rulings are now euphemistically referred to as The Zubulake Duty.

Zubulake I and III. The plaintiff argued that crucial information essential to proving her case existed in emails sent between UBS employees during the time period she alleged the causes of action were occurring. Supporting this claim were the approximately 450 pages of email between UBS employees and herself that she produced during the course of

© 2015 National Paralegal College

litigation. In return, UBS produced . . . not so much. In fact, UBS only produced in totality about 100 pages of email. Clearly there was a disconnect.

The plaintiff argued that UBS should be forced to retrieve the emails from their backup data archives and tapes *and* cover the cost of the recovery. UBS argued the cost was so prohibitive that the plaintiff should bear the cost of the production because she was the party requesting the information. UBS made this cost-shifting argument using the 2002 *Rowe* decision as justification. *Rowe Entertainment v. The William Morris Agency*, 205 F.R.D. 421 (S.D.N.Y. 2002).

In *Rowe*, *id.,* the litigant estimated it would cost approximately $10 million to satisfy a single document request made by the other party. This seems ridiculous on its face but consider that computer chip manufacturer Intel produced over *15 million documents* during its historic antitrust case against Advanced Micro Devices in 2002.

At one point, Intel was given only thirty days to produce over 1,000 emails they had already erased and/or archived—a daunting task for a corporation of any size. ***Advanced Micro Devices, Inc. v. Intel Corp. (AMD)***, Civ. Action No. 05-441-JJF, --- F.Supp.2d ----, 2006 WL 2742297 (D. Del. Sept. 26, 2006).

Today, it's not unusual for even small to medium-sized companies to be tasked with producing large amounts of e-mails, backup tapes and other materials in order to satisfy discovery requirements. EDiscovery and its potentially prohibitive costs are now part of every litigant's reality and the responsibility of managing data so that it can be produced in a reasonable time is no longer limited to only firms or companies with deep pocketbooks and robust employee resources.

The *Zubulake* court ruled the determining factor in deciding what "unduly burdensome or expensive" production was "turn[ed] primarily on whether it [the information] is kept in an accessible or inaccessible format." *Zubulake v. UBS Warburg LLC*, 217 F.R.D. at 318. Eventually, the judge ruled that backup tapes and erased, damaged or otherwise fragmented data (the last two in the list we discussed earlier in this segment) were patently inaccessible and therefore cost-shifting *would* apply in those circumstances.

But, the court also decided that the balancing test set forth in *Rowe, supra,* was a bit outdated and thus set forth a new seven-factor test still in use today. These seven factors are:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total costs of production compared to the amount in controversy;
4. The total costs of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and

   The relative benefits to the parties of obtaining the information.
   (citing *Zubulake* III, 216 F.R.D. at 284)

© 2015 National Paralegal College

UBS was eventually ordered both to pay all the costs of its own production and to produce the information requested. The courts ruled a cost-shifting discussion would only be entertained after the contents of the production were revealed.

In the end, the plaintiff was ordered to pay 25 percent of the restoration cost (the total cost of the restoration was estimated by UBS to be about $273,649). These costs, fortunately for her, did not include the costs of paying an attorney to review the results of the restoration.

Zubulake IV. After settling the cost-shifting debate discussed above, the court then had to decide what was to be done about the backup tapes UBS claimed were no longer available. While the emails sought by the plaintiff were, naturally, stored only on these allegedly unavailable resources much of the information that fell under the production mandate was also irrelevant to her case. The plaintiff argued that she should not be forced to pay for the restoration of information that was, in essence, useless. The judge agreed, flipping the court's previous decision by ruling that UBS must cover the entire cost of both the restoration and its resulting production.

Duty to preserve. Most important was the ruling of the court in *Zubulake IV*: that UBS had a duty to preserve evidence that was likely to be relevant during future litigation (hence, the importance of the litigation hold). This phrase has been the call to arms for every plaintiff from *Zubulake* onward when defendant(s) fail to produce certain information deemed essential by the plaintiff. This ruling prompted what was, at that time, the biggest eDiscovery smackdown in the then-limited history of extreme eDiscovery judicial sanctions.

Zubulake V. It was the ruling that no defendant wants to hear—and that no defendant's IT department manager wants to hear, either—UBS had failed to preserve data it should have *reasonably* known would be relevant to future litigation. This failure had resulted in their inability to produce information crucial to the plaintiff's case (and, of course, information that likely would have been highly adverse to UBS). As punishment, the judge ordered an adverse inference instruction be given to the jury. This instruction said:

> "[i]f you find that UBS could have produced this evidence, evidence within its control, and the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to INFER THE EVIDENCE WOULD HAVE BEEN UNFAVORABLE TO UBS." (emphasis added) *Zubulake V,* slip op. at 40.

Oh, the agony of UBS. An adverse inference instruction, though not necessarily as devastating to UBS as a default or summary judgment, nonetheless blew a gigantic hole of doubt directly through the heart of their defense. The jury went out, came back after a moderate deliberation, ruled for the plaintiff and pounded UBS with a *29 million dollar verdict*.

Ouch. That's a big price to pay for a few deleted emails.

© 2015 National Paralegal College

The *Zubulake* Fallout

Lawyers across America immediately hid underneath their desks quivering with fear. Those attorneys whose only knowledge of servers involved the people who brought them martinis during lunch frantically sent out the S.O.S.—Send us Obviously Savvy technological wizards capable of Saving us—and our clients—from our own ignorance (and our bottom line from decimation, ala UBS).

Zubulake eventually ended in a private settlement of an undisclosed financial nature but the case's effect has lingered on like Limburger in a hot Mercedes. It was clear to everyone that the landscape of litigation had been radically changed by this newfangled eDiscovery element. Serious repercussions for technological ignorance now existed and attorneys became very nervous as every client involved in litigation began to expect their counsel to keep them out of the court's electronically aimed crosshairs.

Lack of investigation grounds for sanctions. Of course, attorneys themselves are not immune to personal sanctions resulting from a lack of eDiscovery knowledge. In ***Phoenix Four, Inc. v. Strategic Resources Corp.***, both a law firm and its clients were sanctioned for the attorneys' failure to personally investigate and understand that two of the clients' computer servers had hidden partitions containing discoverable ESI. The court concluded, "The computer system in [the client's] office was configured in such a way that the desktop workstations did not have a 'drive mapping' to that partitioned section of the hard drive." No. 05-CIV-4837, 2006 WL 1409413; 2006 U.S. Dist. LEXIS 32211 (S.D.N.Y. May 22, 2006).

[If you have trouble understanding the above statement just imagine how the attorneys felt when they (likely) couldn't even decipher the reason for their own sanction!]

In *Phoenix, id.,* the defendants' law firm ended up with $22,581 in sanctions for overlooking the hidden server partitions. (S.D.N.Y. Aug. 1, 2006). The court also applied a standard that would eventually become FRCP rule 26(b)(2)(B) which requires the disclosure of sources of inaccessible data. In this case, however, the data was not inaccessible, it was just hidden in a partitioned section of the hard drive. The attorneys did not understand the difference between the two concepts and personally paid for their mistake.

Lack of knowledge ruled misconduct. It gets worse. In a 2008 case, ***Qualcomm Inc. v. Broadcom Corp., "Qualcomm II"***, 2008 U.S. Dist. LEXIS 911 (S.D. Cal. Jan. 7, 2008), nineteen Qualcomm, Inc., attorneys were found to have committed misconduct and six of them were actually reported to the State Bar for investigation after they failed to conduct an e-mail search on *obvious* custodians regarding an issue that was *obviously* central to the case (emphasis added). Qualcomm was also ordered to recompense more than $8.5 million to Broadcom for attorneys' fees and other litigation costs.

In a happy-ish ending, the judge in *Qualcomm* eventually decided his previously levied sanctions were no longer necessary explaining that even though the lawyers never pursued "several discovery paths that seem[ed] obvious, at least in hindsight . . . the involved attorneys did not act in bad faith." *Id.*

Tardy litigation hold ruled gross negligence. Actions during discovery aren't the only murky waters attorneys (and their paralegals) must traverse. Trouble often begins at the start of or even prior to the actual litigation. The failure to issue a litigation hold early

© 2015 National Paralegal College

enough in a cause of action was held to be gross negligence by counsel in ***Pension*** *Comm. of Univ. of Montreal* ***Pension*** *Plan v.* ***Bank of Am. Secs.***, ***LLC***, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).

Personal embarrassment due to ignorance. Occasionally attorneys are subjected to rather humiliating comments handed down publicly from the bench by tech savvy judges as in ***Martin v. Northwestern Mutual Life Insurance Company***. Here, the court quashed an attorney's excuse of "computer illiteracy" as a reason for mishandling electronic data issues as "frankly ludicrous." 2006 WL 148991 (M.D Fla. Jan. 19, 2006).

Effects stretch far past civil litigation. Criminal trials aren't immune to the eDiscovery mandates being handed down on a regular basis from the courts. In ***State v. Huggett***, the failure to preserve voicemail led to the dismissal of a second degree murder charge. 2010 WI App 69.

Conclusion

As you can clearly see, the brief discussion here of the early days of eDiscovery tribulations should be taken as a present warning to all practicing legal professionals. Advances in technology and eDiscovery continue to change the field of law in both dramatic fashion and quick succession (including the most recent suggested changes to the Federal Rules of Civil Procedure addressing the handling of electronic information that are even now before the Supreme Court). It is our desire that by the end of this electronic discovery and litigation management survey course you will have a greater breadth of knowledge regarding this increasingly essential element of your future practice.

© 2015 National Paralegal College